HAL
open science

ADVANCED METHODS FOR THE RISK, VULNERABILITY AND RESILIENCE ASSESSMENT OF SAFETY-CRITICAL ENGINEERING COMPONENTS, SYSTEMS AND INFRASTRUCTURES, IN THE PRESENCE OF UNCERTAINTIES

Nicola Pedroni

To cite this version:

Nicola Pedroni. ADVANCED METHODS FOR THE RISK, VULNERABILITY AND RESILIENCE ASSESSMENT OF SAFETY-CRITICAL ENGINEERING COMPONENTS, SYSTEMS AND INFRASTRUCTURES, IN THE PRESENCE OF UNCERTAINTIES. Engineering Sciences [physics]. Grenoble 1 UGA - Université Grenoble Alpes, 2016. tel-01436723

HAL Id: tel-01436723

https://hal.science/tel-01436723

Submitted on 23 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Université Grenoble Alpes (UGA)

Institut National Polytechnique de Grenoble (INP)

École Doctorale Electronique, Electrotechnique, Automatique, Traitement du Signal (EEATS)

Rapport d'activité Scientifique

Présenté en vue de l'obtention de

l'Habilitation à Diriger des Recherches (HDR)

par

Nicola Pedroni

ADVANCED METHODS FOR THE RISK, VULNERABILITY AND RESILIENCE ASSESSMENT OF SAFETY-CRITICAL ENGINEERING COMPONENTS, SYSTEMS AND INFRASTRUCTURES, IN THE PRESENCE OF UNCERTAINTIES

Date de soutenance: 04-02-2016

Composition du jury:

Rapporteurs:
Prof. **Terje Aven**, University of Stavanger (UIS)
Prof. **Bruno Sudret**, Swiss Federal Institute of Technology in Zurich (ETHZ)
Prof. **Antoine Grall**, Université de Technologie de Troyes (UTT)

Examinateurs:
Prof. **Christophe Bérenguer**, Université Grenoble Alpes (UGA) – Institut National Polytechnique (INP) de Grenoble
Prof. **Enrico Zio**, École CentraleSupélec and Politecnico di Milano

Table of contents

LIST OF ACRONYMS **4**

LIST OF FIGURES **6**

LIST OF TABLES **7**

1 INTRODUCTION **8**

2 CURRICULUM VITAE **10**

3 SYNTHETIC PRESENTATION OF TEACHING AND ADMINISTRATIVE ACTIVITIES **12**

3.1 TEACHING ACTIVITIES 12

3.2 ADMINISTRATIVE ACTIVITIES 17

4 SYNTHETIC PRESENTATION OF THE RESEARCH ACTIVITIES **18**

4.1 OVERVIEW ON THE RESEARCH ACTIVITIES 18

4.2 PUBLICATIONS STATISTICS 21

4.3 LIST OF PHD AND MASTER STUDENTS CO-DIRECTED 23

4.4 SYNTHETIC PRESENTATION OF FUTURE RESEARCH 28

4.4.1 Research themes *28*

4.4.2 Research methods *31*

4.5 SYNTHETIC PRESENTATION OF THE CAPITALIZATION AND TRANSFER ACTIVITIES 32

4.6 SCIENTIFIC OUTREACH 35

5 COMPLETE AND CLASSIFIED LIST OF PUBLICATIONS AND COMMUNICATIONS **40**

5.1 PEER-REVIEWED INTERNATIONAL JOURNAL PAPERS 40

5.2 BOOK CHAPTERS 43

5.3 CONFERENCE PROCEEDINGS 44

5.4 WORKS PUBLISHED AS TECHNICAL REPORTS OF INTERNATIONAL RESEARCH INSTITUTES 47

6 DETAILED PRESENTATION OF THE PAST RESEARCH ACTIVITIES **48**

6.1 AXIS 1 – RELIABILITY ANALYSIS AND RISK ASSESSMENT OF SAFETY-CRITICAL COMPONENTS AND SYSTEMS: UNCERTAINTY MODELING AND QUANTIFICATION 52

6.1.1 Problem statement *52*

6.1.1.1 Uncertainties in reliability analysis and risk assessment 52

6.1.1.2 Types of uncertainty 54

6.1.2 Issues and possible solution approaches: a critical literature survey *55*

6.1.2.1 Issue 1: Quantitative modeling and representation of uncertainty coherently with the information available on the system 56

6.1.2.2 Issue 2: Propagation of uncertainty to the output of the system model 66

6.1.2.3 Issue 3: Updating as new information becomes available 67

6.1.2.4 Issue 4: Dependences among input variables and parameters 68

6.1.3 Research developed: methodological and applicative contributions *70*

6.1.3.1 Issue 1: Quantitative modeling and representation of uncertainty coherently with the information available on the system 70
6.1.3.2 Issue 2: Propagation of uncertainty to the output of the system model 74
6.1.3.3 Issue 3: Updating as new information becomes available 75
6.1.3.4 Issue 4: Dependences among input variables and parameters 77
6.2 AXIS 2 – SAFETY-CRITICAL SYSTEMS AND INFRASTRUCTURES: ADVANCED METHODS FOR MODELING, SIMULATION AND ANALYSIS CONSIDERING UNCERTAINTIES 80
6.2.1 Problem statement 80
6.2.1.1 Safety-Critical Systems and Infrastructures 80
6.2.1.2 Risk, vulnerability and resilience 82
6.2.2 Issues and possible solution approaches: a critical literature survey 87
6.2.2.1 Issue 1: Development of innovative methods of representation and simulation of Critical Infrastructures (CIs), for the analysis of their vulnerability and resilience 89
6.2.2.2 Issue 2: Design and implementation of innovative algorithms for the efficient risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures 95
6.2.2.3 Issue 3: Development of innovative decision making approaches for the multi-criteria vulnerability analysis of safety-critical systems and infrastructures under uncertainty 102
6.2.3 Research developed: methodological and applicative contributions 105
6.2.3.1 Issue 1: Development of innovative methods of representation and simulation of critical infrastructures, for the analysis of their vulnerability and resilience 105
6.2.3.2 Issue 2: Design and implementation of innovative algorithms for the efficient risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures 111
6.2.3.3 Issue 3: Development of innovative decision making approaches for the multi-criteria vulnerability analysis of safety-critical systems and infrastructures under uncertainty 116
7 DETAILED PRESENTATION OF THE FUTURE RESEARCH ACTIVITIES 120
7.1 RESEARCH THEMES 120
7.2 RESEARCH METHODS 129
8 CONCLUSIONS 132
9 BIBLIOGRAPHY 134
APPENDIX: CONTENTS OF SIX SELECTED PUBLICATIONS 152

List of Acronyms

AK	Adaptive Kernel
AM-SIS	Adaptive Metamodel-based Subset Importance Sampling
ANN	Artificial Neural Network
ARIMA	AutoRegressive-Integrated-Moving Average
BE	Basic Event
BPA	Basic Probability Assignment
CCF	Common Cause Failure
CDF	Cumulative Distribution Function
CE	Cross-Entropy
CESNEF	CEntro Studi Nucleari Enrico Fermi
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
COM	Commission of the European Community
DBC	Dependency Bound Convolution
DEnv	Distribution Envelop Determination
DET	Dynamic Event Tree
DM	Decision Making
DMLD	Dynamic Master Logic Diagram
DS	Dempster-Shafer Dempster-Shafer
DSTE	Theory of Evidence
ECP	Ecole Centrale Paris
EDF	Electricité De France
EENS	Expected Energy Not Supplied
ELECTRE	ELimination Et Choix Traduisant la REalité
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
ERNCIP	European Reference Network for Critical Infrastructure Protection
ESREL	European Safety and RELiability Conference
ET	Event Tree
ETA	Event Tree Analysis
FEM	Finite Element Model
FIA	Fuzzy Interval Analysis
FonCSI	Fondation Pour Une Culture De Securitè Industrielle
FPDF	Fuzzy Probability Density Function
FPTN	French Power Transmission Network
FRV	Fuzzy Random Variable
FT	Fault Tree
FTA	Fault Tree Analysis
GBT	Generalized Bayes Theorem
GFR	Gas-cooled Fast Reactor
GTST	Goal Tree Success Tree
HDR	Habilitation à Diriger des Recherches
ICT	Information and Communication Technology
IDPSA	Integrated Deterministic and Probabilistic Safety Assessment
IEEE	Institute of Electrical and Electronic Engineers
IF	Importance Function
IIR-LRNN	Infinite Impulse Response Locally Recurrent Neural Network
IPTN	Italian Power Transmission Network
IRS	Independent Random Sets
IS	Importance Sampling
ISD	Importance Sampling Density
KS	Kolmogorov-Smirnov
LaRC	Langley Research Center
LASAR	Laboratory of Analysis of Signal and Analysis of Risk
LBE-XADS	Lead Bismuth Eutectic eXperimental Accelerator Driven System
LGI	Laboratoire Génie Industriel
LHS	Latin Hypercube Sampling
LS	Line Sampling

MAUT	Multi-attribute utility theory
MCDA	Multi-Criteria Decision Aid
MCMC	Markov Chain Monte Carlo
MCS	Monte Carlo Simulation
MIP	Mixed Integer Programming
MIT	Massachusetts Institute of Technology
MFM	Multilevel Flow Modeling
ML	Motter-Lai
MLD	Master Logic Diagram
MNE	Master in Nuclear Energy
MOV	Motor-Operated Valves
MR-Sort	Majority Rule Sorting
MUQC	Multidisciplinary Uncertainty Quantification Challenge
NASA	National Aeronautics and Space Administration
NECSI	New England Complex Systems Institute
NPP	Nuclear Power Plant
NSBDE	Non-dominated Sorting Binary Differential Evolution
NSGA	Non-dominated Sorting Genetic Algorithm
OPA	ORNL-PSerc-Alaska
ORNL	Oak Ridge National Laboratory
OSIL	Optimisation des Systèmes Industriels et Logistiques
PCE	Polynomial Chaos Expansion
PDF	Probability Density Function
PDMP	Piecewise Deterministic Markov Processes
PRA	Probabilistic Risk Assessment
Pserc	Power System Engineering Research Center (of Wisconsin University)
QRA	Quantitative Risk Assessment
RAMS	Reliability, Availability, Maintainability and Safety
RBF	Radial Basis Function
RESTART	REpetitive Simulation Trials After Reaching Thresholds
RISEGrid	Research Institute for Smarter Electric Grids
ROP	Resilience Optimization Problem
RS	Response Surface
RTE	Réseau de Transport d'Electricité
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SC	Stochastic Collocation
SCADA	Supervisory Control And Data Acquisition
SOC	Self-Organized Criticality
SoS	System-of-Systems
SPRA	Seismic Probabilistic Risk Assessment
SRA	Society for Risk Analysis
SS	Subset Simulation
SSARS	Summer Safety and Reliability Seminars
SSEC	Systems Science and Energy Challenge
SVM	Support Vector Machine
TE	Top Event
UAV	Unmanned Aerial Vehicle
UCTE	Union for the Coordination of Transmission of Electricity
USNRC	US Nuclear Regulatory Commission
VM	Variance Minimization
WCDR	World Conference on Disaster Reduction

List of Figures

Figure 1. Conceptual structure of the general research framework

Figure 2. Research Axes 1 and 2 developed during my academic activity

Figure 3. Four conceptual and practical issues addressed under research Axis 1

Figure 4. Example of probability box (p-box) for the generic uncertain variable Y

Figure 5. Left: triangular possibility distribution $\pi^Y(y)$ *of a generic uncertain variable Y; in evidence, the α-cuts of level α = 0 (solid segment), 0.5 (dashed segment) and 1 (dot). Right: bounding upper and lower CDFs (i.e., cumulative possibility and necessity) of Y,* $\underline{F}^Y(y) = N^Y(A) = N^Y((-\infty, y])$ *and* $\overline{F}^Y(y) = \Pi^Y(A) = \Pi^Y((-\infty, y])$*, A = (–∞, y], respectively*

Figure 6. Exemplary body of evidence (left) and the corresponding upper and lower CDFs (i.e., cumulative plausibility and belief) (right) for a generic uncertain variable Y

Figure 7. Exemplary Fuzzy Random Variable (FRV). Left: possibility function $\pi^\mu(\mu)$ *for the mean μ of variable Y. Right: bounding upper and lower CDFs of Y,* $\overline{F}_\alpha^Y(y)$ *and* $\underline{F}_\alpha^Y(y)$*, built in correspondence of the α-cuts of level α = 0 (solid lines), 0.5 (dashed lines) and 1 (dot-dashed line) of* $\pi^\mu(\mu)$

Figure 8. Methods here considered and compared to address Issue 1 of research Axis 1, together with the corresponding applications and recommended approaches

Figure 9. Methods here considered and compared to address Issue 2 of research Axis 1, together with the corresponding applications and recommended approaches

Figure 10. Methods here considered and compared to address Issue 3 of research Axis 1, together with the corresponding applications and recommended approaches

Figure 11. Methods here considered and compared to address Issue 4 of research Axis 1, together with the corresponding applications and recommended approaches

Figure 12. Main characteristics of the safety-critical systems and infrastructures of interest to the present dissertation, and the corresponding related issues

Figure 13. Illustration of the concepts of risk, vulnerability, robustness and resilience with reference to the functionality curve Φ(t) of a safety-critical system or infrastructure

Figure 14. Three conceptual and practical issues addressed under research Axis 2

Figure 15. Problems related to the efficient risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures (Issue 2, Axis 2)

Figure 16. Problems related to decision making process for the multi-criteria vulnerability analysis of safety-critical systems and infrastructures under uncertainty (Issue 3, Axis 2)

Figure 17. Methods here considered and compared to address Issue 1 of research Axis 2, together with the corresponding applications

Figure 18. Methods here considered and compared to address Issue 2 of research Axis 2, together with the corresponding applications

Figure 19. Methods here considered and compared to address Issue 3 of research Axis 2, together with the corresponding applications

Figure 20. Themes and methods that will be addressed in my future research

List of Tables

Table 1. Summary of the main teaching activities and content of the lectures

Table 2. Number of classified publications

Table 3. Analysis of the research collaborators

Table 4. Synthetic presentation of the capitalization and transfer activities

Table 5. Planning of the future research activities during 2015-2020

1 Introduction

This thesis presents my complete profile as an assistant professor at: (i) the Laboratory of Analysis of Signal and Analysis of Risk (LASAR) of the Energy Department of the Politecnico di Milano (Milano, Italy) (from March 2010 to February 2013); and (ii) the Chair on Systems Science and Energy Challenge (SSEC) installed in 2010 at CentraleSupélec with the support of Fondation Électricité De France (EDF) (from March 2013 to present). It serves as the main document supporting my application for the Habilitation à Diriger des Recherches (HDR) (Habilitation to Direct the Research).

The research works presented in this thesis entitled "Advanced methods for the risk, vulnerability and resilience assessment of safety-critical engineering components, systems and infrastructures, in the presence of uncertainties" have been conducted before at the LASAR Laboratory and then at the Chair SSEC, both directed by Professor Enrico Zio. The major activities of both research groups have focused on the development, implementation and use of computational models, methods and algorithms for the analysis of the failure behavior of complex engineered systems and the related uncertainty. Then, the research topics of interest to both groups cover aspects related to reliability, availability and maintainability (RAM) engineering, risk assessment, safety and security evaluation, vulnerability and resilience analyses.

Within this wide context, my past research consists of two main axes:

1. *uncertainty modeling* and *quantification* techniques for the reliability analysis and risk assessment of safety-critical components and systems;
2. *advanced methods* for *modeling*, *simulation* and *analysis* of safety-critical systems and infrastructures under uncertainties, in order to assess their associated *risk*, *vulnerability* and *resilience*.

Four main research issues have been treated under Axis 1, whereas three issues have been addressed under Axis 2. The motivations, originalities and contributions within each research line are thoroughly presented in Section 6: in addition, for the sake of clarity and completeness six journal papers have been included in the Appendix at the end of the manuscript in order to provide the interested reader with further technical details about the topics and issues addressed.

The future research has been planned around three main *themes* that are currently credited by many as among the most relevant for the analysis and management of the risk and vulnerability of complex, safety-critical systems and infrastructures:

1. modeling and analysis of (*extreme*) *external natural events*;
2. integration of the risks and vulnerabilities coming from *cyber attacks*;

3. management of *multiple* risks coming from heterogeneous '*contributors*' (e.g., *different* types of *hazard*) and different '*locations*' (e.g., *different* power production *units* on the same site), for their *aggregate evaluation*.

These analyses require substantial and consistent supports from the further advancements of all existing research lines. The detailed presentation of future work is in Section 7. A synthetic description of both past and future research is instead presented in Section 4, together with my supervision works which involved co-directing a number of PhD and master students. Most of them resulted to international journal publications. The complete and classified list of publications and communications is presented in Section 5.

The teaching activities, presented in Section 3, were developed mainly in three areas: (i) Reliability, Availability, Maintenance and Safety (RAMS) techniques and their applications to engineered systems; (ii) advanced computational methods for the efficient representation and propagation of uncertainties through the mathematical models of engineered systems; (iii) thermodynamics and heat transfer in nuclear reactor systems. The levels have ranged from first years of national engineering schools to international masters and PhD courses. The activities have included presenting lectures, delivering tutorials, monitoring exams, and supervising projects and theses. The teaching has fed my research activities and certain research results have been transferred to the students through teaching.

My administrative activities have been carried out mainly at the Laboratoire Génie Industriel (LGI) at CentraleSupélec where the Chair SSDE has been located.

Following is my complete presentation, starting from the curriculum vitae.

2 Curriculum Vitae

Nicola Pedroni

Current position: Assistant Professor, Chair on Systems Science and the Energy Challenge-Fondation EdF, at École CentraleSupélec, Paris.

Professional addresses:
Chaire on Systems Science and the Energy Challenge
3, rue Joliot-Curie – Plateau de Moulon
91192 Gif-sur-Yvette, France
Tel: +33 (0)1 69 85 15 35

Laboratoire Génie Industriel (LGI)
Grande Voie des Vignes
92295 Chatenay-Malabry, France
Tel: +33 (0)1 41 13 19 16 (preferable)
Fax: +33 (0)1 41 31 19 16
Emails: nicola.pedroni@ecp.fr, nicola.pedroni@supelec.fr, nicola.pedroni@centralesupelec.fr

Administrative Supervisors: Prof. Christophe Bérenguer and Prof. Pierre-Yves Coulon
Scientific Supervisor: Prof. Enrico Zio

Educational Experience

- National (Italian) Academic Qualification to be an Associate Professor in the Scientific Disciplinary Area 09/C2 – Thermodynamics and Nuclear Engineering. The qualification has a validity of 6 years, February 2014 – February 2020.

- PhD in Radiation Science and Technology at the Politecnico di Milano (Milano, Italy), with first class honours, March 01, 2010.
  Thesis title: "Advanced Monte Carlo Simulation Methods and Neural Network Regression for the Reliability Analysis of Nuclear Passive Systems".
  The work was carried out at the Laboratory of Signal and Risk Analysis (LASAR) of the Energy Department of the Politecnico di Milano (Milano, Italy).

- Visiting Ph. D. Student at the Department of Nuclear Science and Engineering of the Massachusetts Institute of Technology (MIT) (Cambridge, Massachusetts - USA), under the supervision of Prof. G. E. Apostolakis, September 2008 – May 2009.
  Title of the research project: "Simulation methods for uncertainty and sensitivity analysis of physical-mathematical models of safety-critical systems" (the visit has been supported by the Progetto Roberto Rocca Fellowship).

- (Second Level) Degree in Nuclear Engineering at the Politecnico di Milano (Milano, Italy), with the score of 110/110 cum laude, December 22, 2005.
  Awarded of the prize for the best Graduate Student of the Year in Nuclear Engineering.
  Thesis title: "Genetic Algorithms for Feature Selection in Nuclear Diagnostics".
  The work was carried out at the Laboratory of Signal and Risk Analysis (LASAR) of the Department of Nuclear Engineering – CEntro Studi Nucleari Enrico Fermi (CESNEF) of the Politecnico di Milano (Milano, Italy).

- (First Level) Degree in Energetic Engineering at the Politecnico di Milano (Milano, Italy), with the score of 110/110 cum laude, July 24, 2003.
  Thesis title: "Comparison of 'balance of plants' for space applications of nuclear reactors".
  The work was carried out at the Department of Nuclear Engineering – CEntro Studi Nucleari Enrico Fermi (CESNEF) of the Politecnico di Milano (Milano, Italy).

Post-graduation courses

- Summer School "Summer Safety and Reliability Seminars (SSARS) 2007", 1st Edition, Gdansk-Sopot, Poland, July 22-29, 2007.

- Professional training course titled "Innovative techniques for the evaluation of the reliability and availability of industrial plants", 9th Edition, 25-28 September 2006, held at the Department of Nuclear Engineering – CEntro Studi Nucleari Enrico Fermi (CESNEF) of the Politecnico di Milano (Milano, Italy).

Professional Experience

- Assistant professor at the Electricité de France (EdF) Chair "Systems Science & Energetic Challenge" (funded by Fondation EdF) with a joint appointment at Ecole Centrale Pairs (ECP) (Chatenay-Malabry, France) and Ecole Superieure d'Electricite (SUPELEC) (Gif-Sur-Yvette, France), March 1, 2013 – present.

- Assistant professor at the Laboratory of Signal and Risk Analysis (LASAR) of the Energy Department of the Politecnico di Milano (Milano, Italy), June 01, 2010 – February 28, 2013.
  Scientific Disciplinary Area: ING-IND/19 - Nuclear power plants.
  Title of the research program: "Development of advanced methods and models for the safety, reliability, maintenance, diagnostics and prognostics of nuclear and industrial components and systems".

- Visiting researcher at the Laboratoire Genie Industrielle (LGI) (Laboratory of Industrial Engineering) of the Ecole Centrale Paris (ECP) (Chatenay-Malabry, France), September – December 2012.

- Research grant (post-doc) at the Laboratory of Signal and Risk Analysis (LASAR) of the Energy Department of the Politecnico di Milano (Milano, Italy), January 16 – May 31, 2010.
  Title of the research program: "Study and development of advanced computational methods for the reliability assessment, diagnostics and prognostics of industrial components/systems/plants in presence of uncertainties".

- Research grant at the Laboratory of Signal and Risk Analysis (LASAR) of the Department of Nuclear Engineering – CEntro Studi Nucleari Enrico Fermi (CESNEF) of the Politecnico di Milano (Milano, Italy), March 16 – December 31, 2006.
  Title of the research program: "Study and development of feature selection methods for soft-computing models with applications to safety".

3 Synthetic presentation of teaching and administrative activities

(Présentation synthétique des activités d'enseignement et d'administration)

The relevant teaching activities are detailed in Section 3.1, whereas the main administrative responsibilities are summarized in Section 3.2.

3.1 Teaching activities

(Présentation synthétique des activités d'enseignement)

The courses were mainly developed in three areas: (i) Reliability, Availability, Maintenance and Safety (RAMS) techniques and their applications to engineered systems; (ii) advanced computational methods for the efficient representation and propagation of uncertainties through the mathematical models of engineered systems; (iii) thermodynamics and heat transfer in nuclear reactor systems. The levels range from first years of national engineering schools to international masters and PhD courses. The activities include presenting lectures, delivering tutorials, monitoring exams, and supervising projects and theses (see Table 1 for a summary).

- **Responsibility for the organization of Master courses (Lectures = 69hrs; Exercise sessions = 48hrs; Exams = 15hrs)**
  - Co-responsible of the organization and activity of the course "Managing Uncertainty For Reliability Optimization - Maîtrise Des Incertitudes Pour l'Optimisation De La Fiabilité" (24 hours) of the Master Recherche "Optimisation des Systèmes Industriels et Logistiques (OSIL)" held at **CentraleSupélec**, Chatenay-Malabry, France, **November 2014-January 2015**. The activity has entailed the organization of 3 (three-hour) lectures and 1 (three-hour) project exam. Total activity: lectures (9hrs), exam (3hrs).
  - Co-responsible of the organization and activity of the course "Nuclear Thermohydraulics" (45 hours) of the international Master in "Nuclear Energy" run by a consortium of several academic institutions (Universitè Paris-Sud 11, ParisTech, Ecole Centrale Paris and Supelec) with the support of several industrial establishments (EDF, Areva, GDF SUEZ), at the **Commissariat à l'énergie atomique et aux énergies alternatives (CEA)-Institut national des sciences et techniques nucléaires (INSTN)** (Saclay, France), September-December **2012, 2013, 2014 and 2015**. The activity has entailed the organization of 5 (three-hour) lectures, 4 (three-hour) exercise sessions and 1 (three-hour) mid-term exam, for each year of course. Total activity: lectures (60hrs), exercise sessions (48hrs), exams (12hrs).

- **Lectures held during Ph.D. courses (Lectures = 45hrs; Exercise sessions = 0hrs; Tutorials = 6hrs; Exams = 0hrs)**
  - Four-hour lecture and three-hour tutorial titled "Uncertainty modeling", held during the 4th PhD School on "Vulnerability, risk and resilience of complex system and critical infrastructures", organized by CentraleSupélec (Gif-Sur-Yvette, France), Politecnico di Milano (Milano, Italy) and TIME Association, 14-18 September **2015**, CentraleSupélec (Gif-Sur-Yvette, France). Total activity: lectures (4hrs).
  - Four-hour lecture titled "Advanced Monte Carlo simulation methods: Markov Chain Monte Carlo, Subset Sampling, Line Sampling, and applications to reliability analysis", held during the Multidisciplinary course "Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems" offered by the "Scuola di Dottorato di Ricerca" of the Politecnico di Milano, 6th Edition, **2015**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).
  - Four-hour lecture and three-hour tutorial titled "Uncertainty modeling", held during the 3rd

PhD School on “Vulnerability, risk and resilience of complex system”, organized by Ecole Centrale Paris (Chatenay-Malabry, France), Politecnico di Milano (Milano, Italy) and Supélec (Gif-Sur-Yvette, France), 13-17 October **2014**, Supélec, Gif-Sur-Yvette, France. Total activity: lectures (4hrs), tutorials (3hrs).

- Four-hour lecture and three-hour tutorial titled “Uncertainty modeling”, held during the 2nd PhD School on “Risk and uncertainty modelling”, organized by Ecole Centrale Paris (Chatenay-Malabry, France), Politecnico di Milano (Milano, Italy) and Supélec (Gif-Sur-Yvette, France), 2-8 September **2013**, Palazzo Natta, Como, Italy. Total activity: lectures (4hrs), tutorials (3hrs).
- Two-hour “tutorial” lecture titled “Bootstrapped Artificial Neural Networks for Uncertainty and Sensitivity Analysis in Probabilistic Risk Assessment”, held during Course 22.38 “Probability and its Application to Reliability, Quality Control, and Risk Assessment” by Prof. Apostolakis, included in the Ph.D. Course in “Nuclear Science and Engineering” of the Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts (USA), **2009**. Total activity: lectures (2hrs).
- Four-hour lecture titled “Advanced Monte Carlo simulation methods: Markov Chain Monte Carlo, Subset Sampling, Line Sampling, and applications to reliability analysis”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 5th Edition, January-February **2014**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).
- Four-hour lecture titled “Efficient Methods of Sampling Uncertain Variables: Subset and Line Sampling”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 4th Edition, September-October **2012**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).
- Two-hour lecture titled “Markov Chain Monte Carlo for model and parameter identification”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 3rd Edition, September 15-October 28 **2011**, Politecnico di Milano (Milano, Italy). Total activity: lectures (2hrs).
- Four-hour lecture titled “Efficient Methods of Sampling Uncertain Variables: Subset and Line Sampling”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 3rd Edition, September 15-October 28 **2011**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).
- Two-hour lecture titled “Markov Chain Monte Carlo for model and parameter identification”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 2nd Edition, September 15-October 20 **2010**, Politecnico di Milano (Milano, Italy). Total activity: lectures (2hrs).
- Four-hour lecture titled “Efficient Methods of Sampling Uncertain Variables: Subset and Line Sampling”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 2nd Edition, September 15-October 20 **2010**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).
- Three-hour lecture titled “Markov Chain Monte Carlo for model and parameter identification”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 1st Edition, 18 September-21 October **2009**, Politecnico di Milano (Milano, Italy). Total activity: lectures (3hrs).

- Four-hour lecture titled “Efficient Methods of Sampling Uncertain Variables: Subset and Line Sampling”, held during the Multidisciplinary course “Monte Carlo Simulation Methods for the Quantitative Analysis of Stochastic and Uncertain Systems” offered by the “Scuola di Dottorato di Ricerca” of the Politecnico di Milano, 1st Edition, 18 September-21 October **2009**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).

- **Lectures held during Graduation (Bachelor and Master) courses (Lectures = 27hrs; Exercise sessions = 7hrs; Tutorials = 0hrs; Exams = 0hrs)**
  - Three-hour lecture titled “Markov Models for Reliability and Availability Analysis”, held during the course “Risk Management” of the international Master in “Nuclear Energy” organized by a consortium of several academic institutions (Universitè Paris-Sud 11, ParisTech, Ecole Centrale Paris and Supelec and CEA-INSTN) with the support of several industrial establishments (EDF, Areva, GDF SUEZ), CEA-INSTN (Saclay, France), **2014**. Total activity: lectures (3hrs).
  - Three-hour lecture titled “Markov Models for Reliability and Availability Analysis”, held during the course “Risk Management” of the international Master in “Nuclear Energy” organized by a consortium of several academic institutions (Universitè Paris-Sud 11, ParisTech, Ecole Centrale Paris and Supelec and CEA-INSTN) with the support of several industrial establishments (EDF, Areva, GDF SUEZ), CEA-INSTN (Saclay, France), **2013**. Total activity: lectures (3hrs).
  - Three-hour lecture titled “Markov Models for Reliability and Availability Analysis”, held during the course “Risk Management” of the international Master in “Nuclear Energy” organized by a consortium of several academic institutions (Universitè Paris-Sud 11, ParisTech, Ecole Centrale Paris and Supelec and CEA-INSTN) with the support of several industrial establishments (EDF, Areva, GDF SUEZ), CEA-INSTN (Saclay, France), **2012**. Total activity: lectures (3hrs).
  - Three-hour exercise session titled “Markov Reliability and Availability Analysis”, held during the course “Reliability, Safety and Risk Analysis A+B” of the Second Level graduation course in Nuclear Engineering, Environmental Engineering, Mathematical Engineering and Safety Engineering, Politecnico di Milano (Milano, Italy), **2012**. Total activity: exercise sessions (3hrs).
  - Four-hour lecture titled “Uncertainty and Sensitivity Analysis”, held during the course “Reliability, Safety and Risk Analysis A+B” of the Second Level graduation course in Nuclear Engineering, Environmental Engineering, Mathematical Engineering and Safety Engineering, Politecnico di Milano (Milano, Italy), **2012**. Total activity: lectures (4hrs).
  - Five-hour lecture titled “Markov Reliability and Availability Analysis”, held during the course “Reliability, Safety and Risk Analysis A+B” of the Second Level graduation course in Nuclear Engineering, Environmental Engineering, Mathematical Engineering and Safety Engineering, Politecnico di Milano (Milano, Italy), **2012**. Total activity: lectures (5hrs).
  - One-hour lecture titled “Subset Simulation for the Safety Assessment of Radioactive Waste Repositories”, held during the course “Safety Assessment of Radioactive Waste Repositories” of the Second Level graduation course in Nuclear Engineering, Politecnico di Milano (Milano, Italy), **2012**. Total activity: lectures (1hr).
  - Two-hour lecture titled “Uncertainty and Sensitivity Analysis”, held during the course “Safety Assessment of Radioactive Waste Repositories” of the Second Level graduation course in Nuclear Engineering, Politecnico di Milano (Milano, Italy), **2012**. Total activity: lectures (2hrs).
  - Two-hour lecture titled "Multi-objective Genetic Algorithms", held during the course “Nuclear Power Plants Operation and Maintenance” of the Second Level graduation course in Nuclear Engineering, Politecnico di Milano (Milano, Italy), **2012**. Total activity: lectures (2hrs).

- Four-hour lecture titled “Uncertainty and Sensitivity Analysis”, held during the course “Computational Methods for Reliability and Risk Analysis I+II” of the Second Level graduation course in Nuclear Engineering, Environmental Engineering and Safety Engineering, Politecnico di Milano (Milano, Italy), **2011**. Total activity: lectures (4hrs).
- Four-hour exercise session titled “Markov Reliability and Availability Analysis”, held during the course “Computational Methods for Reliability and Risk Analysis I+II” of the Second Level graduation course in Nuclear Engineering, Environmental Engineering and Safety Engineering, Politecnico di Milano (Milano, Italy), **2011**. Total activity: exercise sessions (4hrs).

- **Lectures held during professional training courses (Lectures = 12hrs; Exercise sessions = 12hrs; Tutorials = 0hrs; Exams = 0hrs)**
  - Four-hour exercise session titled “Genetic Algorithms optimization”, held during the Professional Training Course “Advanced methods for the reliability and availability analyses, safety, maintenance, diagnostics and prognostics of industrial systems and plants”, 14th Edition, 26-29 September **2011**, Politecnico di Milano (Milano, Italy). Total activity: exercise sessions (4hrs).
  - Two-hour lecture titled “Advanced methods of Monte Carlo simulation for the estimation of small failure probabilities”, held during the Professional Training Course “Advanced methods for the reliability and availability analyses, safety, maintenance, diagnostics and prognostics of industrial systems and plants”, 14th Edition, 26-29 September **2011**, Politecnico di Milano (Milano, Italy). Total activity: lectures (2hrs).
  - Eight-hour exercise session titled “Reliability and Availability of Simple Systems” held during the Professional Training Course “Reliability, Availability and Maintainability with Application in the Development Phases for Oil & Gas Upstream Projects”, 13-17 June **2011**, ENI Corporate University, Milano (Italy). Total activity: exercise sessions (8hrs).
  - Four-hour lecture titled “Genetic Algorithms with application to the optimization of system redundancy and maintenance”, held during the Professional Training Course “Advanced methods for the reliability and availability analyses, safety, maintenance, diagnostics and prognostics of industrial systems and plants”, 13th Edition, 20-23 September **2010**, Politecnico di Milano (Milano, Italy). Total activity: lectures (4hrs).
  - Two-hour lecture titled “Advanced Monte Carlo Simulation Methods”, held during the Professional Training Course “Advanced methods for the reliability and availability analyses, safety, maintenance, diagnostics and prognostics of industrial systems and plants”, 13th Edition, 20-23 September **2010**, Politecnico di Milano (Milano, Italy). Total activity: lectures (2hrs).
  - Two-hour lecture titled “Advanced Monte Carlo Simulation Methods”, held during the Professional Training Course “Innovative techniques for the evaluation of the reliability, availability, maintenance and diagnostics of industrial systems and plants”, 12th Edition, 21-24 September **2009**, Politecnico di Milano (Milano, Italy). Total activity: lectures (2hrs).
  - Two-hour lecture titled “Recurrent Neural Networks”, held during the Professional Training Course “Innovative techniques for the evaluation of the reliability, availability, maintenance and diagnostics of industrial systems and plants”, 12th Edition, 21-24 September **2009**, Politecnico di Milano. Total activity: lectures (2hrs).

	Categories of courses and students (institution/course)		
Years	**Bachelor/Master Courses**	**PhD Courses**	**Professional Training Courses**
2007			- Recurrent Neural Networks (Polimi)
2009		- Bootstrapped Artificial Neural Networks (MIT) - Advanced Monte Carlo simulation methods (Polimi) - Markov Chain Monte Carlo for model and parameter identification (Polimi)	- Recurrent Neural Networks (Polimi) - Advanced Monte Carlo simulation methods (Polimi)
2010		- Advanced Monte Carlo simulation methods (Polimi) - Markov Chain Monte Carlo for model and parameter identification (Polimi)	- Advanced Monte Carlo simulation methods (Polimi) - Genetic algorithms for reliability optimization (Polimi)
2011	- Markov Reliability and Availability Analysis (Polimi) - Uncertainty and sensitivity analysis (Polimi)	- Advanced Monte Carlo simulation methods (Polimi) - Markov Chain Monte Carlo for model and parameter identification (Polimi)	- Advanced Monte Carlo simulation methods (Polimi) - Genetic algorithms for reliability optimization (Polimi) - Reliability and Availability of Simple Systems: probability models (ENI Corporate University)
2012	- Nuclear Thermohydraulics (Master Nuclear Energy - MNE): • Thermal design principles • Thermodynamic cycles for nuclear reactors • Thermal analysis of fuel elements - Markov Reliability and Availability Analysis (MNE) - Uncertainty and sensitivity analysis (Polimi) - Multi-Objective Genetic algorithms (Polimi) - Advanced Monte Carlo Simulation methods (Polimi)	- Advanced Monte Carlo simulation methods (Polimi)	
2013	- Nuclear Thermohydraulics (MNE, Paris) (see details of the lectures above) - Markov Reliability and Availability Analysis (MNE)	- Uncertainty modeling (international PhD course)	
2014	- Nuclear Thermohydraulics (MNE, Paris) (see details of the lectures above) - Markov Reliability and Availability Analysis (MNE)	- Uncertainty modeling (international PhD course) - Advanced Monte Carlo simulation methods (Polimi)	
2015	- Nuclear Thermohydraulics (MNE, Paris) (see details of the lectures above) - Managing Uncertainty For Reliability Optimization (Master Recherche ECP, Paris): • Uncertainty in risk assessment • Uncertainty representation methods • Uncertainty propagation methods	- Uncertainty modeling (international PhD course) - Advanced Monte Carlo simulation methods (Polimi)	

Table 1. Summary of the main teaching activities and content of the lectures

3.2 Administrative activities

(Présentation synthétique des activités d'administration)

Relevant administrative responsibilities are the following:

- Member of the organizing committee of the 4th PhD School on "Vulnerability, risk and resilience of complex system and critical infrastructures", organized by École CentraleSupélec (Chatenay-Malabry, France) and Politecnico di Milano (Milano, Italy), 14-18 September **2015**, CentraleSupélec, Chatenay-Malabry, France.
- Member of the Board of Laboratory of LGI, from **2015**.
- Thesis Jury Member: International Master in Nuclear Energy (MNE), Specialty Operations, **2015**. The MNE is run by a consortium of several academic institutions (Universitè Paris-Sud 11, ParisTech, Ecole Centrale Paris and Supelec and CEA-INSTN) with the support of several industrial establishments (EDF, Areva, GDF SUEZ), CEA-INSTN (Saclay, France).
- Member of the evaluation committee of the exam projects of the course "Introduction to complex systems" (by Prof. E. Zio) of the Master "Genie Industriel (GI)", Master Recherche "Optimisation des Systèmes Industriels et Logistiques (OSIL)" and Master Recherche "Modélisation et Management de la Conception" (MoMaC), held at Ecole Centrale Paris (ECP), Chatenay-Malabry, France, **January 2015-March 2015**.
- Member of the evaluation committee of the exam projects of the course "Risk Management" (by Prof. E. Zio and Prof. M. Bouissou) of the Master "Genie Industriel (GI)", held at Ecole Centrale Paris (ECP), Chatenay-Malabry, France, **2013**.

4 Synthetic presentation of the research activities

(Présentation synthétique des activités de recherche)

In this Section, a *synthetic* presentation of my research activity is given: in particular, in Section 4.1, the main technical and scientific issues addressed during my research are briefly outlined; in Section 4.2, some statistics related to my publications are summarized; Section 4.3 contains the list of PhD and Master students co-directed, together with a brief description of their corresponding thesis works; Section 4.4 synthetically proposes medium- and long-term plans for future research; Section 4.5 describes the capitalization of my research in the form of participation to research projects at both national and international levels; finally, Section 4.6 reports a detailed list of technical activities that have been carried out during my academic career and that represent my 'scientific outreach'. For a *thorough*, *detailed* description of my overall research activity the reader is instead referred to Section 6.

4.1 Overview on the research activities

(Bilan des activités de recherche)

My research is focused on the study and development of advanced *models* and *methods* for the *risk, vulnerability* and *resilience assessment* of *complex*, *safety-critical engineering components*, *systems* and *infrastructures* (i.e., including industrial installations – such as nuclear and chemical plants – and critical infrastructures – such as civil, transportation, electric power, water, gas and communication systems), in the presence of *uncertainties*. In this respect, it is worth reminding that the concept of *risk* classically refers to the *probability of occurrence* (frequency) of a specific (mostly undesired/adverse) event leading to loss, damage or injury, and its *extent*. On the other hand, *vulnerability* can be defined as the system *inability* to withstand and "resist" to *strains* and *stresses* and it may be exploited by some perhaps unknown or previously unimagined threats and hazards (component failures, natural and men-made hazards). Finally, *resilience* quantifies the system *ability* to *reduce* the chances of shock, to *adsorb* a shock if it occurs and to *recover* quickly after a shock.

The motivation of my research is the acknowledgement that these subjects nowadays play a relevant role in the design, development, operation and management of components, systems and infrastructures in many types of industry. This is particularly true for civil, nuclear, aerospace and chemical systems that are *safety-critical* and must thus be designed and operated within a quantitative risk-informed approach aimed at systematically integrating deterministic and probabilistic analyses to obtain a rational *decision* on the utilization of resources for *protecting* the systems of interest (possibly from different types of hazards), for reducing their vulnerability and improving their safety and resilience.

A number of models and methods have been developed to these aims. Yet, new challenges emerge from the latest technological systems or the ongoing projects, such as the smart grids, mainly characterized by the complex and possibly intelligent behaviors of the components and the hybrid uncertainties embedded in the available modeling information. Actually, in general safety-critical industrial installations and infrastructures are *complex* systems composed by a *multitude* and *variety* of 'elements', that is, physical hard components (e.g., road, railway, pipelines, pumps, etc.), soft components (e.g., Supervisory Control And Data Acquisition-SCADA, information and telecommunication systems) and human and organizational components. They are highly *interconnected* and mutually *dependent* in complex ways, so that a failure in one critical system or infrastructure can propagate to the others, possibly provoking (*cascading*) *failures* that generate *large consequences* well beyond the initial impact zone. In addition, such failures may be triggered by *multiple* and *various* sources of *hazards* due to exogenous and endogenous stressors, like natural events, terrorism, criminal activities, malicious behavior, market and policy factors, human factors

and technical random failures of hard components. Finally, such systems are affected by large *uncertainties* in the characterization of the failure and recovery behavior of their components, their interconnections and interactions: this makes the corresponding analysis a challenging task, because it requires to quantify the uncertainty and to predict how it propagates throughout the system.
Developing new methods to confront these challenges is the goal of this thesis. With respect to that, my research works are grouped under two main axes: the first deals with the study of approaches for the *modeling* and *quantification* of *uncertainty* in the reliability analysis and risk assessment of safety-critical components and systems; the second focuses on the development of *advanced computational methods* for the modeling, simulation and analysis of safety-critical systems and infrastructures in the presence of uncertainties.

Axis 1 – Reliability Analysis And Risk Assessment Of Safety-Critical Components And Systems: Uncertainty Modeling And Quantification

- Summary: the research work in this axis is mainly focused on the modeling, quantitative treatment and analysis of uncertainties in the reliability analysis and risk assessment of safety-critical systems and components (in particular, for energy production and safety). Four main issues are treated under this axis:
    1. The first issue concerns the *representation* of uncertainty in reliability analysis and risk assessment, coherent with the information and data available. In the corresponding research works, *probability* theory has been typically used to represent *aleatory* uncertainty, related to randomness due to inherent variability in the system behavior. On the contrary, *alternative* (*non-fully probabilistic*) approaches (e.g., Fuzzy, Possibility, Evidence Theories, etc.) have been employed for representing and describing *epistemic* uncertainties, due to lack of knowledge. The relevant studies [6, 7, 38, 68, 69, 70] include the PhD works of Elisa Ferrario and Chung-Kung Lo.
    2. The second issue is about the quantification of the uncertainty in the *outcomes* of a reliability analysis or risk assessment: this is obtained by *propagation* of the uncertainty in the input and parameters of the respective *physical-mathematical models* describing the safety-critical components and systems of interest. In the corresponding research works, efficient methods have been developed and applied for the *joint* propagation of *hybrid* aleatory and epistemic uncertainties, represented by both probabilistic and non-probabilistic approaches, respectively. The relevant studies [3, 6, 7, 9, 10, 38, 50, 53, 54, 66, 67] include the PhD works of Elisa Ferrario and Chung-Kung Lo.
    3. The third issue is about the modeling of *dependences* between uncertain variables and parameters. In the corresponding research works, different methods have been employed to model *all* types of (possibly *unknown*) dependences between uncertain variables, parameters and events. The relevant studies [3, 7, 9, 10, 39] include the PhD works of Elisa Ferrario.
    4. The fourth issue concerns the *updating* of the uncertainty representation as *new information* and *data* become available. In the corresponding research works, techniques for updating in a 'Bayesian' framework also the (epistemic) uncertainty described by *non-fully probabilistic* approaches have been considered and their effectiveness has been compared. The relevant studies [3, 6, 38, 39, 51, 52] include the PhD works of Chung-Kung Lo.
- Publications: international journal papers [3, 6, 7, 9, 10, 38, 39]; international conference proceedings [50-54]; international technical reports [66-70].
- Students: *PhDs* Elisa Ferrario, Chung-Kung Lo (at CentraleSupélec); *Masters* Elisa Ferrario (at Politecnico di Milano).

Axis 2 – Safety-Critical Systems And Infrastructures: Advanced Methods For Modeling, Simulation and Analysis Considering Uncertainties

- Summary: the research work in this axis is mainly focused on the study and development of advanced computational methods for the efficient modeling, simulation and analysis of safety-critical systems and infrastructures, in the presence of uncertainties. There are three research issues under this axis:
    1. The first issue concerns the development of innovative methods of *representation* and *simulation* of critical infrastructures (in particular, for energy production and transmission), for the analysis of their vulnerability and resilience characteristics. In the corresponding research works, the following activities have been carried out: (a) *representation* of the real system to capture its *main features* and the *logical connections* between the components and the subsystems, and to provide a *picture* of the information needed to answer relevant questions; (b) *modeling* the propagation of (*cascading*) *failures* in the critical systems and infrastructures of interest; (c) *optimizing* some characteristics of such critical systems and infrastructures (e.g., their topology and components capacities) in order to make them *less vulnerable* to natural external events and/or malevolent intentional attacks; (d) identifying *optimal strategies* for the *timely recovery* of the critical infrastructure performance after a cascading failure or a disruptive event (technically speaking, for increasing their *resilience*). The relevant studies are the PhD works of Elisa Ferrario and Yi-Ping Fang [1, 2, 5, 34, 36, 37, 47-49].
    2. The second issue is about designing and implementing innovative *algorithms* for the *efficient* risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures (in particular, for energy production and/or transmission). These algorithms can be grouped into two classes. The first class comprises advanced methods of Monte Carlo Simulation (MCS) of stochastic degradation, failure and repair processes, and of Monte Carlo sampling for quantitative uncertainty analysis (e.g., Subset Simulation, Importance Sampling, etc.). Such techniques allow *robust* risk and/or reliability estimations with a *limited* number of system model simulations (and associated *low* computational cost). The relevant studies [11, 13-15, 19, 21, 24, 29, 30, 35, 40, 45, 46, 55, 57, 59, 60] include the PhD works of Pietro Turati. The second class comprises surrogate models (also called meta-models, like artificial neural networks, response surfaces, etc.) for regression and prediction of the physical processes of interest for the specific risk assessment and reliability analysis. Such techniques allow *approximating* the *response* of the original (typically long-running) system model in a very *limited computational time*. The relevant studies [12, 14, 16-18, 20, 25-27, 41, 42, 44, 56, 58, 61-64] include the Master works of Lucia R. Golea.
    3. The third research issue regards the development of innovative *decision making* approaches for the (*multi-criteria*) vulnerability analysis of safety-critical systems and infrastructures under uncertainty. In more detail, an *optimization-based* framework has been undertaken in order to find one or more *sets* of *protective actions*, such that the *overall* vulnerability level (or class) of a *group* of safety-critical systems or infrastructures of interest is *minimized* under given *constraints*. The relevant studies are the PhD works of Tai-Ran Wang [4, 31-33].
- Publications: international journal papers [1, 2, 4, 5, 11-21, 24-27, 29-37]; book chapters [40-42]; international conference proceedings [44-49, 55-64].
- Students: *PhDs* Elisa Ferrario, Yi-Ping Fang, Tai-Ran Wang, Pietro Turati (at CentraleSupélec); *Masters* Lucia Roxana Golea (at Politecnico di Milano).

4.2 Publications statistics

(Statistiques concernant les publications)

Number of classified publications

	Before 2008	2008	2009	2010	2011	2012	2013	2014	2015 or in press	Under review/revision
Journal papers	2	2	7	3	1	4	3	1	5	11
Book Chapters		2	1	1						
Conference proceedings	3	2	1	5		2		6	3	
Technical reports						2	2	1		

Table 2. Number of classified publications

H-index of the Author ID 14049106600 on Scopus: 11
H-index on ISI Web of Science: 9
H-index on Google Scholar: 12 (http://scholar.google.it/citations?user=YRRNEzAAAAAJ&hl=it)

List of the main journals where my publications appear

- Reliability Engineering and System Safety (IF=2.410; JCR quartile Q1 in 2014)
- Risk Analysis, an International Journal (IF=2.502; JCR quartile Q1 in 2014)
- Computers and Structures (IF=2.134; JCR quartile Q1 in 2014)
- IEEE Systems Journal (IF=1.980; JCR quartile Q1 in 2014)
- IEEE Transactions on Nuclear Science (IF=1.283; JCR quartile Q1 in Nuclear Science and Technology and JCR quartile Q2 in Electrical and Electronic Engineering in 2014)
- IEEE Transactions on Power Systems (IF=2.814; JCR quartile Q1 in 2014)
- International Journal of Intelligent Systems (IF=1.886; JCR quartile Q2 in 2014)
- Progress in Nuclear Energy (IF=1.119; JCR quartile Q2 in 2014)

Representative papers

- E. Zio, N. Pedroni, "Estimation of the Functional Failure Probability of a Thermal-Hydraulic Passive System by Subset Simulation", *Nuclear Engineering and Design*, Volume 239, Issue 3, Mar. 2009, pp. 580-599, ISSN 0029-5493, published by Elsevier Ltd (Web of Science citations = 36, Scopus citations = 51, Google Scholar citations = 53).
- N. Pedroni, E. Zio, "Uncertainty analysis in fault tree models with dependent basic events", *Risk Analysis, an International Journal*, Vol. 33, Issue 6, 2013, pp. 1146–1173, ISSN 0272-4332, published by Wiley-Blackwell (Web of Science citations = 1, Scopus citations = 2, Google Scholar citations = 3).
- N. Pedroni, E. Zio, E. Ferrario, A. Pasanisi, M. Couplet, "Hierarchical propagation of probabilistic and non-probabilistic uncertainty in the parameters of a risk model", *Computers and Structures* (*Special Issue on Uncertainty Quantification in Structural Analysis and Design*), Vol. 126, Sept. 2013, pp. 199–213, ISSN 0045-7949, published by Elsevier Ltd (Web of Science citations = 3, Scopus citations = 6, Google Scholar citations = 7).
- Y.-P. Fang, N. Pedroni, E. Zio, "Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network",

IEEE Systems Journal, 2015, doi: 10.1109/JSYST.2014.2352152, ISSN 1932-8184, published by IEEE Systems Council, Institute of Electrical and Electronics Engineers.

Analysis of the main co-authors

Most research works are done through collaborations with SSEC researchers, external researchers, and students (including PhD students and master students) as shown in the following Table 3. The percentages are computed based on the 70 works on international journals, conference proceedings, book chapters and works published as reports of international research institutes. This presentation also shows the names of the main co-authors.

SSEC Researchers		**External researchers**		**Students**	
E. Zio	100%	F. Cadini (Polimi)	11.43%	***PhD***	
Y. Li	1.43%	A. Pasanisi (EdF)	8.57%	Y.-P. Fang (SSEC)	8.57%
E. Ferrario (Post-doc)	1.43%	M. Couplet (EdF)	8.57%	T.-R. Wang (SSEC)	5.71%
		P. Baraldi (Polimi)	8.57%	E. Ferrario (SSEC)	4.30%
		M. Broggi (University Liverpool)	7.14%	P. Turati (SSEC)	4.29%
		G.E. Apostolakis (MIT)	5.71%	C.-K. Lo (SSEC)	2.86%
		V. Mousseau (CentraleSupélec)	4.29%	***Master***	
		G. Gola (Polimi)	1.43%	L.R. Golea (Polimi)	7.14%
		G. Sansavini (ETHZ)	1.43%	E. Ferrario (Polimi)	5.71%
		D. Avram (Polimi)	1.43%		

Table 3. Analysis of the research collaborators

4.3 List of PhD and Master students co-directed

(Liste des masters encadrés et thèses codirigées)

This Section contains the list of PhD and Master students co-directed, together with a brief description of their corresponding thesis works and of the research output produced (in terms of published papers).

PhD Students

1. Elisa FERRARIO: **50%** *"System-of-systems modeling and simulation for the risk analysis of industrial installations and critical infrastructures"*, thesis of École Centrale Paris, defended on 10 September **2014**, supervisors: Nicola PEDRONI, Enrico ZIO. Now post-doctoral fellow at CentraleSupélec, Laboratoire Génie Industriel (LGI).
   - Main contributions and results: This thesis addresses the risk analysis of industrial installations and Critical Infrastructures (CIs) within a System-of-Systems (SoS) framework. A SoS consists of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels that evolve over time. System representation, modeling and simulation methods are developed to capture the peculiar features of SoS, with respect to their vulnerability and physical resilience to random failures and natural hazards. Several representation techniques of literature, i.e., Fault Tree, Muir Web, Hierarchical Modeling, Goal Tree Success Tree – Dynamic Master Logic Diagram, are explored and originally extended/tailored to fit the purpose of SoS analysis. One representation method is developed ex-novo, namely the Hierarchical Graph. Within these representation frameworks, binary and multiple states are used to model the performances of the SoS under analysis. Monte Carlo simulation and interval analysis are combined for the quantitative evaluation of the SoS models in presence of uncertainty (due to both randomness and lack of knowledge). Examples of analyses are carried out within two application areas: external event risk assessment and vulnerability of CIs. In particular, the first application deals with the safety and the physical resilience of a critical plant (i.e., a nuclear power plant) exposed to the risk of natural events (i.e., earthquakes and aftershocks). The second application considers the robustness and the recovery capacity of interdependent CIs (i.e., gas and electricity networks and a SCADA system).
   - Research outputs: 4 journal papers and 1 conference proceedings have been published and 1 journal paper is currently under review.
   - Jury for the thesis defense: Terje AVEN, Frank GUARNIERI, Mohamed HIBTI, Alois J. SIEBER, Enrico ZIO.

2. Yi-Ping FANG: **50%** *"Critical Infrastructure Protection by Advanced Modelling, Analysis and Optimization for Cascading Failure Mitigation and Resilience"*, thesis of CentraleSupélec, defended on 2 February **2015**, supervisors: Nicola PEDRONI, Enrico ZIO. Now post-doctoral fellow at ETH Zurich, Laboratory of Reliability and Risk Engineering, Institute of Energy Technology at the Department of Mechanical and Process Engineering (D-MAVT).
   - Main contributions and results: The focus of this thesis is on the modelling, simulation and optimization of Critical Infrastructures (CIs) (e.g., power transmission networks) with respect to their vulnerability and resilience to cascading failures. This study approaches the problem by firstly modelling CIs at a

fundamental level, by focusing on network topology and physical flow patterns within the CIs. A hierarchical network modelling technique is introduced for the management of system complexity. Within these modelling frameworks, advanced optimization techniques (e.g., the Non-dominated Sorting Binary Differential Evolution – NSBDE – algorithm) are utilized to maximize both the robustness and resilience (recovery capacity) of CIs against cascading failures. Specifically, the first problem is taken from a holistic system design perspective, i.e., some system properties, such as its topology and link capacity, are redesigned in an optimal way in order to enhance system's capacity of resisting to systemic failures. Both topological and physical cascading failure models (namely, the Motter-Lai and the ORNL-Pserc-Alaska models, respectively) are applied and their corresponding results are compared. With respect to the second problem, a novel framework is proposed for optimally selecting proper actions in order to maximize the capacity of the CI network to recover from a disruptive event. A heuristic, computationally cheap optimization algorithm is proposed for the solution of the problem, by integrating fundamental concepts from network flows and project scheduling. Examples of analysis are carried out by referring to several realistic CI systems, including the 380kV Italian Power Transmission Network (IPTN380), the 400kV French Power Transmission Network (FPTN400) and the IEEE 30 Bus test network.

- Research outputs: 4 journal papers and 2 conference proceedings have been published and 2 journal papers are currently under review.
- Jury for the thesis defense: Roberto SETOLA, Giovanni SANSAVINI, Stephane ANDRIEUX, Georgios GIANNOPOULOS, Enrico ZIO.

3. Tai-Ran WANG: **30%** *"Decision making and modeling uncertainty for the multi-criteria analysis of complex energy systems"*, thesis of CentraleSupélec, defended on 8 July **2015**, supervisors: Nicola PEDRONI, Vincent MOUSSEAU, Enrico ZIO.
   - Main contributions and results: This work addresses the vulnerability analysis of safety-critical systems (e.g., nuclear power plants) within a framework that combines the disciplines of risk analysis and multi-criteria decision-making. The scientific contribution follows four directions: (i) a quantitative hierarchical model is developed to characterize the susceptibility of safety-critical systems to multiple types of hazard, within the needed 'all-hazard' view of the problem currently emerging in the risk analysis field; (ii) the quantitative assessment of vulnerability is tackled by an empirical classification framework: to this aim, a model, relying on the Majority Rule Sorting (MR-Sort) Method, typically used in the decision analysis field, is built on the basis of a (limited-size) set of data representing (a priori known) vulnerability classification examples; (iii) three different approaches (namely, a model-retrieval-based method, the Bootstrap method and the leave-one-out cross-validation technique) are developed and applied to provide a quantitative assessment of the performance of the classification model (in terms of accuracy and confidence in the assignments), accounting for the uncertainty introduced into the analysis by the empirical construction of the vulnerability model; (iv) on the basis of the models developed, an inverse classification problem is solved to identify a set of protective actions which effectively reduce the level of vulnerability of the critical system under consideration. Two approaches are developed to this aim: the former is based on a novel sensitivity indicator, the latter on optimization. Applications on fictitious and real case studies in the nuclear power plant risk field demonstrate the effectiveness of the proposed methodology.
   - Research outputs: 1 journal paper and 1 conference proceeding have been published and 3 journal papers are currently under review.

- Jury for the thesis defense: Ahti SALO, Vytis KOPUSTINSKAS, François BEAUDOUIN, Maria Francesca MILAZZO, Enrico ZIO, Vincent MOUSSEAU.

4. Chung-Kung LO: **10%** *"Methods for accounting of uncertainties in system analysis and decision making"*, thesis of CentraleSupélec, defense expected by the end of **2015**, supervisors: Nicola PEDRONI, Enrico ZIO.
   - Main contributions and results: The objective of this work is to establish a systematic approach to deal with uncertainties in the Seismic Probabilistic Risk Assessment (SPRA) of Nuclear Power Plants (NPPs) in order to provide more robust information and to improve the decision making practice. Actually, SPRA analyses are affected by significant aleatory and epistemic uncertainties. These uncertainties have to be represented and quantified coherently with the data, information and knowledge available, to provide reasonable assurance that related decisions can be taken robustly and with confidence. The amount of data, information and knowledge available for seismic risk assessment is typically limited, so that the analysis must strongly rely on expert judgments. In this thesis, several non-probabilistic techniques for handling uncertainties (e.g., Dempster-Shafer Theory of Evidence-DSTE, possibility theory and probability boxes) are considered and applied to exemplary case studies of NPP SPRAs. The main contributions of this work are two: (i) developing a complete, unitary and systematic framework of uncertainty treatment and applying it to SPRA models, showing how to describe the uncertain parameters based on industry generic data; (ii) embedding Bayesian updating based on plant specific data into the framework. The results of the application to realistic case studies show that the approach is feasible and effective in: (i) describing and jointly propagating aleatory and epistemic uncertainties in SPRA models; and (ii) providing 'conservative' bounds on the safety quantities typically of interest to NPP SPRAs (e.g., the Core Damage Frequency): such bounds reflect the (limited) state of knowledge of the experts about the system analyzed.
   - Research outputs so far: 1 journal paper and 1 conference proceeding have been published.

5. Pietro TURATI: **50%** *"Advanced computational methods for uncertainty/sensitivity analysis and risk assessment in complex system"*, thesis of CentraleSupélec, defense expected in February **2017**, supervisors: Nicola PEDRONI, Enrico ZIO.
   - Main contributions and results: The main objective of this thesis is to develop advanced simulation techniques for the efficient exploration of extreme and unexpected events in the risk assessment of complex, dynamic engineered systems. Actually, the end states reached by a dynamic engineered system as outcomes of an accident scenario depend not only on the sequences of the events (i.e., on the scenario), but also on the exact timing and magnitudes of the failures. Including these additional features can make the analysis infeasible, due to the high dimension of the system state-space and the corresponding computational effort needed to simulate all possible system evolutions. In this thesis, we address the problem of efficiently probing the space of event sequences of a dynamic system by a means of "smart" and guided exploration techniques. In particular, the proposed approaches (mainly based on the concept of entropy, taken from information theory) are able to adaptively and intelligently allocate the simulation efforts preferably on those time sequences leading to "interesting" outcomes, e.g., on those that are more safety-critical and/or rare. The resulting diversification in the precision of the state-space exploration supports the retrieval of critical system features, which can aid analysts and designers to prevent and mitigate dangerous and/or unexpected consequences.

- Research outputs so far: 1 conference proceeding has been published and 2 journal papers are currently under review.

Master Students

1. Elisa FERRARIO: **100%** *"Uncertainty Analysis in Risk Assessment for Environmental Applications"*, final thesis for the Master in Environmental Engineering at Politecnico di Milano (Milano, Italy), defended in April **2011** (score: 110/110 cum laude), supervisor: Nicola PEDRONI, co-supervisors: Enrico ZIO, Alberto PASANISI.
   - Main contributions and results: Environmental risk assessment is an essential part of any decision-making process because it allows evaluating all potential risks associated with human activities that may cause environmental damage. However, environmental risk assessment studies are affected by significant aleatory and epistemic uncertainties. In the present thesis, the important issues of representation and propagation of uncertainties in environmental risk assessment applications have been addressed, by way of a model for the risk-based design of a flood protection dike. Different methods of joint propagation of aleatory and epistemic uncertainties have been embraced depending on the different frameworks adopted for uncertainty modeling and epistemic uncertainty representation. Two uncertainty model frameworks have been analyzed: in the first one a mixture of purely aleatory and purely epistemic uncertainties is considered ("level-1" setting); in the second one, aleatory and epistemic uncertainties are separated into two hierarchical levels ("level-2" setting). In addition, two frameworks for epistemic uncertainty representation have been adopted, i.e., probability and possibility theories. Within these frameworks, the efficiency of purely probabilistic and "hybrid" (i.e., mixed probabilistic and possibilistic) approaches has been compared in the task of jointly propagating aleatory and epistemic uncertainties, in both "level-1" and "level-2" settings. All the approaches have been tested on a case study involving the risk-based design of a flood protection dike.
   - Research outputs: 2 conference proceedings and 1 journal paper have been published.

2. Lucia Roxana GOLEA: **50%** *"Locally Recurrent Neural Networks for Nonlinear Dynamic Modelling"*, final thesis for the Master in Automatic Engineering at Politechnica University of Timisoara (Timisoara, Romania), defended in July **2007** (score: 9.72/10), supervisors: Nicola PEDRONI, Enrico ZIO.
   - Main contributions and results: The ability to model nonlinear dynamic systems has become a fundamental aspect for the safe and economically competitive operation of modern industrial systems and plants. Obviously, the knowledge of the state of a system during each instant of its operation is a fundamental feature for optimal control and safety. In practice, one wishes to get accurate estimates in real time. This entails the capability of performing fast calculations, which cannot be achieved with the large, detailed dynamic codes typically used in safety analysis, due to the long computing times involved. One has then to resort to either simplified or empirical models, whose parameters must be determined so that the model response best fits to the actual system behavior. Artificial Neural Networks (ANNs) are among the most powerful algorithms for empirical modelling. Whereas classical feedforward ANNs can model only static input/output mappings, dynamic Infinite Impulse Response Locally Recurrent Neural Networks (IIR-LRNNs) have proven capable of providing accurate approximations of the dynamic behavior of nonlinear systems. The time dependencies on the previous input values and system states are accounted for by

employing tapped-delay-lines (temporal buffers) and internal recurrence (feedback connections). In this thesis, IIR-LRNNs have been applied to two different contexts: (i) modelling the dynamics of a nuclear reactor, i.e., the Lead Bismuth Eutectic eXperimental Accelerator Driven System (LBE-XADS), under different transient conditions; (ii) forecasting failures and predicting the reliability of hardware engineered components (e.g., engine systems). The method has been compared to other empirical models, i.e., the radial basis function (RBF), the traditional ANN model and the Box-Jenkins autoregressive-integrated-moving average (ARIMA), showing its superiority.

- Research outputs: 1 conference proceeding and 2 journal papers have been published.

4.4 Synthetic presentation of future research

(Présentation synthétique de projet de recherche)

Medium- and long-term developments of my activities in the field of risk, vulnerability and resilience assessment of safety-critical engineering components, systems and infrastructures will concern both novel research *themes* (Section 4.4.1) and *methods* (Section 4.4.2). In this Section, the main issues are *synthetically* summarized: a *thorough*, *detailed* presentation is instead given in Section 7, together with the precise, synoptic *time scheduling* of the developments of these lines.

4.4.1 Research themes

My future research will be carried out around three main *themes* that are currently credited by many as among the most relevant for the analysis and management of the risk and vulnerability of complex, safety-critical systems and infrastructures:

1. Modeling and analysis of (*extreme*) *external natural events* and the corresponding quantitative assessment of the *robustness* and *resilience* of safety-critical systems and infrastructures with respect to this class of threats and hazards.
   It is a recognized fact that *extreme events* and *weather conditions* can cause natural disasters that can impact safety-critical systems (such as nuclear and chemical plants) and infrastructures (such as electric grids, energy and water supply systems, communication systems and transport routes), at the same time putting a strain on emergency and crisis response capabilities, and trigger accidents simultaneously at *several* installations. In addition, *multiple hazards* may develop at the *same time* (e.g., heavy winds and precipitation) or one hazard may trigger others (e.g., an earthquake followed by a tsunami, as in the dramatic catastrophe of Fukushima).
   Furthermore, recent studies predict that climate change will lead to more frequent and more intense natural disasters, also in areas where there are industrial facilities and infrastructures.
   In this newly arising context of extreme conditions assessment, one of the specific issues that I will address is the *seismic risk assessment* for *nuclear systems* and *components* with adequate treatment of the associated uncertainties. The goal is the quantitative assessment of the (failure) behavior of nuclear systems and components under the occurrence of a seismic event: in more detail, the response of structural systems subject to seismic risk will be studied and the structure fragility curves will be identified, representing the conditional probability of failure of a nuclear component for any given level of seismic excitation. The specific objectives of the research are the following:
   a) the study and development of robust and efficient methods to treat the available (scarce) information of different types, e.g., numerical simulations, expert judgement, real data, etc.;
   b) the quantification and efficient propagation of the (aleatory and epistemic) uncertainties through the (long-running) computer codes (i.e., Finite Element Models-FEMs) typically used to simulate the behavior of structural systems, by advanced simulation techniques and meta-models;
   c) the development of a methodology that is robust enough to be included in a general framework of seismic probabilistic risk assessment for nuclear power plants.

   This topic will be the subject of a PhD thesis in collaboration with the Électricité de France (EdF) R&D Department of "Mechanical and Acoustic Analyses" from October 2015 to October 2018.
   Another branch of this research theme will regard the probabilistic risk assessment of future *electric power systems*, exposed to natural hazards and extreme weather conditions. The research is motivated by the fact that the energy challenges faced by Europe and the rest of

the world are changing the landscape of these electric power systems. For example, originally developed as loosely interconnected networks of local systems, electric power grids have now extended on *large scales*, across regional and national boundaries. In addition, *distributed resources*, mostly in the form of small power generators based on renewable energies (such as photovoltaic panels and wind turbines), that are often geographically separated from the traditional power sources, are being increasingly connected to the existing backbone.

In this light, environmental conditions can strongly influence the operation and performance of future generation and distribution systems for several reasons. First, the growing shares of renewable-energy generators installed inject considerable amounts of *(aleatory) uncertainty* into power system operation (due to the *inherently random* nature of the corresponding natural resources). In addition, these systems employ relatively *new technologies*, and this introduces a significant amount of *(epistemic) uncertainty* (due to the limited or possibly null operating experience of the corresponding components or systems over the wide range of conditions encountered during operation). Furthermore, several *intrinsically stochastic* environment-related *contingencies* (e.g., high winds, thunderstorms, heavy snows, or even earthquake and flooding events) can damage or deeply degrade the components of the power grid. Finally, the large *spatial scale* of these *distributed* infrastructures introduces an additional important aspect to consider in the analysis: that of the *global impact* of *spatially local hazards*. Indeed, whereas the spatially local hazards threaten relatively small-scale systems whose components are located in the hazard influence area, these relatively small-scale systems are usually a part of much larger or national scale systems, and then the impact of localized natural hazards can extend to the large-scale systems they are embedded in.

In this context, we will embrace a Probabilistic Risk Assessment (PRA) framework for a systemic analysis of system-scale scenarios, and to estimate the probability (or frequency) of such scenarios of disturbance to power system operation and their consequences: these elements are the constituents of risk. As for the boundary of the analysis, the extreme events and weather conditions can also significantly affect system risk by increasing the frequency of failures of the power components and/or inducing severe damage.

In order to address these issues, I plan to put forward a *multi-level* analysis framework, based on two successive stages: (i) a "coarse" screening analysis for identifying the parts of the critical infrastructure most relevant with respect to its risk and (ii) a more detailed modeling of the operational dynamics of the identified parts for gaining insights on the causes and mechanisms responsible for the associated risk. In particular, I will evaluate the potentials of: (i) using *network analysis* based on measures of *topological interconnection* and *reliability efficiency*, for the screening task; (ii) using *object-oriented*/*agent-based* modeling as the simulation framework to capture the *detailed dynamics* of the operational scenarios involving the most vulnerable parts of the critical infrastructure as identified by the preceding network analysis.

One of the major advantages of an object-oriented approach for modeling and simulating critical infrastructures, is the possibility to include *physical laws* into the simulation and to emulate the behavior of the infrastructure as it emerges from the behaviors of the individual objects and their interactions. On the other hand, this simulation-based approach becomes highly computer intensive for complex realistic infrastructures such as the power generation and distribution systems here of interest. The challenge in this respect is to reduce the computational burden, e.g., making use of rare event simulation techniques or by substituting some objects with empirical meta-models, while quantifying the uncertainty introduced in the approximation of the empirical models (see details below).

Eventually, the problem of *optimally designing* these future power generation and distribution systems (possibly including renewable generation sources) in the face of extreme events and conditions will be also tackled in the long term.

2. Integration of the risks and vulnerabilities coming from *cyber attacks*, given that modern industrial installations and infrastructures currently rely on the massive and still increasing use of "soft components", such as Supervisory Control And Data Acquisition-SCADA, information and telecommunication systems.
   Critical infrastructures (e.g., civil, transportation, electric power, water, gas and communication systems) are getting more and more *automated*, and strongly interconnected due to their increasing extension on large scales and the progressive advances in *information technology*. For example, today's ability to run largely distributed power networks with a variety of generation technologies (e.g., nuclear, thermo, hydro, etc.) is only possible through the intense use of *information* and *communication* systems. If, on one hand, these advances and interdependences have increased their efficiency (e.g., provide better measurements, allow quicker operations, more powerful control schemes and broad access to data), on the other hand, they have created *new vulnerabilities* to component failures, natural and manmade events. The objective of the research is the development of novel methodologies for the assessment of the vulnerability of interdependent critical infrastructures (e.g., power transmission and telecommunication networks) to '*combined*' physical and cyber attacks. The main challenge will be the development of novel methods to assess and model the *interactions* between the cyber and the physical security systems to understand the *effects* of cyber technology on *overall* security system effectiveness.
   This topic will be the subject of a PhD thesis in collaboration with the Électricité de France (EdF) R&D Department of "Measures and Information Systems for Electrical Networks" and the "Research Institute for Smarter Electric Grids" (RISEGrid) from January 2017 to January 2020: the application domain will be that of '*smart grids*', i.e., power transmission networks characterized by an important use of informatics and telecommunication means.

3. Management of *multiple* risks coming from heterogeneous '*contributors*' (e.g., *different* types of *hazard*, like internal failure events, fires, cyber attacks, earthquakes, floods, etc.) and different '*locations*' (e.g., *different* power production *units* on the same site), for their *aggregate evaluation* according to different and possibly conflicting (safety-related, environmental, economical, etc.) *criteria*. It is evident how this third theme naturally "envelops" and includes also issues 1. and 2. reported above.
   Risk aggregation can be defined as the process of combining information on the risk from various: (i) 'contributors' (i.e., different types of hazard – for example, internal failure events, fires, earthquakes, etc.) and (ii) 'locations' (i.e., different power production units on the same site), in order to provide an overall characterization of risk. Traditional PRA approaches address these issues respectively as follows: (i) *mean* value contributions to the risk metrics of interest from various hazards are straightforwardly *summed*; (ii) risks from *different* units are considered *separately*, while *dependencies* and interactions between the units are introduced *a posteriori*, informally and on an 'ad-hoc' basis. On the other hand, events like the nuclear accident occurred in March 2010 at the Fukushima Daiichi plant in Japan call for new, more rigorous methods to address multi-hazard, multi-unit site risk. The challenges to the "risk aggregation process" are the following: (a) *differing levels of maturity* of the analyses used in the construction of the PRAs for the various hazard groups and for the various units; (b) *different degrees of approximations* made to facilitate the construction of the PRA models for the different hazards and sites; and (c) the *varied nature* and *magnitude* of the *uncertainties* associated with the different analyses (for example, extremely rare - possibly never observed historically - environmental conditions related only

to some particular hazard may be so uncertain to call into question any classical, probabilistic statistical analysis).
This topic will be the subject of a PhD thesis in collaboration with the Électricité de France (EdF) R&D Department of "Industrial Risk Management" from October 2015 to October 2018.

4.4.2 Research methods

In tackling themes 1.-3. described above, I will contribute to the development of mathematical models of the safety-critical systems and infrastructures of interest for the simulation of their behavior in the presence of uncertainties. In this view, the complexity of the problems and of the systems addressed calls also for further *methodological* research:

1. Novel approaches will be studied and developed that allow dealing with *uncertainties* in system models with *multiple inputs/outputs*, which are *functions* of *time* (and possibly of *space*) and show *functional dependencies* and *correlations* between each other. In this broad framework, particular attention will be devoted to the identification by *sensitivity analysis* of those (uncertain) "internal" system elements and "external" environmental contingencies that contribute the most to system risk, with the objective of properly driving resource allocation for uncertainty reduction and consequent confidence gain for design, maintenance and operation decision making.
2. In order to *reduce* the *computational effort* associated to the risk, vulnerability and resilience assessment of complex safety-critical engineering systems (e.g., in the presence of object-oriented modeling and long-running computer codes), special attention will be devoted to *surrogate modeling* (meta-modeling), with particular reference to the promising Polynomial Chaos Expansion (PCE) and Stochastic Collocation (SC) techniques. These methods expand (and approximate) the real system response as a truncated series of properly selected basis functions, "calibrated" by means of a *limited-size* set of available computer experiments. In particular, PCE surrogates the computer model with a series of orthonormal polynomials that are chosen in coherency with the probability distributions of the uncertain model input parameters. Instead, SC is a stochastic expansion method which constructs multidimensional interpolation polynomials over the system responses evaluated at a structured set of collocation points.
   In addition, further efforts will be made in the task of *intelligently probing* the space of the (undesired) event sequences of the complex, dynamic systems of interest. In particular, I plan to "complement" the research work carried out so far by developing advanced simulation techniques for *scenario analysis*, i.e., methods tailored to the "*creation*" of scenarios of potential future conditions and events of particular interest. In this case, the aim of simulation is *neither* of *completeness nor* of *accuracy* of *estimation*, as in traditional risk analysis, but rather of enabling the *generation* of "*surprising*" scenarios that may provide useful insights about what could happen. Methods of "adjoint" simulation may be of particular interest for generating deductive (anticipatory, backwards) scenarios, where we start from a future imagined event/state of the total system and question what is needed for this to occur. Interpretation of these scenarios by system thinking, to see the holes and interconnections, is critical if one has to identify "black swans".

4.5 Synthetic presentation of the capitalization and transfer activities

(Présentation synthétique des activités de valorisation et de transfert)

This Section describes the capitalization of my activity in the form of participation to research projects at both national and international levels: a synthetic presentation is given also in Table 4.

- Research project *"SINAPS@ - Earthquake and Nuclear Facilities: Ensuring and Sustaining Safety"* (€ 12.5 million), partly funded by the French National Agency for Research and coordinated by the Commissariat pour l'Energie Atomique (CEA) with the following partners: Electricite' de France (EdF), Ecole Normale Supérieure (ENS) de Cachan, CentraleSupélec, the Institute for Radiological Protection and Nuclear Safety, Laboratory Soil-Solids-Structures and Risks (Institut Polytechnique de Grenoble), Ecole Centrale de Nantes, EGIS – industry, AREVA, ISTerre, IFSTTAR and CEREMA. Years of participation: **2014-2015**.
  - Objective: One of the key aspects of the project is the quantitative assessment of the (failure) behavior of nuclear systems under the occurrence of a seismic event. In this respect, computer codes based on Finite Element Models (FEMs) are adopted for the simulation of the system structural behavior and response: an example is represented by the "Code Aster" developed by the EDF Research & Development Department of "Mechanical and Acoustic Analyses" or "Analyses Mécaniques et Acoustique" in Clamart, France. However: (i) an accurate assessment of the system failure behavior typically requires a very large number (e.g., several thousands) of FEM simulations under many different scenarios and conditions, and (ii) FEMs are computationally expensive: thus, the computational burden associated to the analysis is often impracticable. In this respect, the objective is to study and develop advanced simulation techniques that allow reducing the computing time, while producing accurate and precise failure probability estimates.
  - Role: research collaborator with Dr. Elisa Ferrario in the team of CentraleSupélec.
  - Contributions:
    a) Collaboration in the research development with respect to the study of different fast-running regression models (such as Artificial Neural Networks, quadratic response surfaces, etc.), to approximate the response of the original long-running FEMs and replace them into the seismic analysis. The bootstrap method is also employed to quantify the meta-model's error and build confidence into the analysis.
    b) Collaboration and supervision in papers and reports writing.

- Electricite' de France (EdF)-Research and Development (R&D) project (Chatou, France): *"Advanced computational methods for modelling the mechanisms of degradation in equipments of electricity production plants and uncertainty modelling and propagation"*, 40000EUR/year, Co-operation contract no. 5910059554, years of participation: January **2010**-December **2012**.
  - Objective: The purpose of the research has been to investigate the feasibility of using advanced computational methods, like Monte Carlo simulation and soft computing techniques (artificial neural networks, fuzzy logic systems, evolutionary computing), for: (i) effectively modelling the degradation mechanisms which typically affect the equipment of electricity production plants (Track 1); (ii) effectively modelling and propagating uncertainties from input to output variables of deterministic computational codes (Track 2).
  - Role: main researcher within the team of the Politecnico di Milano.
  - Contributions:
    a) research development with respect to the following issues within Track 2: (i) hybrid representation and modelling of aleatory and epistemic uncertainties (i.e., how to

elicit scarce or imprecise knowledge about input variables to feed possibility distributions and/or fuzzy numbers; how to take into account dependency between uncertain variables in presence of scarce knowledge and a "vague", qualitative definition of dependence; how to place the different uncertainty settings - frequentist, Bayesian, hybrid - in a common methodological framework; how to interpret and communicate the results in an industrial framework); (ii) identifying and pointing out the main difficulties whilst performing hybrid Monte Carlo uncertainty propagation and in giving directions for the effective way to speed up calculations (i.e., rationale of advanced hybrid Monte Carlo methods for estimating low failure probabilities or low-probability quantiles of the uncertain output of a numerical code; analysis of the robustness of the hybrid Monte Carlo estimation and comparison with probabilistic Monte Carlo); (iii) describing and putting into practice soft computing meta-models (mainly artificial neural networks) to replace the original system model, potentially highly time-consuming, for faster uncertainty propagation (i.e., rationale of soft computing meta-models; estimation of meta-model's errors; advantages and drawbacks of soft computing meta-models, in comparison with other "classical" meta-models, e.g., polynomial regression).

b) Delivery of scientific seminars and participation to the exchange meetings with the other members of the project team (Dr. Alberto Pasanisi and Dr. Mathieu Couplet, members of the EdF Research & Development Department of "Industrial Risk Management" or "Maitrise des Risques Industriels (MRI)" in Chatou, France).

c) Papers and reports writing.

– Students supervised: Elisa Ferrario (M.Sc. 1 of Section 4.3)

- Fondation Pour Une Culture De Securitè Industrielle (FonCSI) project (Toulouse, France): *"Quantitative methods of uncertainty representation and modelling in risk analysis for decision-making practice"*, 100000EUR, Co-operation contract no. AO-2008, years of participation: September **2009**-October **2012**.
  – Objective: This project has investigated techniques for modelling and analyzing uncertainties in the risk management of complex socio-technical systems, and their ability to provide useful decision-support information (estimating and representing uncertainty in a way which is understandable by and useful to decision-makers).
  – Role: main researcher within the team of the Politecnico di Milano.
  – Contributions:

a) research development with respect to: (i) the implementation of innovative techniques for the application of recent methods of uncertainty modelling (e.g., possibility theory, belief theory, Bayesian approaches, interval theory, etc.) in risk analysis; (ii) the study and assessment of the contribution of these innovative techniques for people who make decisions on the basis of the outputs of a risk analysis (contribution in terms of decision support, support for ex ante and ex post justification of decisions, support for communication related to a decision, etc.); (iii) the identification of an optimal trade-off between the degree of sophistication of these techniques (in terms of their ability to represent different types of uncertainty in a precise way) and the simplified approaches often inevitable in practice, owing to data, time and/or budget limitations or to the current formulation of regulations and the cultural habits and know-how of decision-makers (in particular, contrasting the complexity of the information presented to decision-makers with its concrete contribution to real decisions); (iv) the indication of guidelines on the selection and concrete use of these representation techniques for practical decision-making.

b) Delivery of scientific seminars and participation to the exchange meetings with the other members of the project team (i.e., École des Mines d'Albi Carmaux, ENTPE

Lyon, Université de Provence, ESCP-Europe, Université de Grenoble, Technische Universität Berlin).

c) Papers and reports writing.

– Students supervised: Elisa Ferrario (M.Sc. 1 of Section 4.3)

	Years						
Research project	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
SINAPS@						**Research collaborator**	
EDF		**Main researcher**					
FonCSI	**Main researcher**						

Table 4. Synthetic presentation of the capitalization and transfer activities

4.6 Scientific outreach

(Rayonnement Scientifique)

This Section reports a detailed list of technical activities that have been carried out during my academic career: they represent my 'scientific outreach' and provide a picture of my position in the international scientific community.

International Journal Editorial Board

- One-year appointment as a Guest Editor for the *International Journal ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, December 2014 - December 2015.
- Guest Co-Editor for the *International Journal ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*. Special Issue on "Advanced Monte Carlo Methods and Applications in Reliability and Risk Analyses", 2014-2015.

International Journals Referee (number of papers reviewed)

- Journal of Mechanical Systems and Signal Processing (1).
- International Journal of Reliability and Safety (1).
- Applied Mathematical Modelling (1).
- ASCE-ASME Risk and Uncertainty in Engineering Systems Part B: Mechanical Engineering (2).
- Journal of Aerospace Information Systems (2).
- ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering (7).
- IEEE Systems Journal (4).
- International Journal of Uncertainty, Fuzziness and Knowledge-based Systems (1).
- IEEE Transactions on Reliability (2).
- Proceedings of the Institution of Mechanical Engineers, Part O, Journal of Risk and Reliability (5).
- Computers and Structures (1).
- Aerospace Science and Technology (1).
- Statistics and Computing (2).
- Nuclear Engineering and Technology (2).
- Science and Technology of Nuclear Installations (2).
- Nuclear Engineering and Design (2).
- Reliability Engineering and System Safety (12).
- IEEE Transactions on Evolutionary Computation (1).

Referee for international conferences

- Invited to review two papers submitted for publication in the Proceedings of the 2015 European Safety and RELiability Conference (ESREL 2015), 7-10 September **2015**, at ETH, the Swiss Federal Institute of Technology, Zürich, Switzerland.
- Invited to review two papers submitted for publication in the Proceedings of the 1st International Conference on Information and Digital Technologies (IDT) 2015, 7-9 July **2015**, Zilina, Slovak Republic.
- Invited to review seven papers submitted for publication in the Proceedings of the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM

11) & European Safety and RELiability Conference (ESREL 2012), 25-29 June **2012**, Helsinki, Finland.

- Invited to review one paper submitted for publication in the Proceedings of the European Safety and RELiability (ESREL) 2011 Conference, 18-23 September **2011**, Troyes, France.
- Invited to review several abstracts submitted for publication in the Proceedings of the Tenth International Probabilistic Safety Assessment and Management (PSAM 10) Conference, 7-11 June **2010**, Seattle, Washington (USA).
- Invited to review one paper submitted for publication in the Proceedings of the 8th International FLINS Conference on Computational Intelligence in Decision and Control, 21-24 September **2008**, Madrid, Spain.
- Invited to review several abstracts submitted for publication in the Proceedings of the Ninth International Probabilistic Safety Assessment and Management (PSAM 9) Conference, 18-23 May **2008**, Hong Kong, China.

Coordinator of technical-scientific areas at international conferences

- Coordinator of the technical-scientific area "Stochastic Modeling and Simulation Techniques" at the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012), 25-29 June **2012**, Helsinki, Finland.

Member of Technical Program Committees of International Conferences

- Member of the Technical Programme Committee (TPC) of the 1st International Conference on Information and Digital Technologies (IDT) 2015, 7-9 July **2015**, Zilina, Slovak Republic.
- Member of the Technical Programme Committee (TPC) of the 2015 European Safety and RELiability Conference (ESREL 2015), 7-10 September **2015**, at ETH, the Swiss Federal Institute of Technology, Zürich, Switzerland.
- Member of the Technical Programme Committee (TPC) of the 10th International Conference on Digital Technologies (DT) 2014 - International Workshop on Reliability Technologies, 9-11 July **2014**, Zilina, Slovak Republic.
- Member of the Technical Programme Committee (TPC) of the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012), 25-29 June **2012**, Helsinki, Finland.

Chairman of Sessions at International Conferences

- Chairman of the session titled "Simulation frameworks for Reliability, Availability, Maintenance and Safety (RAMS) I" at the 2015 European Safety and RELiability Conference (ESREL 2015), 7-10 September **2015**, at ETH, the Swiss Federal Institute of Technology, Zürich, Switzerland.
- Chairman of the session titled "Reliability and risk: automating analyses" at the 2015 European Safety and RELiability Conference (ESREL 2015), 7-10 September **2015**, at ETH, the Swiss Federal Institute of Technology, Zürich, Switzerland.
- Chairman of the session titled "Stochastic simulation for reliability and risk analysis" at the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012), 25-29 June **2012**, Helsinki, Finland.
- Co-chairman of the session titled "Advanced Reactors 16-1: Passive system reliability I" during the "10th International Probabilistic Safety Assessment & Management (PSAM) Conference", Seattle, Washington (USA), 7-11 June **2010**.

Organization of International PhD courses

- Member of the organizing committee of the 4th PhD School on "Vulnerability, risk and resilience of complex system and critical infrastructures", organized by École CentraleSupélec (Chatenay-Malabry, France) and Politecnico di Milano (Milano, Italy), 14-18 September **2015**, CentraleSupélec, Chatenay-Malabry, France.

Seminars, Workshops, Invited Talks and Presentations at International Conferences

- Séminaire Francilien de Sûreté de Fonctionnement, organized by the Groupe de travail de l'Institut de Maitrise des Risques (IMdR), at Ecole Centrale Paris, Chatenay-Malabry, France, 06 June **2014**. **Invited seminar** titled "Efficient Methods for Treating Uncertain Variables in Risk Assessment Models".
- Young Researcher Workshop on "The Future of Reliability and Risk Analysis", supported by ESRA (European Reliability and Safety Association) and SRA (Society of Risk Analysis), Ragusa, Italy, 26-27 May **2014**. **Invited seminar** titled: "Considerations on the treatment of uncertainty in risk assessment, in the presence of 'extreme' events".
- European Safety and RELiability Conference (ESREL) 2013, Amsterdam, The Netherlands, 29 September-2 October **2013**. **Oral presentation of the paper**: N. Pedroni, E. Zio, A. Pasanisi, M. Couplet, "Bayesian probabilistic analysis of a nuclear power plant small loss of coolant event tree model with possibilistic parameters.
- Seminar organized by the Department of Research & Development (R&D) – Management des Risques Industriels (MRI) of the Electricité de France (EdF), Clamart, France, 11 December **2012**. **Invited seminar** title: "Representing and Modeling Uncertainty in the Risk Assessment of Engineering Systems".
- Second seminar of the "Institut des Sciences du Risque et de l'Incertain (ISRI)" & "Chaire sur les Sciences de Système et Défis Energétiques (SSDE)"-European Foundation for New Energy-Electricité de France, Chatenay-Malabry, France, 29 November **2012**. **Invited seminar** title: "Representing and Modeling Uncertainty in the Risk Assessment of Engineering Systems".
- Seminar organized by the "Fondation pour une Culture de Securitè Industrielle (FonCSI)" (Toulouse, France) within the contract "Quantitative methods of uncertainty representation and modelling in risk analysis for decision-making practice", Politecnico di Milano, Milano, Italy, 15-16 November **2012**. **Invited seminar** titled: "Bayesian updating of the possibilistic parameters of aleatory probability distributions in risk assessment: an application".
- 5th International Conference on Safety & Environment in Process & Power Industry (CISAP-5), Milano, Italy, 3-6 June **2012**. **Oral presentation of the paper**: "Failure and Reliability Predictions by Locally Recurrent Neural Networks".
- Seminar organized by the "Fondation pour une Culture de Securitè Industrielle (FonCSI)" (Toulouse, France) within the contract "Quantitative methods of uncertainty representation and modelling in risk analysis for decision-making practice", Technical University of Berlin (TUB), Berlin, Germany, 23-24 February **2012**. **Invited seminar** titled "Decision-making in presence of uncertainties: an application".
- Workshop on "Uncertainty and Risk Quantification", held at the School of Engineering of the University of Liverpool, 2-3 December **2011**. **Invited oral presentation** titled "The problem of uncertainty in system risk assessment".
- European Safety and RELiability (ESREL) 2011 Conference, Troyes, France, 18-23 September **2011**. **Oral presentation of the paper**: P. Baraldi, N. Pedroni, E. Zio, E. Ferrario, A. Pasanisi, M. Couplet, "Monte Carlo and fuzzy interval propagation of hybrid uncertainties on a risk model for the design of a flood protection dike".
- Seminar organized by the "Fondation pour une Culture de Securitè Industrielle (FonCSI)" (Toulouse, France) within the contract "Quantitative methods of uncertainty representation and modelling in risk analysis for decision-making practice", Institut d'Etudes Politiques

(IEP), Lyon, France, 11-12 July **2011**. **Invited seminar** titled "Quantitative methods of uncertainty representation and modeling in risk analysis for decision-making practice".

- 6th International Conference on Sensitivity Analysis of Model Output (SAMO), Milano, Italy, 19-22 July **2010**. **Oral presentation of the paper**: E. Zio, N. Pedroni, "Sensitivity analysis of the model of a nuclear passive system by means of Subset Simulation".
- 10th International Probabilistic Safety Assessment & Management (PSAM) Conference, Seattle, Washington (USA), 7-11 June **2010**. **Oral presentation of the paper**: G.E. Apostolakis, N. Pedroni, E. Zio, "Artificial Neural Networks and quadratic Response Surfaces for the functional failure analysis of a thermal-hydraulic passive system".
- Seminar organized by the "Fondation pour une Culture de Securitè Industrielle (FonCSI)" (Toulouse, France) within the contract "Quantitative methods of uncertainty representation and modelling in risk analysis for decision-making practice", École Nationale des Travaux Publics de l'État (ENTPE), Lyon, France, 8-9 April **2010**. **Invited seminar** titled "Uncertainty characterization in risk analysis for decision making practice".
- European Safety and RELiability (ESREL) 2009 Conference, Prague, Czech Republic, 6-10 September **2009**. **Oral presentation of the paper**: E. Zio, N. Pedroni, "Subset Simulation and Line Sampling for Advanced Monte Carlo Reliability Analysis".
- **Two-hour invited seminar** titled "Advanced Monte Carlo Simulation Methods for Uncertainty and Sensitivity Analysis in Probabilistic Risk Assessment", held at the Research and Development Department of the US Nuclear Regulatory Commission (NRC), Church Street CSB 6B1, Rockville, Maryland (USA), January 19, **2009**.
- 8th World Congress on Computational Mechanics (WCCM8) – 5th European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2008), Venice, Italy, June 30 – July 5, **2008**. **Oral presentation of the paper**: E. Zio, M. Broggi, L. Golea, N. Pedroni, "Predicting Reliability by Recurrent Neural Networks".
- 1st Summer Safety and Reliability Seminars (SSARS) 2007, Gdansk-Sopot, Poland, 22-29 July **2007**. **Oral presentation of the paper**: F. Cadini, E. Zio, N. Pedroni, "Recurrent Neural Networks for Dynamic Reliability Analysis".
- 7th International Fuzzy Logic and Intelligent Technologies in Nuclear Science (FLINS) Conference on Applied Artificial Intelligence, Genova, Italy, 29-31 August **2006**. **Oral presentation of the paper**: E. Zio, P. Baraldi, N. Pedroni, "Feature Selection for Transients Classification by a Niched Pareto Genetic Algorithm".

Awards, recognitions and scholarships

- Outstanding Reviewer for the ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 2015.
- "Premio giovani ricercatori": prize for the most consistent scientific production in 2010 among the young researchers of the Nuclear Division of the Energy Department of the Politecnico di Milano (Milano, Italy), 2011.
- Progetto Roberto Rocca Visiting Student Fellowship for the Fall 2008 and Spring 2009 semesters at MIT, obtained in 2008 – The award is one of the activities funded by the Progetto Rocca, which promotes collaborations and exchanges between MIT and the Politecnico di Milano.
- Student's congress scholarship covering the registration fee for the 8th World Congress on Computational Mechanics (WCCM8) – 5th European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2008), June 30 – July 5, 2008, Venice, Italy.
- Awarded of a scholarship from the Italian Ministry of Education for supporting the three-year PhD studies in "Radiation Science and Technology" at the Energy Department of the Politecnico di Milano (Milano, Italy), 2007.

- Gold Medal Award, Best Graduate Student of the Year in Nuclear Engineering – Politecnico di Milano (Milano, Italy), 2006.

International collaborations

- Politecnico di Milano (Milano, Italy).
- The Institute of Nuclear Energy Research (INER), Taiwan, within the supervision of PhD student Chung-Kung Lo at École Centrale Paris (see Section 4.3).
- Fondation Pour Une Culture De Securitè Industrielle (FonCSI) (Toulouse, France), within contract AO-2008 *"Quantitative methods of uncertainty representation and modelling in risk analysis for decision-making practice"* (see Section 4.5).
- Electricite' de France (EdF)-Research and Development (R&D) group of "Maîtrise des Risques Industriels" (MRI) (Chatou, France) within contract no. 5910059554 *"Advanced computational methods for modelling the mechanisms of degradation in equipments of electricity production plants and uncertainty modelling and propagation"* (see Section 4.5).

Activities for supporting expertises

- Collaboration with Elisa FERRARIO within the research project "SINAPS@ - Earthquake and Nuclear Facilities: Ensuring and Sustaining Safety" (€ 12.5 million), partly funded by the French National Agency for Research and coordinated by CEA with the following partners: EDF, Ecole Normale Supérieure de Cachan, Ecole Centrale Paris, the Institute for Radiological Protection and Nuclear Safety, Laboratory Soil-Solids-Structures and Risks (Institut Polytechnique de Grenoble), Ecole Centrale de Nantes, EGIS – industry, AREVA, ISTerre, IFSTTAR and CEREMA (see Section 4.5).
- Supervision of Elisa FERRARIO for the research project of EDF, 2010 (see Section 4.5).

5 Complete and classified list of publications and communications

(Liste complète et classée des publications et des communications)

In Section 5.1, we list the papers accepted, published or submitted to peer-reviewed international journals; in Section 5.2, we indicate the book chapters; in Section 5.3, we report the articles published or accepted for publication in the proceedings of international conferences; finally, in Section 5.4, we list the works published as technical reports of international research institutes.

5.1 Peer-reviewed international journal papers

Published or Accepted

1. Y.-P. Fang, **N. Pedroni**, E. Zio, "Optimization of Cascade-Resilient Electrical Infrastructures and its Validation by Power Flow Modelling", *Risk Analysis, an International Journal*, Volume 35, Issue 4, April 2015, pp. 594–607, ISSN 0272-4332, published by Wiley-Blackwell.

2. E. Ferrario, **N. Pedroni**, E. Zio, "Analysis of the robustness and recovery of critical infrastructures by Goal Tree Success Tree – Dynamic Master Logic Diagram, within a multi-state system-of-systems framework, in the presence of epistemic uncertainty", accepted for publication on the *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering* (*Special Issue on Non-probabilistic Approaches for Handling Uncertainty in Engineering*), doi: 10.1115/1.4030439, ISSN 2332-9025, published by the American Society of Mechanical Engineers.

3. **N. Pedroni**, E. Zio, "Hybrid Uncertainty and Sensitivity Analysis of the Model of a Twin-Jet Aircraft", *Journal of Aerospace Information Systems* (*Special Issue on NASA Langley Multidisciplinary Uncertainty Quantification Challenge*), Vol. 12, 2015, pp. 73-96, doi: 10.2514/1.I010265, ISSN 2327-3097, published by American Institute of Aeronautics and Astronautics.

4. T.-R. Wang, V. Mousseau, **N. Pedroni**, E. Zio, "Assessing the Performance of a Classification-Based Vulnerability Analysis Model", accepted for publication on *Risk Analysis, an International Journal*, 2014, doi: 10.1111/risa.12305, ISSN 0272-4332, published by Wiley-Blackwell.

5. Y.-P. Fang, **N. Pedroni**, E. Zio, "Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network", accepted for publication on *IEEE Systems Journal*, 2015, doi: 10.1109/JSYST.2014.2352152, ISSN 1932-8184, published by IEEE Systems Council, Institute of Electrical and Electronics Engineers.

6. C.-K. Lo, **N. Pedroni**, E. Zio, "Treating uncertainties in a nuclear seismic probabilistic risk assessment by means of the Dempster-Shafer theory of evidence", *Nuclear Engineering and Technology*, Vol. 46, Issue 1, 2014, pp. 11-26, ISSN 1738-5733, published by Korean Nuclear Society.

7. **N. Pedroni**, E. Zio, E. Ferrario, A. Pasanisi, M. Couplet, "Hierarchical propagation of probabilistic and non-probabilistic uncertainty in the parameters of a risk model", *Computers and Structures* (*Special Issue on Uncertainty Quantification in Structural Analysis and Design*), Vol. 126, Sept. 2013, pp. 199–213, ISSN 0045-7949, published by Elsevier Ltd.

8. Y.F. Li, **N. Pedroni**, E. Zio, "A Memetic Evolutionary Multi-Objective Optimization Method

for Environmental Power Unit Commitment", *IEEE Transactions on Power Systems*, Vol. 28, Issue 3, 2013, pp. 2660-2669, ISSN 0885-8950, published by IEEE Power & Energy Society.

9. **N. Pedroni**, E. Zio, "Uncertainty analysis in fault tree models with dependent basic events", *Risk Analysis, an International Journal*, Vol. 33, Issue 6, 2013, pp. 1146–1173, ISSN 0272-4332, published by Wiley-Blackwell.

10. **N. Pedroni**, E. Zio, "Empirical comparison of methods for the hierarchical propagation of hybrid uncertainty in risk assessment, in presence of dependences", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 20, Issue 4, 2012, pp. 509-557, ISSN 0218-4885, published by World Scientific Publishing.

11. E. Zio, **N. Pedroni**, "Monte Carlo Simulation-based Sensitivity Analysis of the model of a Thermal-Hydraulic Passive System", *Reliability Engineering and System Safety*, Vol. 107, Nov. 2012, pp. 90-106, ISSN 0951-8320, published by Elsevier Ltd.

12. E. Zio, M. Broggi, L. Golea, **N. Pedroni**, "Failure and Reliability Predictions by Locally Recurrent Neural Networks", in: V. Cozzani, E. De Rademaeker (Eds.), *Chemical Engineering Transactions – Proceedings of the 5th International Conference on Safety & Environment in Process & Power Industry (CISAP-5)*, Milano, Italy, 3-6 June 2012, Volume 26, pp. 117-122, published by The Italian Association of Chemical Engineering-AIDIC, 2012, ISBN 978-88-95608-17-4, ISSN 1974-9791.

13. F. Cadini, D. Avram, **N. Pedroni**, E. Zio, "Subset Simulation of a reliability model for radioactive waste repository performance assessment", *Reliability Engineering and System Safety*, Volume 100, Apr. 2012, pp. 75-83, ISSN 0951-8320, published by Elsevier Ltd.

14. E. Zio, **N. Pedroni**, "How to effectively compute the reliability of a thermal-hydraulic passive system", *Nuclear Engineering and Design*, Volume 241, Issue 1, Jan. 2011, pp. 310-327, ISSN 0029-5493, published by Elsevier Ltd.

15. E. Zio, **N. Pedroni**, "An optimized Line Sampling method for the estimation of the failure probability of nuclear passive systems", *Reliability Engineering and System Safety*, Volume 95, Issue 12, Dec. 2010, pp. 1300-1313, ISSN 0951-8320, published by Elsevier Ltd.

16. E. Zio, G. E. Apostolakis, **N. Pedroni**, "Quantitative functional failure analysis of a thermal-hydraulic passive system by means of bootstrapped Artificial Neural Networks", *Annals of Nuclear Energy*, Volume 37, Issue 5, 2010, pp. 639-649, ISSN 0306-4549, published by Elsevier Ltd.

17. **N. Pedroni**, E. Zio, G. E. Apostolakis, "Comparison of bootstrapped Artificial Neural Networks and quadratic Response Surfaces for the estimation of the functional failure probability of a thermal-hydraulic passive system", *Reliability Engineering and System Safety*, Volume 95, Issue 4, 2010, pp. 386-395, ISSN 0951-8320, published by Elsevier Ltd.

18. E. Zio, **N. Pedroni**, M. Broggi, L. Golea, "Modelling the dynamics of the Lead Bismuth Eutectic eXperimental Accelerator Driven System by an Infinite Impulse Response Locally Recurrent Neural Network", *Nuclear Engineering and Technology*, Volume 41, Issue 10, 2009, pp. 1293-1306, ISSN 1738-5733, published by the Korean Nuclear Society.

19. E. Zio, **N. Pedroni**, "Functional Failure Analysis of a Thermal-Hydraulic Passive System by Means of Line Sampling", *Reliability Engineering and System Safety*, Volume 9, Issue 11, Nov. 2009, pp. 1764-1781, ISSN 0951-8320, published by Elsevier Ltd.

20. E. Zio, M. Broggi, **N. Pedroni**, "Nuclear Reactor Dynamics On-Line Estimation by Locally Recurrent Neural Networks", *Progress in Nuclear Energy*, Volume 51, Issue 3, Apr. 2009, pp. 573-581, ISSN 0149-1970, published by Elsevier Ltd.

21. E. Zio, **N. Pedroni**, "Estimation of the Functional Failure Probability of a Thermal-Hydraulic Passive System by Subset Simulation", *Nuclear Engineering and Design*, Volume 239, Issue 3, Mar. 2009, pp. 580-599, ISSN 0029-5493, published by Elsevier Ltd.

22. P. Baraldi, **N. Pedroni**, E. Zio, "Application of a Niched Pareto Genetic Algorithm for Selecting Features for Nuclear Transients Classification", *International Journal of Intelligent Systems*, Volume 24, Issue 2, Feb. 2009, pp. 118-151, ISSN 0884-8173, published by Wiley Periodicals, Inc., A Wiley Company.

23. E. Zio, P. Baraldi, **N. Pedroni**, "Optimal Power System Generation Scheduling by Multi-Objective Genetic Algorithms With Preferences", *Reliability Engineering and System Safety*, Volume 94, Issue 2, Feb. 2009, pp. 432-444, ISSN 0951-8320, published by Elsevier Ltd.

24. E. Zio, **N. Pedroni**, "Building Confidence in the Reliability Assessment of Thermal-Hydraulic Passive Systems", *Reliability Engineering and System Safety*, Volume 94, Issue 2, Feb. 2009, pp. 268-281, ISSN 0951-8320, published by Elsevier Ltd.

25. F. Cadini, E. Zio, **N. Pedroni**, "Recurrent Neural Networks for Dynamic Reliability Analysis", *Reliability & Risk Analysis: Theory & Applications*, Volume 1, Issue 2, Jun. 2008, pp. 30-42, ISSN 1932-2321, published by Gnedenko Forum Publications.

26. F. Cadini, E. Zio, **N. Pedroni**, "Validation of Infinite Impulse Response Multi-Layer Perceptron for Modeling Nuclear Dynamics", *Science and Technology of Nuclear Installations*, Volume 2008, Article ID 681890, doi: 10.1155/2008/681890, ISSN 1687-6075, published by Hindawi Publishing Corporation.

27. F. Cadini, E. Zio, **N. Pedroni**, "Simulating the Dynamics of the Neutron Flux in a Nuclear Reactor by Locally Recurrent Neural Networks", *Annals of Nuclear Energy*, Volume 34, Issue 6, Jun. 2007, pp. 483-495, ISSN 0306-4549, published by Elsevier Ltd.

28. E. Zio, P. Baraldi, **N. Pedroni**, "Selecting Features for Nuclear Transients Classification by Means of Genetic Algorithms", *IEEE Transactions on Nuclear Science*, Volume 53, Issue 3, Jun. 2006, pp.1479-1493, ISSN 0018-9499, published by IEEE Nuclear and Plasma Sciences Society.

Under Review/Revision

29. P. Turati, **N. Pedroni**, E. Zio, "An adaptive simulation framework for the efficient, semi-automatic exploration of extreme and unexpected events in the risk assessment of dynamic engineered systems", submitted for publication on *Risk Analysis, an International Journal*, 2015, ISSN 0272-4332, published by Wiley-Blackwell.

30. **N. Pedroni**, E. Zio, "An Adaptive Metamodel-Based Subset Importance Sampling method for the efficient estimation of the small functional failure probability of a thermal-hydraulic passive system", submitted for publication on *Applied Mathematical Modelling*, 2015, ISSN: 0307-904X, published by Elsevier Ltd.

31. T. R. Wang, V. Mousseau, **N. Pedroni**, and E. Zio, "Identification of protective actions to reduce the vulnerability of safety-critical systems to malevolent intentional acts: an optimization-based decision-making approach", submitted for publication on *European Journal of Operational Research*, 2015, ISSN: 0377-2217, published by Elsevier Ltd.

32. T.-R. Wang, V. Mousseau, **N. Pedroni**, E. Zio, "An empirical classification-based framework for the safety-related criticality assessment of complex energy production systems, in presence of inconsistent data", under first review on *Reliability Engineering and System Safety*, 2015, ISSN 0951-8320, published by Elsevier Ltd.

33. T.-R. Wang, **N. Pedroni**, E. Zio, "Identification of protective actions to reduce the vulnerability of safety-critical systems to malevolent intentional acts: a sensitivity-based decision-making approach", under revision on *Reliability Engineering and System Safety*, 2015, ISSN 0951-8320, published by Elsevier Ltd.

34. E. Ferrario, **N. Pedroni**, E. Zio, "Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation", under first review on *Reliability Engineering and System Safety*, ISSN 0951-8320, published by Elsevier Ltd.

35. P. Turati, **N. Pedroni**, E. Zio, "Advanced RESTART method for the estimation of the probability of failure of highly reliable hybrid dynamic systems", under second review on *Reliability Engineering and System Safety*, 2015, ISSN 0951-8320, published by Elsevier Ltd.

36. Y.-P. Fang, **N. Pedroni**, E. Zio, "Resilience-based component importance measures for critical infrastructure network systems", under second review on *IEEE Transactions on Reliability*, 2015, ISSN 0018-9529, published by IEEE Reliability Society.

37. Y.-P. Fang, **N. Pedroni**, E. Zio, "Assessment and optimization of the resilience of infrastructure network systems subject to disruptive events", under first review on *IEEE Systems Journal*, 2015, ISSN 1932-8184, published by IEEE Systems Council, Institute of Electrical and Electronics Engineers.

38. **N. Pedroni**, E. Zio, A. Pasanisi, M. Couplet, "Bayesian update of the parameters of probability distributions for risk assessment in a two-level hybrid probabilistic-possibilistic uncertainty framework", under first review on the *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, 2015, eISSN 2376-7642, published by the American Society of Civil Engineers.

39. **N. Pedroni**, E. Zio, A. Pasanisi, M. Couplet, "A critical discussion and practical recommendations on some issues relevant to the non-probabilistic treatment of uncertainty in engineering risk assessment", under second revision for publication on *Risk Analysis, an International Journal*, 2015, ISSN 0272-4332, published by Wiley-Blackwell.

5.2 Book chapters

40. E. Zio, **N. Pedroni**, "Reliability Estimation by Advanced Monte Carlo Simulation", In: J. Faulin, A.A. Juan, S. Martorell, J.E. Ramirez-Marquez (Eds.), *Simulation Methods for Reliability and Availability of Complex Systems* (Springer series in *Reliability Engineering*), pp. 3-39, Springer-Verlag, London, United Kingdom, 2010, ISBN 978-1-84882-212-2.

41. F. Cadini, E. Zio, **N. Pedroni**, "Nuclear Dynamics Modelling by Recurrent Neural Networks", in: A.L. Zenfora (Ed.), *Encyclopedia of Energy Research and Policy*, pp. 675-729, Nova Science Publishers, Hauppauge, New York (USA), 2009, ISBN 978-1-60692-161-6.

42. F. Cadini, E. Zio, **N. Pedroni**, "Nuclear Dynamics Modelling by Recurrent Neural Networks", in: V.B. Durelle (Ed.), *Nuclear Energy Research Progress*, pp. 7-62, Nova Science Publishers, Hauppauge, New York (USA), 2008 - 3rd quarter, ISBN 978-1-60456-365-8.

43. E. Zio, P. Baraldi, G. Gola, **N. Pedroni**, "Fault Classifiers Based on Features Selected by Multi-Objective Genetic Algorithms", in: B.C Arnold, N. Balakrishnan, J.M. Sarabian, R. Minguez (Eds.), *Advances in Mathematical and Statistical Modeling* (Springer series in *Statistics for Industry and Technology*), pp. 317-328, Birkhauser, Boston, Massachusetts (USA), 2008, ISBN 978-0-8176-4625-7.

5.3 Conference proceedings

44. E. Ferrario, **N. Pedroni**, E. Zio, F. Lopez-Caballero, "Application of metamodel-based techniques for the efficient seismic analysis of structural systems", accepted for publication on the *Proceedings of the European Safety and RELiability Conference (ESREL) 2015*, Zurich, Switzerland, 7-10 September 2015.

45. P. Turati, **N. Pedroni**, E. Zio, "An entropy-driven method for exploring extreme and unexpected accident scenarios in the risk assessment of dynamic engineered systems", accepted for publication on the *Proceedings of the European Safety and RELiability Conference (ESREL) 2015*, Zurich, Switzerland, 7-10 September 2015.

46. **N. Pedroni**, E. Zio, "Estimating the small failure probability of a nuclear passive safety system by means of an efficient Adaptive Metamodel-Based Subset Importance Sampling method", accepted for publication on the *Proceedings of the European Safety and RELiability Conference (ESREL) 2015*, Zurich, Switzerland, 7-10 September 2015.

47. Y-P. Fang, **N. Pedroni**, Enrico Zio, "Comparing Topological and Physical Approaches to Network Modelling for the Optimization of Failure Resilient Electrical Infrastructures", in: Michael Beer, Siu-Kui Au, Jim W. Hall (eds.), *"Vulnerability, Uncertainty, and Risk", Proceedings of the Second International Conference on Vulnerability and Risk Analysis and Management (ICVRAM2014) & Sixth International Symposium on Uncertainty Modelling and Analysis (ISUMA2014)*, University of Liverpool, Liverpool, UK, 13-16 July 2014, pp. 725-735, ASCE – American Society of Civil Engineers, 2014, ISBN 978-0-7844-1360-9.

48. E. Ferrario, **N. Pedroni**, E. Zio, "Analysis of the Robustness of Critical Infrastructures within a Multistate Systems-of-Systems Framework in the Presence of Epistemic Uncertainties", in: Michael Beer, Siu-Kui Au, Jim W. Hall (eds.), *"Vulnerability, Uncertainty, and Risk", Proceedings of the Second International Conference on Vulnerability and Risk Analysis and Management (ICVRAM2014) & Sixth International Symposium on Uncertainty Modelling and Analysis (ISUMA2014)*, University of Liverpool, Liverpool, UK, 13-16 July 2014, pp. 715-724, ASCE – American Society of Civil Engineers, 2014, ISBN 978-0-7844-1360-9.

49. Y.-P. Fang, **N. Pedroni**, E. Zio, "Optimal production facility allocation for failure resilient critical infrastructures", in: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia and A. C.W.M. Ton. Vrouwenvelder (Eds.), *Safety, Reliability and Risk Analysis, Beyond the Horizon,*

Proceedings of the European Safety and RELiability Conference (ESREL) 2013, Amsterdam, The Netherlands, 29 September-2 October 2013, pp. 2605–2612, Taylor and Francis Group, London, UK, 2014, ISBN 978-1138001237.

50. E. Ferrario, **N. Pedroni**, E. Zio, "Line sampling and Fuzzy Interval Analysis for the propagation of aleatory and epistemic uncertainties in risk models", in: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia and A. C.W.M. Ton. Vrouwenvelder (Eds.), *Safety, Reliability and Risk Analysis, Beyond the Horizon, Proceedings of the European Safety and RELiability Conference (ESREL) 2013*, Amsterdam, The Netherlands, 29 September-2 October 2013, pp. 3273–3280, Taylor and Francis Group, London, UK, 2014, ISBN 978-1138001237.

51. **N. Pedroni**, E. Zio, A. Pasanisi, M. Couplet, "Bayesian update of the parameters of probability distributions for risk assessment in a two-level hybrid probabilistic-possibilistic uncertainty framework", in: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia and A. C.W.M. Ton. Vrouwenvelder (Eds.), *Safety, Reliability and Risk Analysis, Beyond the Horizon, Proceedings of the European Safety and RELiability Conference (ESREL) 2013*, Amsterdam, The Netherlands, 29 September-2 October 2013, pp. 3295–3302, Taylor and Francis Group, London, UK, 2014, ISBN 978-1138001237.

52. C.-K. Lo, **N. Pedroni**, E. Zio, "Bayesian probabilistic analysis of a nuclear power plant small loss of coolant event tree model with possibilistic parameters", in: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia and A. C.W.M. Ton. Vrouwenvelder (Eds.), *Safety, Reliability and Risk Analysis, Beyond the Horizon, Proceedings of the European Safety and RELiability Conference (ESREL) 2013*, Amsterdam, The Netherlands, 29 September-2 October 2013, pp. 3321-3328, Taylor and Francis Group, London, UK, 2014, ISBN 978-1138001237.

53. **N. Pedroni**, E. Zio, E. Ferrario, A. Pasanisi, M. Couplet, "Propagation of aleatory and epistemic uncertainties in the model for the design of a flood protection dike", in: *Proceedings of the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012)*, Helsinki, Finland, 25-29 June 2012, Volume 2, pp. 1193-1202, IAPSAM & ESRA, Printed by Curran Associates, Red Hook, NY USA, ISBN: 978-162276436-5.

54. P. Baraldi, **N. Pedroni**, E. Zio, E. Ferrario, A. Pasanisi, M. Couplet, "Monte Carlo and fuzzy interval propagation of hybrid uncertainties on a risk model for the design of a flood protection dike", in: C. Bérenguer, A. Grall & C. Guedes Soares (Eds.), *Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and RELiability (ESREL) 2011 Conference*, Troyes, France, 18-23 September 2011, pp. 2167-2175, Taylor & Francis Group, London, United Kingdom, 2012, ISBN 978-0-415-68379-1.

55. E. Zio, L. Golea, **N. Pedroni**, G. Sansavini, "Estimation of cascade failure probability in electrical transmission networks by Subset Simulation", in: B. Ale, I.A. Papazoglu, E. Zio (Eds.), *Reliability, Risk and Safety - Proceedings of the European Safety and RELiability (ESREL) 2010 Conference*, Rhodes, Greece, 5-9 September 2010, pp. 694-698, Taylor & Francis Group, London, United Kingdom, 2010, ISBN 978-0-415-60427-7.

56. E. Zio, G.E. Apostolakis, **N. Pedroni**, "Estimation of the failure probability of a thermal-hydraulic passive system by means of Artificial Neural Networks and quadratic Response Surfaces", in: B. Ale, I.A. Papazoglu, E. Zio (Eds.), *Reliability, Risk and Safety - Proceedings of the European Safety and RELiability (ESREL) 2010 Conference*, Rhodes, Greece, 5-9 September 2010, pp. 714-721, Taylor & Francis Group, London, United Kingdom, 2010, ISBN 978-0-415-60427-7.

57. E. Zio, **N. Pedroni**, “Sensitivity analysis of the model of a nuclear passive system by means of Subset Simulation”, in: E. Borgonovo, A. Saltelli, S. Tarantola (Eds.), *Procedia Social and Behavioral Sciences - Proceedings of the 6th International Conference on Sensitivity Analysis of Model Output (SAMO)*, Milano, Italy, 19-22 July 2010, Volume 2, Issue 6, pp. 7778-7779, Elsevier, 2010, ISSN 1877-0428.

58. G.E. Apostolakis, **N. Pedroni**, E. Zio, “Artificial Neural Networks and quadratic Response Surfaces for the functional failure analysis of a thermal-hydraulic passive system”, *Proceedings of the 10th International Probabilistic Safety Assessment & Management (PSAM) 2010 Conference*, Seattle, Washington (USA), 7-11 June 2010, Volume 4, pp. 3161-3172, IAPSAM, ISBN: 978-162276578-2.

59. E. Zio, **N. Pedroni**, “Subset Simulation and Line Sampling for Advanced Monte Carlo Reliability Analysis”, in: R. Bris, C. Guedes Soares and S. Martorell. (Eds.), *Safety, Reliability and Risk Analysis: Theory and Applications - Proceedings of the European Safety and RELiability (ESREL) 2009 Conference*, Prague, Czech Republic, 6-10 September 2009, pp. 687-694, Taylor & Francis Group, London, United Kingdom, 2010, ISBN 978-0-415-55509-8.

60. E. Zio, **N. Pedroni**, “Reliability Analysis of Discrete Multi-State Systems by Means of Subset Simulation”, in: in: S. Martorell, C. Guedes Soares, J. Barnett (Eds.), *Safety, Reliability and Risk Analysis: Theory, Methods and Applications - Proceedings of the European Safety and RELiability (ESREL) 2008 Conference*, Valencia, Spain, 22-25 September 2008, pp. 709-716, Taylor & Francis Group, London, United Kingdom, 2009, ISBN 978-0-415-48513-5.

61. E. Zio, **N. Pedroni**, M. Broggi, L. Golea, “Locally Recurrent Neural Networks for Nuclear Dynamics Modelling”, in: D. Ruan, J. Montero, J. Lu, L. Martinez, P. D’ Hondt, E.E. Kerre (Eds.), *Computational Intelligence in Decision and Control - Proceedings of the 8th International Fuzzy Logic and Intelligent Technologies in Nuclear Science (FLINS) 2008 Conference*, Madrid, Spain, 21-24 September 2008, pp. 367-372, World Scientific Publishing, Singapore, Singapore, 2008, ISBN 978-981-279-946-3.

62. E. Zio, M. Broggi, L. Golea, **N. Pedroni**, “Predicting Reliability by Recurrent Neural Networks”, in: B.A. Schrefler, and U. Perego (Eds.), *Proceedings of the 8th World Congress on Computational Mechanics (WCCM8) – 5th European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2008)*, 30 June – 5 July 2008, Venice, Italy, p. 101 (abstract), International Centre for Numerical Methods in Engineering (CIMNE), Barcelona, Spain, 2008, ISBN 978-84-96736-55-9.

63. F. Cadini, E. Zio, **N. Pedroni**, “Recurrent Neural Networks for Dynamic Reliability Analysis”, In: E. Zio, K. Kolowrocky (Eds.), *Proceedings of the 1st Summer Safety and Reliability Seminars (SSARS) 2007*, Gdansk-Sopot, Poland, 22-29 July 2007, Vol. 1, pp. 45-53, Polish Safety and Reliability Association, Gdansk, Poland, 2007, ISBN 978-83-925436-0-2.

64. F. Cadini, E. Zio, **N. Pedroni**, “Dynamic Systems Modelling by Locally Recurrent Neural Networks”, in: T. Aven & J.E. Vinnem (Eds.), *Risk, Reliability and Societal Safety - Proceedings of the European Safety and RELiability (ESREL) 2007 Conference*, Stavanger, Norway, 25-27 June 2007, pp. 395-403, Taylor & Francis Group, London, United Kingdom, 2007, ISBN-13 978-0-415-44786-7.

65. E. Zio, P. Baraldi, **N. Pedroni**, "Feature Selection for Transients Classification by a Niched Pareto Genetic Algorithm", in: D. Ruan, P. D’ Hondt, P. Fantoni, M. De Cock, M. Nachtegael, E.E. Kerre (Eds.), *Applied Artificial Intelligence - Proceedings of the 7th International Fuzzy*

Logic and Intelligent Technologies in Nuclear Science (FLINS) Conference, Genova, Italy, 29-31 August 2006, pp. 938-945, World Scientific Publishing, Singapore, Singapore, 2006, ISBN 978-981-256-690-4.

5.4 Works published as technical reports of international research institutes

66. E. Zio, **N. Pedroni**, "Possibilistic methods for uncertainty treatment applied to maintenance policy assessment", Number 2014-07 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France, 2014, ISSN 2100-3874. Available at http://www.FonCSI.org/en/cahiers/.

67. E. Zio, **N. Pedroni**, "Case studies in uncertainty propagation and importance measure assessment", Number 2013-12 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France, 2013, ISSN 2100-3874. Available at http://www.FonCSI.org/en/cahiers/.

68. E. Zio, **N. Pedroni**, "Literature review of methods for representing uncertainty", Number 2013-03 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France, 2013, ISSN 2100-3874. Available at http://www.FonCSI.org/en/cahiers/.

69. E. Zio, **N. Pedroni**, "Overview of risk-informed decision-making processes", Number 2012-10 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France, 2012, ISSN 2100-3874. Available at http://www.FonCSI.org/en/cahiers/.

70. E. Zio, **N. Pedroni**, "Uncertainty characterization in risk analysis for decision-making practice", Number 2012-07 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France, 2012, ISSN 2100-3874. Available at the website: http://www.FonCSI.org/fr/cahiers/.

6 Detailed presentation of the past research activities

(Présentation détaillée des activités de recherche)

ADVANCED METHODS FOR THE RISK, VULNERABILITY AND RESILIENCE ASSESSMENT OF SAFETY-CRITICAL ENGINEERING COMPONENTS, SYSTEMS AND INFRASTRUCTURES, IN THE PRESENCE OF UNCERTAINTIES

Safety-critical industrial installations (e.g., nuclear and chemical plants) and infrastructures (e.g., civil, transportation, electric power, water, gas and communication systems) are *complex* systems composed by a multitude and variety of 'elements', that is, physical hard components (e.g., road, railway, pipelines, pumps, etc.), soft components (e.g., SCADA, information and telecommunication systems) and human and organizational components [Gheorghe and Schlapfer, 2006; Kröger and Zio, 2011]. They are highly *interconnected* and mutually *dependent* in complex ways, so that a failure in one critical system or infrastructure can propagate to the others, possibly provoking (*cascading*) *failures* that generate *large consequences* well beyond the initial impact zone [Weron and Simonsen, 2006; Hines et al., 2009; Helbing, 2013]. In addition, such failures may be triggered by *multiple* and *various* sources of *hazards* due to exogenous and endogenous stressors, like natural events, terrorism, criminal activities, malicious behavior, market and policy factors, human factors and technical random failures of hard components [Amin, 2001; Zio, 2009]. Finally, such systems are affected by large *uncertainties* in the characterization of the failure and recovery behavior of their components, their interconnections and interactions: this makes the corresponding analysis a challenging task, because it requires to quantify the uncertainty and to predict how it propagates throughout the system [Apostolakis, 1990; Helton and Pilch, 2011; Aven and Zio, 2010; Zio and Aven, 2011]. All these elements raise concerns with respect to the *risk*, *vulnerability* and *resilience* properties characterizing such systems.

With respect to that, it is worth reminding that *risk* classically refers to the *probability of occurrence* (frequency) of a specific (mostly undesired/adverse) event leading to loss, damage or injury, and its *extent* [Kaplan and Garrick, 1981; Aven, 2012a and b]. These quantities and their associated uncertainties are considered as being numerically quantifiable: e.g., for Critical Infrastructures (CIs), risk can be computed as the loss of service with its resulting consequences for the people concerned [Kröger and Zio, 2011]. On the other hand, *vulnerability* can be defined as the system *inability* to withstand and "resist" to *strains* and *stresses* and it may be exploited by some perhaps unknown or previously unimagined threats and hazards (component failures, natural and men-made hazards) [Aven, 2007; Johansson and Hassel, 2010]. Finally, *resilience* quantifies the

system *ability* to *reduce* the chances of shock, to *adsorb* a shock if it occurs and to *recover* quickly after a shock: it may include technical (physical), organizational, social and economic aspects: see, e.g., [Bruneau et al., 2003; Hollnagel et al., 2006; Aven, 2011b] among many others[1]. These quantities must be *accurately* and *precisely* assessed in order to take rational *decisions* on the utilization of resources for *protecting* the safety-critical systems of interest (possibly from different types of hazards), for reducing their vulnerability and improving their safety and resilience [COM, 2004; EPA, 2009; USNRC, 2009; NASA, 2010].

In general, the tasks outlined above are carried out by the following main steps:

1. System representation: this step aims at capturing the *main features* of the real system providing a picture of the information needed to answer relevant questions. It depends on the type of the system and the outputs of interest: actually, different types of systems can be better described by different representation frameworks (e.g., complex network theory may be more suitable for large distributed systems [Dueñas-Osorio et al., 2007], whereas fault and event trees can be used for industrial installations [Zio, 2007]).
2. System modeling: for a *quantitative* evaluation of risk, vulnerability and resilience, the 'pictorial' representation of the system should be supported by a *mathematical model* [Cox, 2011]. In general, actions, events and physical phenomena that may provoke system failures are described by mathematical models, which are then implemented in *computer codes* for numerical quantification [Bayarri et al., 2007]. Such models are intended to provide: (i) an *approximate* description of the behavior of the real system dependent on a number of (input) *hypotheses* and *parameters*; (ii) the numerical *outputs* of interest (i.e., in this case, the relevant risk, vulnerability and resilience metrics) [Helton and Sallaberry, 2012].
3. System simulation: the mathematical model is employed to *simulate* the behavior of the system under various conditions of interest (e.g., operational transitions and accident scenarios) and to *evaluate* the corresponding critical *outputs* of interest (see step 2. above). Notice that usually, many of the (input) parameters and hypotheses contained in the predictive models of the complex real-world systems are *uncertain* (see details below): thus, this step of 'system simulation' typically amounts to propagating the input uncertainty onto the outputs through the mathematical model [Helton, 2011; Helton et al., 2014b].
4. Decision making: the risk, vulnerability and resilience metrics produced in the simulation step are compared with predefined numerical safety criteria for guidance to risk-informed decision making processes [Helton and Breeding, 1993; Helton et al., 1999; Dubois and

[1] Further details are not given here for brevity. For more precise (and quantitative) definitions and a synthetic, critical discussion on the concepts of risk, vulnerability and resilience, the reader is referred to Section 6.2.1.2.

Guyonnet, 2011; Helton et al., 2011]. In particular, the objective could be that of (optimally) determining a set of protective actions to be taken (e.g., increasing the number of monitoring devices, reducing the number of accesses to the safety-critical system, etc.) in order to effectively reduce (resp., increase) the level of risk and vulnerability (resp., resilience) of the safety-critical systems under consideration [Pepyne et al., 2001; Piwowar et al., 2009].

As a fundamental remark (see step 3. above), it is worth noting that not all the characteristics of the system under analysis can be fully captured in the corresponding mathematical models, due to: (i) the intrinsically *random* nature of several of the phenomena occurring during system operation (e.g., component degradation, failures, or more generally, stochastic transitions among different performance states), and (ii) the *incomplete knowledge* about some of the phenomena (e.g., due to lack of experimental data and results) [Apostolakis, 1990]. This leads to *uncertainty* on both the values of the model (input) parameters and on the hypotheses supporting the model structure; such input uncertainty causes uncertainty in the model outputs and, thus, in the corresponding risk, vulnerability and resilience estimates. This output uncertainty must be estimated as *accurately* and *precisely* as possible (compatibly with the *information available* on the problem) for a realistic quantification of the system behavior and of the associated risk, which builds *confidence* in the overall decision making process [Helton, 1997; Helton and Oberkampf, 2004; Helton et al., 2006]. The general research framework just described is pictorially represented in Figure 1.

Within this general framework, my research has been carried out along two main axes: the first deals with the study of approaches for the *modeling* and *quantification* of *uncertainty* in the reliability analysis and risk assessment of safety-critical components and systems (Section 6.1); the second focuses on the development of *advanced computational methods* for the efficient modeling, simulation and analysis of safety-critical systems and infrastructures in the presence of uncertainties (Section 6.2). A pictorial representation of the two research axes explored in this dissertation is provided in Figure 2.

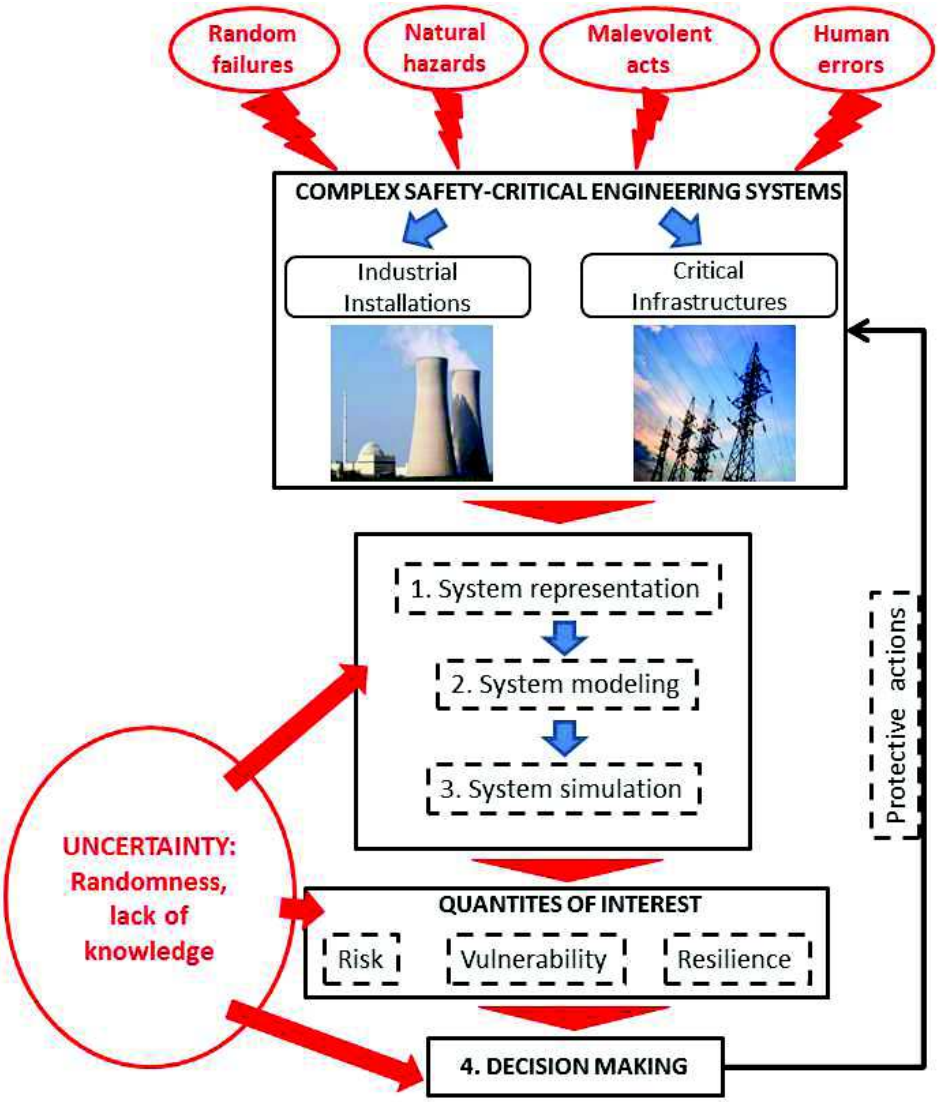


Figure 1. Conceptual structure of the general research framework

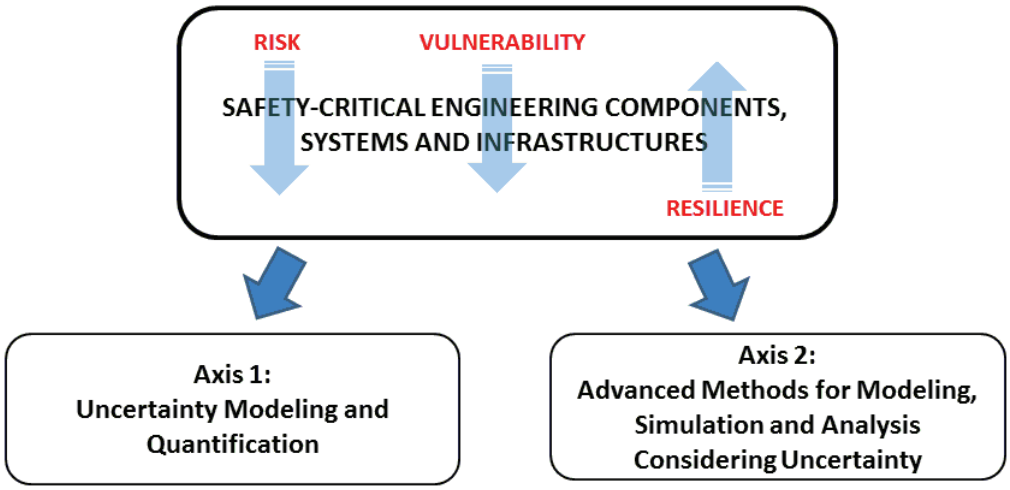


Figure 2. Research Axes 1 and 2 developed during my academic activity

6.1 Axis 1 – Reliability Analysis and Risk Assessment of Safety-Critical Components and Systems: Uncertainty Modeling and Quantification

This Section intends to provide a complete overview on the research activities carried out under Axis 1. It starts by framing the problem of uncertainty in the reliability analysis and risk assessment of safety-critical engineered components and systems (Section 6.1.1); then, it critically surveys some conceptual and practical research issues relevant to this field and the corresponding possible solution approaches (Section 6.1.2); finally, it briefly summarizes the methodological and applicative contributions of the present work to each of the issues addressed (Section 6.1.3).

6.1.1 Problem statement

In this Section, the role of uncertainty in reliability analysis and risk assessment is discussed: in Section 6.1.1.1, the problem of uncertainty affecting the behavior and modeling of safety-critical components and systems is stated; in Section 6.1.1.2, the distinction between aleatory and epistemic uncertainty is recalled.

6.1.1.1 Uncertainties in reliability analysis and risk assessment

In the contexts of reliability analysis and risk assessment of interest to the present thesis, the quantitative analyses of the phenomena occurring in many safety-critical engineering systems, components and applications are based on *mathematical (risk) models*, which are then translated into numerical computer codes for quantification. Such models are intended to provide a representation of the real phenomena, based on a number of *hypotheses* and *parameters*. The models can be deterministic (e.g. Newton's dynamic laws or Darcy's law for groundwater flow) or stochastic (e.g. the Poisson model for describing the occurrence of earthquake events) [EPA, 2009; USNRC, 2009; NASA, 2010]. The risk models provide numerical outputs (e.g., relevant safety parameters) possibly to be compared with predefined numerical safety criteria for further guidance to risk-informed decision making processes [Helton and Breeding, 1993; Helton et al., 2000a; Dubois and Guyonnet, 2011; Helton et al., 2011].

In engineering practice, the mathematical models are *not* capable of capturing *all* the characteristics of the system under analysis. This is due to: (i) the intrinsically *random nature* of several of the phenomena occurring during system operation (e.g., component degradation, failures, or more generally, stochastic transitions among different performance states); (ii) the *incomplete knowledge* about some of the phenomena (e.g., due to lack of experimental results) (see the following Section 6.1.1.2) [USNRC, 1975; Apostolakis, 1990]. This leads to uncertainty on both the values of the model input parameters/variables (*parameter uncertainty*) and on the hypotheses supporting the

model structure (*model uncertainty*). Such uncertainty propagates within the model and causes uncertainty in its outputs and, thus, in the corresponding *risk estimates*. The quantification and characterization of the resulting output uncertainty is of paramount importance for a realistic assessment of the system behaviour and associated risk, for use in decision making [Helton and Davis, 2003; Helton and Oberkampf, 2004]: it defines the scope of the *uncertainty analysis*.

Uncertainty analysis aims at determining the uncertainty in analysis results that derives from uncertainty in the input parameters [Helton et al., 2006]. We formally illustrate this by considering a generic mathematical model $\boldsymbol{f_Z}(\boldsymbol{Y})$, which depends on the input quantities $\boldsymbol{Y} = \{Y_1, Y_2, \ldots, Y_j, \ldots, Y_N\}$ and on the (possibly implicit) function $\boldsymbol{f_Z}(\cdot)$. The model is used to evaluate one or more output quantities $\boldsymbol{Z} = \{Z_1, Z_2, \ldots, Z_l, \ldots, Z_O\}$ of the system under analysis:

$$\boldsymbol{Z} = \{Z_1, Z_2, \ldots, Z_l, \ldots, Z_O\} = \boldsymbol{f_Z}(\boldsymbol{Y}) = \boldsymbol{f_Z}(Y_1, Y_2, \ldots, Y_j, \ldots, Y_N). \quad (1)$$

By way of examples, in the risk-based design of a flood protection dike the output quantity of interest may be represented by the water level of the river in proximity of a residential area [Pasanisi et al., 2009; Limbourg and de Rocquigny, 2010]; in the reliability analysis of emergency safety systems in nuclear reactors the relevant quantity could be represented by, e.g., the peak temperature reached by the fuel cladding during an accidental scenario characterized by loss of coolant [Mackay et al., 2008; Patalano et al., 2008]. In what follows, for the sake of simplicity of illustration and without loss of generality we consider only one (scalar) output Z, i.e., $\boldsymbol{Z} = \{Z_1, Z_2, \ldots, Z_l, \ldots, Z_O\} \equiv Z = f_Z(\boldsymbol{Y})$.

The uncertainty analysis of Z requires an assessment of the uncertainties about $\boldsymbol{Y}$ and their propagation through the model $f_Z(\cdot)$ to produce an assessment of the uncertainties about Z. Typically, the uncertainty about model *parameters* $\boldsymbol{Y}$ and the uncertainty related to the *model structure* $f_Z(\cdot)$, i.e., uncertainty due to the existence of alternative plausible hypotheses on the phenomena involved, are treated separately; actually, while the first source of uncertainty has been widely investigated and more or less sophisticated methods have been developed to deal with it, research is still ongoing to obtain effective and agreed methods to handle the uncertainty related to the model structure [Ferson et al., 2003; Perry and Drouin, 2009; Le Duy et al., 2013]. See also [Aven, 2010b] who distinguishes between *model inaccuracies* (the differences between Z and $f_Z(\boldsymbol{Y})$), and *model uncertainties* due to alternative plausible hypotheses on the phenomena involved[2]. In this thesis, we are concerned only with the uncertainty in the model *parameters* $\boldsymbol{Y} = \{Y_1, Y_2, \ldots, Y_j, \ldots, Y_N\}$.

[2] Notice that model uncertainty also includes the fact that the model could be too *simplified* and therefore would neglect some important phenomena affecting the final result. This latter type of uncertainty is sometimes identified independently from model uncertainty and is known as *completeness* uncertainty [USNRC, 2002 and 2009].

Finally, it is worth reminding that contrary to uncertainty analysis, the aim of *sensitivity analysis* is to identify (and rank) those input parameters, variables and possibly model hypotheses and assumptions that *contribute* the most to the uncertainty in the model outputs and, thus, in the corresponding *risk estimates*. This is of paramount importance for properly driving resource allocation for uncertainty reduction and consequent confidence gain for design, maintenance and operation decision making [Sudret, 2008; Blatman and Sudret, 2010; Sudret and Mai, 2015].

6.1.1.2 Types of uncertainty

In the context of reliability analysis and risk assessment, uncertainty is conveniently distinguished into *two* different *types*: 'aleatory' (also known as 'objective' or 'stochastic') and 'epistemic' (also known as 'subjective' or 'state-of-knowledge') [Parry and Winter, 1981; Apostolakis, 1990; Helton, 1994; Hoffman et al., 1994; Helton and Burmaster, 1996; Parry, 1996; Paté-Cornell, 1996; USNRC, 2009]. The former refers to phenomena occurring in a *random* way. The latter captures the analyst *confidence* in the model by quantifying the degree of belief of the analysts on how well it represents the actual system [Apostolakis, 1993 and 1999].

Aleatory uncertainty is related to the intrinsically *random nature* of several of the phenomena occurring during system operation. It concerns, for instance, the occurrence of the events that define various possible accident scenarios for a safety-critical system (e.g., a nuclear power plant), the time to failure of a component or the random variation of the actual geometrical dimensions and material properties of a component or system (due to differences between the as-built system and its design upon which the analysis is based) [USNRC, 1990, 2002 and 2009; Breeding et al., 1992a and b; Gregory et al., 1992; Brown et al., 1992; Payne et al., 1992; Helton et al., 2000a-c, 2014a and b; Sallaberry et al., 2014]; moreover, examples taken from civil or environmental engineering comprise physical quantities like the maximal water flow of a river during a year, unexpected events like earthquakes or unpredictable processes like erosion, sedimentation and so on [USNRC, 2005; Limbourg and de Rocquigny, 2010].

Epistemic uncertainty is instead associated to the *lack of knowledge* about some properties and conditions of the phenomena underlying the behavior of the systems. This uncertainty manifests itself in the model representation of the system behavior, in terms of both (*model*) uncertainty in the hypotheses assumed and (*parameter*) uncertainty in the (fixed but poorly known) values of the internal parameters of the model [Helton et al., 2000c; Cacuci and Ionescu-Bujor, 2004]; in the present paper, we are concerned only with the uncertainty in the model *parameters*. By way of example, the failure of a mechanical component is a random (i.e., aleatory) event (and, correspondingly, the time to failure T of the component is a random variable). In practice, an exponential probability model ($p^T(t|\lambda) = \lambda \cdot e^{-\lambda t}$) is often built to represent such random phenomenon

(i.e., component failure) and the corresponding random variable (i.e., time to failure T). This aleatory model contains a parameter (i.e., the failure rate λ) that may be known with limited precision by the analyst, i.e., epistemic uncertainty is associated with it [Apostolakis and Kaplan, 1981; Huang et al., 2001; USNRC, 2009].

Finally, notice that whereas epistemic uncertainty can be *reduced* by gathering information and data to improve the knowledge on the system behavior, the aleatory uncertainty cannot, and for this reason it is sometimes also called *irreducible* uncertainty.

6.1.2 Issues and possible solution approaches: a critical literature survey

The conceptual and practical issues related to the modeling and quantification of uncertainty in reliability analysis and risk assessment rise in their extensions to the contemporary or future safety-critical engineered components and systems. In this thesis, we focus on four major ones that we have encountered in our research and practice and that are also confronted by other researchers in the field of reliability and risk engineering (the corresponding possible solution approaches available in the open literature are also presented and critically discussed):

1. The uncertainties in the model (input) parameters and hypotheses have to be first systematically *identified* and *classified*; then, they have to be *quantitatively modeled* and *described* by rigorous mathematical approaches coherently with the *information* available on the system. The key point is to guarantee that uncertainties are taken into account in a way that the *knowledge* relevant for the risk assessment process is *represented* in the most *faithful* manner [Helton et al., 2014a-e; Aven, 2010a,b and 2011; Aven and Steen, 2010]. For sake of simplicity, we will not deal here explicitly with uncertainties tainting the system's model itself. Whether this point is the object of many research and engineering works in the computer experiments community, e.g. [Kennedy and O'Hagan, 2001; Bayarri et al., 2007; Oberkampf and Trucano, 2008; Roy and Oberkampf, 2011], in engineering practice it is more common to separate the phases of assessing model's accuracy and propagating uncertainties from input to output variables [Pasanisi and Dutfoy, 2012]. See also the interesting and pragmatic viewpoint on this issue in [Aven, 2010b] (see Section 6.1.2.1).
2. The uncertainties in the input(s) have to be *propagated* onto the output(s) of the risk model (i.e., onto the risk measures), to provide the decision makers with a clearly *risk-informed* picture of the problem upon which they can confidently reason and deliberate [Aven and Zio, 2010; Dubois and Guyonnet, 2011; Helton and Sallaberry, 2012] (see Section 6.1.2.2).
3. The quantitative representation of uncertainty needs to be *updated*, in a Bayesian framework, when *new* information/evidence (e.g., data) about the system of interest

becomes available [Bernardo and Smith, 1996; Bedford and Cooke, 2001; Kelly and Smith, 2011] (see Section 6.1.2.3).

4. Possible *dependences* existing among the input parameters and variables of the system risk model need to be properly accounted for [Ferson et al., 2004]. Actually, it is widely acknowledged that neglecting such dependences could lead to dramatic *underestimations* of the risk associated to the functioning of complex, safety-critical engineering systems [Ferson, 1996; Ferson and Burman, 1995; Ferson and Long, 1995; Ferson and Ginzburg, 1996] (see Section 6.1.2.4).

A pictorial view of the four conceptual and practical issues addressed in this thesis under research Axis 1 is given in Figure 3.

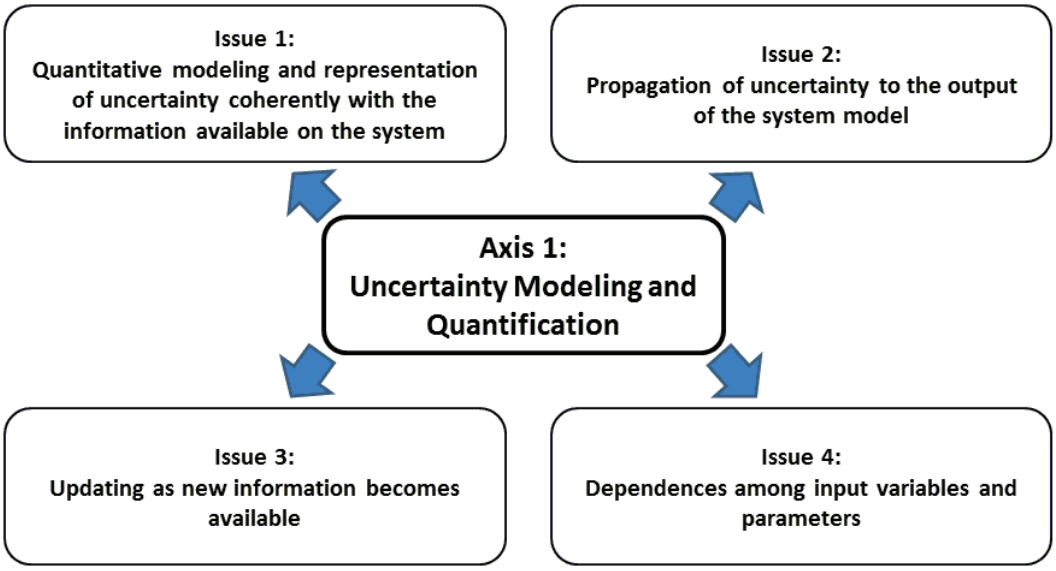


Figure 3. Four conceptual and practical issues addressed under research Axis 1

6.1.2.1 Issue 1: Quantitative modeling and representation of uncertainty coherently with the information available on the system

As already mentioned above, aleatory uncertainty is related to randomness due to inherent variability in the system behavior (thus, it cannot be reduced by acquiring knowledge and information on the system). Probability models are typically introduced to represent this type of uncertainty. Examples of classical probabilistic models used to describe aleatory uncertainties in risk assessment are the Poisson/exponential model for events randomly occurring in time (e.g., random variations of the operating state of a valve) [Hofer et al., 2002; USNRC, 2005; Helton et al., 2014e; Sallaberry et al., 2014], the binomial model for events occurring "as the immediate consequence of a challenge" (e.g., failures on demand of mechanical safety systems) [Krzykacz-Hausmann, 2006; USNRC, 2009] and the Gumbel model for the maximal water level of a river in a particular year [Limbourg and de Rocquigny, 2010]. Probability models constitute the basis for the

statistical analysis of the data and information available on a system, and are considered essential for assessing the aleatory uncertainties and drawing useful insights on its random behaviour [Helton, 1994; Winkler, 1996]. They are also capable of coherently updating the probability values, as new data and information on the system become available.[3]

A probability model presumes some sort of model *stability*, by the construct of *populations* of *similar* units (in the Bayesian context, formally an *infinite* set of *exchangeable* random variables) [Bernardo and Smith, 1996; De Finetti, 1974]. In this framework, the standard procedure for constructing (aleatory) probability models of random events and variables is as follows: (i) observe the random process of interest over a finite period of time, (ii) collect data about the phenomenon, (iii) perform statistical analyses to identify the probability model (i.e., distribution) that best captures the variability in the available data and (iv) estimate the internal parameters of the selected probability model[4] [Bernardo and Smith, 1994; Atwood et al., 2003; Frey and Burmaster, 1999]. For instance, the probability model for the time to failure of a given type of mechanical component can be estimated by collecting a large (in theory, infinite) number of failure times of identical or similar components (e.g., by resorting to experimental reliability tests and/or to historical data bases) and then 'fitting the data' by a proper probability distribution (traditionally, exponential or Weibull distributions are used to this aim) [Apostolakis, 1990; USNRC, 2005; USNRC, 2002 and 2009; NASA, 2010]. However, such 'presumed' model stability is often not fulfilled and the procedure (i)-(iv) above cannot be properly carried out [Bergman, 2009].

In the engineering risk assessment practical context the situations are often *unique*, because the structures systems and components are, in the end, uniquely manufactured, operated and maintained, so that their life realizations is not identical to any others. Then, the collection of repeated random realizations of the related random phenomena of interest (e.g., failure occurrences) means *in reality* the construction of *fictional* populations of *non-existing* similar situations. Then, probability models in general cannot be easily defined; in some cases, they cannot be meaningfully defined at all. For example, it makes no sense to define the (frequentist) probability of a terrorist

---

[3] For the sake of completeness, it is worth remembering that classical probability theory is formally defined by a triple (U, S, p), called a probability space, where: (i) U is a set that contains everything that could occur in the particular universe under consideration, (ii) S is a suitably restricted set of subsets of U, and (iii) p is the function that defines probability for (elements of) S. Notice that p is required to have the following properties: (i) if $A \in S$, then $0 \leq p(A) \leq 1$; (ii) $p(U) = 1$, and (iii) if A_1, A_2, …, is a sequence of disjoint sets from S, then $p(\cup_i A_i) = \sum_i p(A_i)$. Finally, one of the important properties of probability is that $p(A) + p(A^c) = 1$, for $A \in S$. In words, the probability of an event occurring (i.e., $p(A)$) and the probability of an event not occurring (i.e., $p(A^c)$) must sum to one. As discussed in what follows, *less restrictive* conditions on the specification of *likelihood* are present in other approaches to uncertainty representation, e.g., possibility and evidence theories [Helton et al., 2004; Baudrit and Dubois, 2006].

[4] In a *frequentist* view, the available data are interpreted as *observable* random *realizations* of an underlying, *repeatable* probabilistic model (e.g., a probability distribution) representing the aleatory phenomenon of interest, which can be approximated with *increasing precision* by the analyst as the *size* of the available data set *increases* [Apostolakis, 1990].

attack [Aven and Heide, 2009]. In other cases, the conclusion may not be so obvious. For example, the (frequentist) probability of an explosion scenario in a process plant may be introduced in a risk assessment, although the underlying population of infinite similar situations is somewhat difficult to describe [Aven and Zio, 2010].

In addition, even when probability models with parameters can be established (justified) reflecting aleatory uncertainty, in many cases the amount of data available is insufficient for performing a meaningful statistical analysis on the random phenomenon of interest (e.g., because collecting this data is too difficult or costly); in other casas, the pieces of data themselves may be highly imprecise: in such situations, the internal parameters of the selected probability model cannot be estimated with sufficient accuracy and epistemic (state-of-knowledge) uncertainty is associated with them [Baudrit et al., 2008; Dubois, 2010]. A full risk description needs to assess the (epistemic) uncertainties about these quantities. This framework of *two hierarchical* levels of uncertainty is referred to as "two-level" setting in the literature [Helton, 1996 and 2011; Helton and Sallaberry, 2011; Helton et al., 2011 and 2014b, d, e]. Examples of this "two-level" setting may be the following. First, we may consider a generic uncertain (input) variable Y, whose (aleatory) uncertainty is described by a Probability Density Function (PDF) $p^Y(y\,|\,\boldsymbol{\theta})$ with *epistemically-uncertain* internal parameters $\boldsymbol{\theta} = \{\theta_1, \theta_2, ..., \theta_m, ..., \theta_P\}$. In a reliability analysis framework, Y may represent the (random) time to failure T of a mechanical component, classically modeled by a Weibull distribution $p^Y(y\,|\,\boldsymbol{\theta}) = p^T(t|\alpha, \beta) = Weibull(\alpha, \beta)$ with poorly known location and scale parameters $\boldsymbol{\theta} = \{\alpha, \beta\}$. Another example can be taken from Fault Tree Analysis (FTA). In this case, the (aleatory) probability model is constituted by the Fault Tree (FT) itself, where the logic of the functioning/disfunctioning of the system of interest is systematically captured and the (random) event of system failure (namely, the Top Event-TE) is described by the combinations of the (random) failures of the individual (hardware, software and human) elements composing the system (namely, the Basic Events-BEs). If the internal parameters of such model, i.e., the probabilities (frequencies) of the BEs, are known with poor precision by the analysts, then epistemic uncertainty is associated with them (and consequently with the probability-frequency of the TE).

In the current risk assessment practice, the epistemic uncertainty in the parameters entering the (probability) models of random events is typically represented by (subjective) probability distributions within a *Bayesian* framework: subjective probability distributions capture the analyst *confidence* in the probability model by quantifying his/her *degree of belief* on how well the model represents the actual phenomenon [Apostolakis and Kaplan, 1981; Apostolakis, 1990, 1993 and 1999; Cooke, 1991; Ayyub, 2001; Meyer and Booker, 2001; Baudrit et al., 2006; Aven, 2010a, b; Huang et al., 2001; Singpurwalla, 2006; North, 2010; USNRC, 2002, 2005 and 2009]. The common

term used is Probabilistic Risk Assessment (PRA, also referred to as Quantitative Risk Assessment-QRA) [Garrick et al., 1967; Helton et al., 2000a-c and 2014a-e; Apostolakis, 2006; NAS/NRC, 2008]. In facts, probability has been used to represent both aleatory and epistemic uncertainty from the beginning of the formal development of probability in the late 1600's [Hacking, 1975]. However, one of the foundations of this approach is the de Finetti's representation theorem (see [Bernardo, 1996] for a pedagogical presentation), the underlying hypothesis of which is, in practice, the exchangeability of the observations depending on epistemically uncertain variables. However, the probability-based approach to epistemic uncertainty representation can be considered unsatisfactory in some particular conditions of practical risk assessment when the hypothesis of exchangeability could be challenged [Aven and Zio, 2010]. Besides these mathematical considerations, the practical arguments against the fully probabilistic approach are evoked hereinafter.

First of all, representing epistemic uncertainty by probability distributions (albeit subjective) amounts *in practice* to representing partial ignorance (imprecision) in the *same* way as randomness (variability) [Baudrit et al., 2008; Dubois, 2010]. Also, the fully probabilistic framework for assessing risk and uncertainties may be too narrow, as the subjective expert knowledge that the probability distributions are based on could be poor and/or even based on wrong assumptions, thus leading to conclusions that can mislead decision making. In the unique situations of risk assessment, the information available usually is *not* a *sufficiently* strong basis for assigning *specific* probability distributions. In practical risk assessment and decision making, there are often many stakeholders and they may not be satisfied with a probability-based assessment based on subjective judgments made by one analysis group [Aven and Zio, 2010].

To overcome the above shortcomings of the fully probabilistic representation of uncertainty in risk assessment, *alternative* (*non-fully probabilistic*) approaches for representing and describing epistemic uncertainties in risk assessment have been suggested [Helton and Oberkampf, 2004; Helton and Johnson, 2011; Aven, 2010a,b and 2011a; Aven and Steen, 2010; Aven and Zio, 2011; Flage et al., 2009; Beer et al., 2013b and 2014b], e.g., fuzzy set theory [Klir and Yuan, 1995], fuzzy probabilities [Buckley, 2005; Beer, 2009b; Pannier et al., 2013], random set theory [Molchanov, 2005], Dempster-Shafer theory of evidence [Dempster, 1967a and b; Shafer, 1976, 1987 and 1990; Ferson et al., 2003 and 2004; Helton et al., 2007a,b and 2010; Sentz and Ferson, 2002; Le Duy et al., 2013; Sallak et al., 2013], possibility theory (that can be considered also a 'special case' of evidence theory) [Baudrit and Dubois, 2006; Baudrit et al., 2006 and 2008; Dubois, 2006; Dubois and Prade, 1988], interval analysis [Moore, 1979; Ferson and Hajagos, 2004; Ferson and Tucker,

2006; Ferson et al., 2007 and 2010; Jalal-Kamali and Kreinovich, 2013; Muscolino and Sofi, 2013; Zhang et al., 2013], interval probabilities [Weichselberger, 2000] and probability bound analyses using p-boxes [Ferson and Ginzburg, 1996; Crespo et al., 2013; Mehl, 2013]. These settings are becoming popular in the reliability analysis and risk assessment frameworks and the remainder of the Section will be essentially focused on them. On the other hand, notice that the technical details of the different frameworks will be exposed only to the extent necessary to analyze and judge how these contribute to the communication of risk and the representation of the associated uncertainties to decision makers, in the typical settings of reliability analysis and risk assessment of safety-critical systems with limited knowledge on their behavior. The driver of the critical analysis is really the need to feed the decision making process with representative information derived from the risk assessment, to robustly support the decision.

In probability bound analysis, *intervals* are used for those components whose uncertainty cannot be accurately estimated (in other words, the knowledge of the analyst is not sufficient for providing a single, precise value or probability distribution for the parameter of interest, that is thus 'imprecisely' defined by a *range* of possible values, all of which are *coherent* with the scarce information available). For the other components, traditional probabilistic analysis is carried out. This procedure results in a couple of *extreme* limiting Cumulative Distribution Functions (CDFs) (namely, a probability box or p-box) that *bound* above and below the "true" CDF of the quantity of interest. For illustration purposes, Figure 4 shows an example of probability box (p-box) for a generic uncertain (input) variable *Y*: the upper and lower CDFs, $\overline{F}^Y(y)$ and $\underline{F}^Y(y)$, respectively, represent *sure* bounds on the "true" (unknown) CDF $F^Y(y)$ of *Y*, i.e., $\underline{F}^Y(y) \leq F^Y(y) \leq \overline{F}^Y(y)$, $\forall y \in \Re$. The distance between the CDF bounds $\overline{F}^Y(y)$ and $\underline{F}^Y(y)$ pictorially reflects the limited knowledge of the analyst who is *not* able to specify a *single* (aleatory) probability model (i.e., a single CDF) for *Y*. Actually, the *family* of *all* the CDFs that can be "drawn" within $\overline{F}^Y(y)$ and $\underline{F}^Y(y)$ is *coherent* with the (scarce and/or vague) information available on *Y*; thus, in principle *any* CDF belonging to such family could represent the "true" (unknown) probability model $F^Y(y)$.

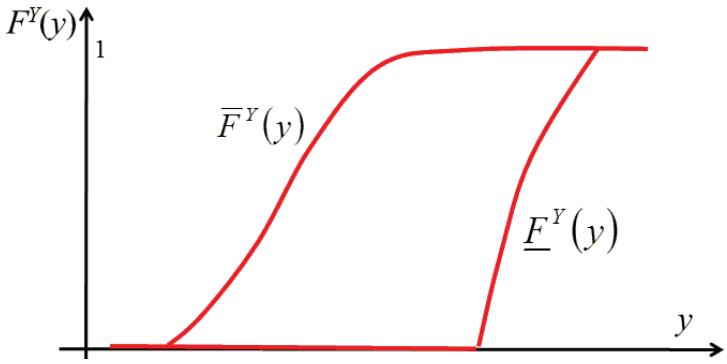


Figure 4. Example of probability box (p-box) for the generic uncertain variable Y

However, this way of proceeding results often in very *wide* intervals and the approach has been criticised for not providing the decision-maker with specific analyst and expert judgments about epistemic uncertainties [Aven, 2010b]. The other frameworks mentioned above allow for the incorporation and representation of *incomplete* information. Their motivation is to be able to treat situations where there is *more* information than that supporting just an *interval* assignment on an uncertain parameter, but *less* than that required to assign a *single specific probability distribution*.

All these theories produce epistemic-based uncertainty descriptions and in particular *probability intervals*. In few details, in fuzzy set theory membership functions are employed to express the *degree of compatibility* of a given numerical value to a fuzzy (i.e., vague, imprecisely defined) set (or interval). In possibility theory, uncertainty is represented by using a *possibility distribution function* that quantifies the *degree of possibility* of the values of a given uncertain (input) parameter, say, Y. Formally, an application of possibility theory involves the specification of a pair $(U, \pi^Y(y))$ (called a possibility space), where: (i) U is a set that contains everything that could occur in the particular universe under consideration (e.g., it contains all the values that parameter Y can assume); (ii) $\pi^Y(y)$ is the possibility distribution function mentioned above: this function is defined on U and is such that $0 \leq \pi^Y(y) \leq 1$ for $y \in U$ and $\sup\{\pi^Y(y): y \in U\} = 1$. The function $\pi^Y(y)$ provides a measure of the likelihood that can be assigned to each element y of the universal set U (i.e., sample space) U. With respect to that, whereas in probability theory a *single* probability distribution function is introduced to define the (*single-valued*) probability of any interval (or event) A, in possibility theory one possibility function gives rise to *two measures* of likelihood, referred to as possibility and necessity measures $\{\Pi^Y(A), N^Y(A)\}$. These two measures represent *probability bounds*, i.e., upper and lower probabilities, respectively: such measures are mathematically defined as $\Pi^Y(A) = \sup_{y \in A}\{\pi^Y(y)\}$ and $N^Y(A) = 1 - \sup_{y \notin A}\{\pi^Y(y)\} = 1 - \Pi^Y(A^c)$, respectively [Helton et al., 2004; Baudrit and Dubois, 2006; Baudrit et al., 2006 and 2008; Dubois, 2006; Dubois and Prade, 1988]. It can be demonstrated that the probability $P^Y(A)$ associated to an event or to a set (interval)

A of parameter values is *bounded above* and *below* by such necessity and possibility values, i.e., $N^Y(A) \le P^Y(A) \le \Pi^Y(A)$. In other words, such bounds reflect the fact that due to the scarce information available, the analyst is *not* able or willing to precisely assign his/her probability $P^Y(A)$: he/she can only bound it by *upper* and *lower limits*. From the definitions of $\{\Pi^Y(A), N^Y(A)\}$ above and referring to the particular set (interval) $A = (-\infty, y]$, we can deduce the associated *cumulative* necessity/possibility measures $N^Y(A) = N^Y((-\infty, y])$ and $\Pi^Y(A) = \Pi^Y((-\infty, y])$. Given that $N^Y(A) \le P^Y(A) \le \Pi^Y(A)$ and that $P^Y((-\infty, y]) = F^Y(y)$ by definition, then $N^Y((-\infty, y])$ and $\Pi^Y((-\infty, y])$ can be interpreted as the lower and upper limiting CDFs $\underline{F}^Y(y)$ and $\overline{F}^Y(y)$, respectively, for the uncertain variable Y. For illustration purposes and by way of example, we consider an uncertain parameter Y. We suppose that the *only* information available on Y is that it can take values in the range (support) [900, 1300] and the most likely value (mode) is 1100. To represent this information a triangular possibility distribution on the interval [900, 1300] is typically used, with maximum value at 1100 (Figure 5 left). The corresponding cumulative necessity and possibility measures, $N^Y((-\infty, y]) = \underline{F}^Y(y)$ and $\Pi^Y((-\infty, y]) = \overline{F}^Y(y)$, respectively, are shown in Figure 5 right. This means that the triangular possibility distribution $\pi^Y(y)$ of Figure 5 left "produces" the couple of CDFs shown in Figure 5 right: more importantly, it can be demonstrated that such CDFs bound *all* the possible CDFs (i.e., *all* the possible probability models) characterized by mode equal to 1100 and support [900, 1300]. In other words, the *single* possibility function $\pi^Y(y)$ "encodes" the *family* of *all* the CDFs (i.e., of *all* the probability models) with mode equal to 1100 and support [900, 1300] (see [Ferson et al., 2003; Baudrit and Dubois, 2006; Dubois, 2006] for a formal proof of this statement).

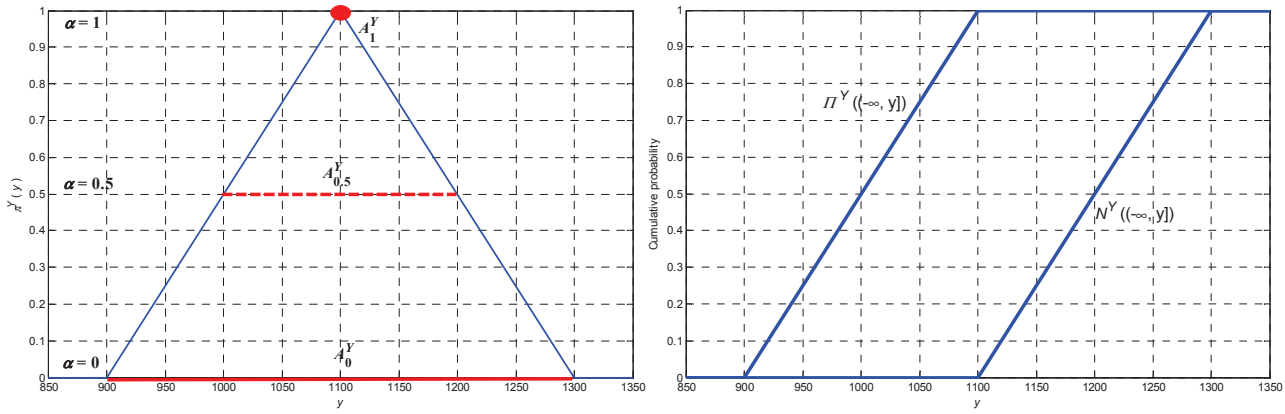


Figure 5. Left: triangular possibility distribution $\pi^Y(y)$ of a generic uncertain variable Y; in evidence, the α-cuts of level α = 0 (solid segment), 0.5 (dashed segment) and 1 (dot). Right: bounding upper and lower CDFs (i.e., cumulative possibility and necessity) of Y, $\underline{F}^Y(y) = N^Y(A) = N^Y((-\infty, y])$ and $\overline{F}^Y(y) = \Pi^Y(A) = \Pi^Y((-\infty, y])$, $A = (-\infty, y]$, respectively

In order to provide an additional *practical* interpretation of the possibility distribution function $\pi^Y(y)$, we can define its so-called α-cut sets (intervals) $A_\alpha^Y = \{y: \pi^Y(y) \geq \alpha\}$, with $0 \leq \alpha \leq 1$. For example, $A_{0.5}^Y = [1000, 1200]$ is the set (interval) of y values for which the possibility function is greater than or equal to 0.5 (dashed segment in Figure 5 left). In the light of the discussion above, the α-cut set A_α^Y of parameter Y can be interpreted as the $(1 - \alpha)\cdot 100\%$ Confidence Interval for Y, i.e., the interval such that $P[Y \in A_\alpha^Y] \geq 1-\alpha$. Actually, $N(A_\alpha^Y) \leq P[Y \in A_\alpha^Y] \leq \Pi(A_\alpha^Y)$, which is equivalent to write $1-\sup_{Y \notin A_\alpha^Y}\{\pi^Y(y)\} \leq P[Y \in A_\alpha^Y] \leq \sup_{Y \in A_\alpha^Y}\{\pi^Y(y)\}$, i.e., $1 - \alpha \leq P[Y \in A_\alpha^Y] \leq 1$. For example, $A_0^\gamma = [900, 1300]$ is the $(1 - 0)\cdot 100\% = 100\%$ CI for γ, i.e., the interval that contains the "true" value of γ with certainty (solid segment in Figure 5, top left); $A_{0.8}^\gamma = [1050, 1150]$ ($\subset A_0^\gamma$) is the $(1 - 0.8)\cdot 100\% = 20\%$ confidence interval, and so on. In this view, the possibility distribution $\pi^Y(y)$ can be interpreted as a *set* of *nested* confidence intervals for parameter Y [Baudrit and Dubois, 2006].

Finally, in Dempster-Shafer Theory of Evidence (DSTE) uncertainty is described by a so-called *body of evidence*, i.e., a list of *focal sets/elements* (e.g., intervals) each of which is assigned a *probability* (or *belief*) *mass* (so-called Basic Probability Assignment-BPA). Formally, an application of evidence theory involves the specification of a triple (U, S, m) (called evidence space), where: (i) U is a set that contains everything that could occur in the particular universe under consideration, e.g., all the values that a given uncertain (input) parameter Y can assume (namely, the sample space or universal set); (ii) S is a countable collection of subsets of U (i.e., the ensemble of the so-called *focal elements*); (iii) m is a function (i.e., the BPA) defined on subsets of U, such that: (i) $m(A) > 0$, if $A \in S$; (ii) $m(A) = 0$, if $A \subset U$ and $A \notin S$, and (iii) $\sum_{A \in S} m(A) = 1$. For a subset A of U, $m(A)$ is a number characterizing the *amount* of *likelihood* that can be assigned to A, but no proper subset of A. In this respect, it is worth noting that differently from probability theory, the function m is *not* the fundamental measure of likelihood. Rather, two measures (namely, *plausibility* and *belief* measures) are induced by m that *bound* the probability $P^Y(A)$ of a set A of values of a given uncertain parameter Y. Such measures are mathematically defined as $Pl^Y(A) = \sum_{B \cap A \neq \emptyset} m(B)$ and $Bel^Y(A) = \sum_{B \subset A} m(B)$, respectively, and they are such that $Bel^Y(A) \leq P^Y(A) \leq Pl^Y(A)$. In concept, $m(B)$ can be thought of as the amount of likelihood that is associated with set B but without any specification of how this likelihood might be apportioned over B; thus, this likelihood might be associated with *any* subset of B. Given this conceptualization of $m(B)$, the belief

$Bel^Y(A)$ can be viewed as the *minimum* amount of likelihood that *must* be associated with A (i.e., this amount of likelihood cannot move out of A because the summation $\sum_{B \subset A} m(B)$ only involves B that satisfies $B \subset A$). Similarly, the plausibility $Pl^Y(A)$ can be viewed as the *maximum* amount of likelihood that *could* be associated with A (i.e., this amount of likelihood could move into A because the summation $\sum_{B \cap A \neq \varnothing} m(B)$ involves all B that satisfies $B \cap A \neq \varnothing$) [Dempster, 1967a and b; Shafer, 1976, 1987 and 1990; Ferson et al., 2003 and 2004; Helton et al., 2007a,b and 2010; Sentz and Ferson, 2002; Le Duy et al., 2013; Sallak et al., 2013]. For illustration purposes, let us assume that uncertain variable Y is described by the following body of evidence, $\{(A_Y^i, m(A_Y^i)): i = 1,2\}$ = $\{([0.20,0.50], 0.35), ([0.40,0.60], 0.65)\}$ (Figure 6 left). It can be interpreted as follows: input Y lies within interval (focal set) A_Y^1 = [0.20, 0.50] with probability at least equal to $m(A_Y^1) = 0.35$, whereas it lies within interval (focal set) A_Y^2 = [0.40, 0.60] with probability at least equal to $m(A_Y^2) = 0.65$. Notice that using the relations reported above, this body of evidence can be transformed into upper and lower CDFs $\overline{F}^Y(y)$ and $\underline{F}^Y(y)$ for Y (also called *cumulative plausibility* and *belief* functions, respectively): in particular, $\overline{F}^Y(y) = Pl^Y((-\infty, y]) = \sum_{A_Y^i \cap [-\infty, y] \neq \varnothing} m(A_Y^i)$ and $\underline{F}^Y(y) = Bel^Y((-\infty, y]) = \sum_{A_Y^i \subset [-\infty, y]} m(A_Y^i)$ (Figure 6 right).

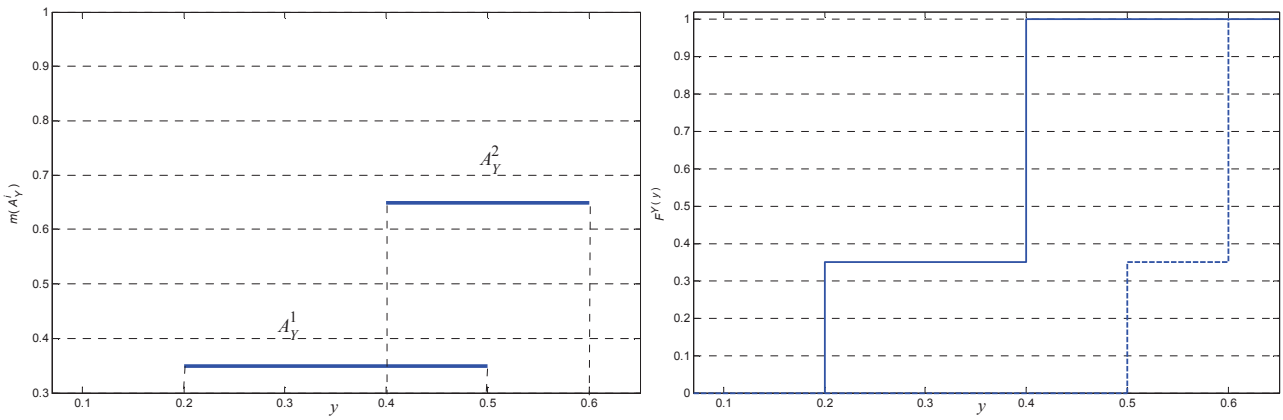


Figure 6. Exemplary body of evidence (left) and the corresponding upper and lower CDFs (i.e., cumulative plausibility and belief) (right) for a generic uncertain variable Y

For the sake of completeness and precision, it is worth pointing out that the most of the theories mentioned above (in particular, random set theory, probability bound analysis using p-boxes, interval probabilities, fuzzy probabilities and evidence theory) are 'covered' by the general common framework of *imprecise probabilities* [Beer and Ferson, 2013; Beer et al., 2013a; Blockley, 2013; Reid, 2013; Sankararaman and Mahadevan, 2013]. Actually, as highlighted above, "a key feature of imprecise probabilities is the identification of bounds on probabilities for events of interest; the

uncertainty of an event is characterized with two measure values — a lower probability and an upper probability" [Kozine and Filimonov, 2000]. The distance between the probability bounds reflects the indeterminacy in model specifications expressed as imprecision of the models and "this imprecision is the concession for not introducing artificial model assumptions" [Beer and Ferson, 2013]. Peter M. Williams developed a mathematical framework for imprecise probabilities, based on de Finetti's betting interpretation of probability [de Finetti, 1974]. This foundation was further developed independently by Vladimir P. Kuznetsov and Peter Walley (the former only published in Russian), see [Kuznetsov, 1991; Walley, 1991]. Following de Finetti's betting interpretation, the lower probability is interpreted as the maximum price for which one would be willing to buy a bet which pays 1 if an event occurs and 0 if not, and the upper probability as the minimum price for which one would be willing to sell the same bet. These references, and [Walley, 1991] in particular, provide an in-depth analysis of imprecise probabilities and their interpretations, with a link to applications to probabilistic reasoning, statistical inference and decisions. It is however also possible to interpret the lower and upper probabilities using the reference to a standard interpretation of a subjective probability: such an interpretation is indicated by [Lindley, 2006], p. 36. Consider the subjective probability $P(A)$ and say that the analyst states that his/her assigned degree of belief is greater than the urn chance of 0.10 (the degree of belief of drawing one particular ball from an urn which include 10 balls) and less than the urn chance of 0.5. The analyst is not willing to make any further judgment. Then, the interval [0.10, 0.50] can be considered an imprecision interval for the subjective probability $P(A)$. Finally, imprecise probabilities are also linked to the relative frequency interpretation of probability [Coolen and Utkin, 2007]. The simplest case reflects that the "true" frequentist probability p is in the interval $[\underline{P}(A), \overline{P}(A)]$ with certainty. More generally and in line with the above interpretations of imprecision intervals based on subjective probabilities $P(\bullet)$, a two-level uncertainty characterization can be formulated (see, e.g., [Kozine and Utkin, 2002]): $[\underline{P}(A), \overline{P}(A)]$ is an imprecision interval for the subjective probability $P(a \leq p \leq b)$ where a and b are constants. In the special case that $\underline{P}(A) = \overline{P}(A)$ (= q, say) we are led to the special case of a q•100% credibility interval for p (i.e., with subjective probability q, the true value of p is in the interval $[a, b]$). For further details, the reader is referred, e.g., to the *Special Issue on Imprecise Probabilities* recently appeared on the *Journal of Mechanical Systems and Signal Processing* [Beer and Ferson, 2013].

It is worth admitting that these imprecise probability-based theories have *not* yet been *broadly accepted* for use in the risk assessment community. Till now, the development effort made on these subjects has mostly had a mathematical orientation, and it seems fair to say that no established

framework presently exists for practical risk assessment based on these alternative theories [Aven and Zio, 2010].

6.1.2.2 Issue 2: Propagation of uncertainty to the output of the system model

The scope of the uncertainty analysis is the quantification and characterization of the uncertainty in the output Z of the mathematical model $f_Z(\boldsymbol{Y}) = f_Z(Y_1, Y_2, \ldots, Y_j, \ldots, Y_N)$ that derives from uncertainty in analysis inputs $\boldsymbol{Y} = \{Y_1, Y_2, \ldots, Y_j, \ldots, Y_N\}$ (see Section 6.1.1.1) [Helton et al., 2006]. In the light of the considerations reported in the previous Section 6.1.2.1, this requires the *joint*, *hierarchical* propagation of *hybrid* aleatory and epistemic uncertainties through the model $f_Z(\boldsymbol{Y})$ [Helton et al., 2014a, c, e; Sallaberry et al., 2014]: actually, a "two-level" setting is considered where the probability models describing random phenomena contain parameters that are known with poor precision, i.e., that are affected by epistemic uncertainty.

When both aleatory and epistemic uncertainties in a two-level framework are represented by probability distributions, a two-level (or double loop) Monte Carlo (MC) simulation is usually undertaken to accomplish this task [Cullen and Frey, 1999; Frey and Burmaster, 1999]. The approach comprises the following two main steps [Rao et al., 2007; Karanki et al., 2009; Limbourg and de Rocquigny, 2010]:

i. repeated MC sampling of the parameters affected by epistemic uncertainty from the corresponding (subjective) probability distributions (outer loop processing epistemic uncertainty);
ii. repeated MC sampling of possible values of the random variables from the corresponding aleatory probability distributions *conditioned* at the values of the epistemically-uncertain parameters sampled at step (i) above (inner loop processing aleatory uncertainty).

The resulting output Z is described by a 'bundle' of aleatory probability distributions, *one* for *each* realization of the epistemically-uncertain parameters.

Alternatively, when the epistemic uncertainties are represented by possibility distributions, the hybrid Monte Carlo (MC) and Fuzzy Interval Analysis (FIA) approach[5] is typically considered. In the hybrid MC-FIA method the MC technique [Kalos and Withlock, 1986; Zio, 2013] is combined with the extension principle of fuzzy set theory [Baraldi and Zio, 2008; Baudrit et al., 2005a,b and 2007a, b; Cooper et al., 1996; Flage et al., 2010; Guyonnet et al., 2003; Kentel and Aral, 2004 and 2007; Zadeh, 1965], within a "two-level" hierarchical setting [Baudrit et al., 2008; Kentel and Aral, 2005; Moller, 2004; Moller and Beer, 2004 and 2008; Moller et al., 2003 and 2006]. This is done by:

[5] In the following, this method will be referred to as "hybrid MC-FIA approach" for brevity.

i. FIA to process the uncertainty described by possibility distributions: in synthesis, several *intervals* for the epistemically-uncertain parameters described by possibility distributions are identified by performing a *repeated*, *level-wise* interval analysis. Technically speaking, with reference to the previous Section 6.1.2.1, several *cuts* of the possibility distribution functions are obtained for different confidence levels α;

ii. MC sampling of the random variables to process aleatory uncertainty [Baudrit et al., 2008]: for *each* interval (α-cut) of the epistemically-uncertain parameters identified at step (i) above, a *family* of (aleatory) probability distributions is generated; then, such families are propagated through the system model $f_Z(\boldsymbol{Y})$ by MC simulation.

In this approach the resulting output Z is represented by a *set* of *nested* 'bundles' of aleatory probability distributions: *one* 'bundle' is produced for *each* α-cut of the possibilistic epistemically-uncertain parameters [Baudrit et al., 2008].

Finally, if the epistemic uncertainties are described within the framework of evidence theory, the Monte Carlo (MC)-based Dempster-Shafer (DS) approach employing Independent Random Sets (IRSs)[6] is typically undertaken. In the MC-based DS-IRS method the *focal sets* (i.e., intervals) representing the epistemically-uncertain parameters are *randomly* sampled by MC according to the corresponding probability (or belief) masses [Baudrit and Dubois, 2005; Baudrit et al., 2003; Fetz, 2001; Fetz and Oberguggenberger, 2004; Helton et al., 2004, 2005, 2007a,b and 2010; Helton and Johnson, 2011; Moral and Wilson, 1996; Oberkampf and Helton, 2002; Oberkampf et al., 2001; Tonon, 2004; Tonon et al., 2000a and b]. As for the double-loop MC, the result is a 'family' of aleatory probability distributions: *one* family is generated for *each* random *combination* of the focal sets representing the epistemically-uncertain parameters.

6.1.2.3 Issue 3: Updating as new information becomes available

In this Section, we address the issue of updating the representation of the epistemically-uncertain parameters of aleatory models (e.g., probability distributions), as *new* information/evidence (e.g., data) about the system becomes available.

The framework adopted for this is the typical Bayesian one that is based on the well-known Bayes rule when epistemic uncertainties are represented by (subjective) probability distributions [Bernardo and Smith, 1994; Siu and Kelly, 1998; Lindley, 2000; Bedford and Cooke, 2001; Atwood et al., 2003; Kelly and Smith, 2009 and 2011; Pasanisi et al., 2012].

Alternatively, when the representation of epistemic uncertainty is non-probabilistic, other methods of literature can be undertaken [Ferson, 2005]. In [Smets, 1993], a Generalized Bayes Theorem

[6] In the following, this method will be referred to as "MC-based DS-IRS approach" for brevity.

(GBT) has been proposed within the framework of evidence theory and applied by [Le-Duy et al., 2011] to update the estimates of the failure rates of mechanical components in the context of nuclear Probabilistic Risk Assessment (PRA). In [Viertl, 1996, 1997, 1999, 2008a, b and 2011; Viertl and Hareter, 2004a, b; Viertl and Hule, 1991], a modification of Bayes theorem has been presented to account for the presence of fuzzy data and fuzzy prior Probability Distribution Functions (PDFs). In [Dubois and Prade, 1997; Lapointe and Bobee, 2000], a purely possibilistic counterpart of the classical, well-grounded probabilistic Bayes theorem has been proposed to update the possibilistic representation of the epistemically-uncertain parameters of (aleatory) probability distributions: this requires the construction of a possibilistic likelihood function, which is used to revise the prior possibility distributions of the uncertain parameters (determined, as usual, on the basis of a priori subjective knowledge and/or data). Finally, [Beer, 2009a; Stein and Beer, 2011; Stein et al., 2013; Beer et al., 2014a] have introduced a hybrid probabilistic-fuzzy method that relies on the use of Fuzzy Probability Density Functions (FPDFs), i.e., PDFs with fuzzy parameters (e.g., fuzzy means, fuzzy standard deviations, etc.). Similarly to the MC-FIA approach for hybrid uncertainty propagation (Section 6.1.2.2), it is based on the combination of: (i) Fuzzy Interval Analysis (FIA) to process the uncertainty described by fuzzy numbers and (ii) repeated Bayesian updating of the uncertainty represented by (classical) probability distributions. This way of proceeding results in *nested families* of (probabilistic) posteriors for the epistemic parameters of interest: by resorting to the rules of possibility theory (see Section 6.1.2.1), such nested families can be finally synthesized into a *single* (posterior) possibility distribution function.

6.1.2.4 Issue 4: Dependences among input variables and parameters

Two types of dependence need to be considered in reliability analysis and risk assessment [Ferson et al., 2004]. The first type relates to the (dependent) *occurrence* of different (random) events (in the following, this kind of dependence will be referred to as ‘objective’ or ‘aleatory’). An example of this objective (aleatory) dependence may be represented by the occurrence of multiple failures which result directly from a common or shared root cause (e.g., extreme environmental conditions, failure of a piece of hardware external to the system, or a human error): they are termed Common Cause Failures (CCFs) and typically can concern identical components in redundant trains of a safety system [USNRC, 1993, 2007 and 2009; Zio, 2009]; another example is that of cascading failures, i.e., multiple failures initiated by the failure of one component in the system, as a sort of chain reaction or domino effect [Guimera et al., 2002; Watts, 2002; Sansavini et al., 2009; Zio and Sansavini, 2011a and b].

The second type refers to the dependence possibly existing between the *estimates* of the epistemically-uncertain *parameters* of the aleatory probability models used to describe random

events/variables (in the following, this kind of dependence will be referred to as 'state-of-knowledge' or 'epistemic'). This state-of-knowledge (epistemic) dependence exists when the epistemically-uncertain *parameters* of aleatory models are estimated by resorting to dependent *information sources* (e.g., to the same experts/observers or to correlated data sets) [Apostolakis and Kaplan, 1981; USNRC, 2009]. By way of example, consider the case of a system containing a number of *physically distinct*, but *similar/nominally identical* components whose failure rates are estimated by means of the *same data set*: in such situation, the *state of knowledge* about these failure rates is exactly the *same* and, thus, the distributions describing the epistemic uncertainty associated to such failure rates have to be considered *totally (perfectly) dependent*[7].

Considerable efforts have been done to address objective and state-of-knowledge dependences in risk analysis. In [Vaurio, 2002 and 2007; Karanki and Dang, 2010], objective dependencies among random events/variables have been treated by means of alpha factor models within the traditional framework of Common Cause Failure (CCF) analysis. In [Ferson et al., 2004; Sadiq et al., 2008], the use of Frank copula and Pearson correlation coefficient has been proposed to describe a wide range of objective dependences among aleatory events/variables. In [Li, 2007; Ferdous et al., 2011], (fuzzy) dependency factors are employed to model dependent events/variables. In [Iman and Conover, 1982; Iman and Davenport, 1982], the rank correlation method has been proposed to characterize dependencies between epistemically uncertain variables. In [Apostolakis and Kaplan, 1981; USNRC, 2009], total (perfect) state-of-knowledge dependence among the failure rates of mechanical components has been modeled by imposing maximal correlation among the corresponding (subjective) probability distributions. In [Zhang, 1989 and 1993; Rushdi and Kafrawy, 1988; Kafrawy and Rushdi, 1990], state-of-knowledge dependences among the probabilities of the Basic Events (BEs) of a Fault Tree (FT) have been described by traditional correlation coefficients and propagated by the method of moments. In [Karanki and Dang, 2010; Karanki et al., 2010], statistical epistemic correlations have been modeled by resorting to the Nataf transformation [Huang and Du, 2006] within a traditional Monte Carlo Simulation (MCS) framework. In [Karanki et al., 2009], the Dependency Bound Convolution (DBC) approach [Ferson et al., 2004; Regan et al., 2004; Williamson and Downs, 1989] has been adopted to account for all

[7] As stated in [USNRC, 2009], Page 54, "an analyst's state of knowledge about the possible values of a parameter θ can be expressed in terms of a probability density function $f^{\theta}(\theta)$ when using Bayesian updating or expert judgment. It is common practice to assign the same value to the parameters of BEs of identical or similar components. Therefore, for example, the probability of failure of a class of identical motor-operated valves (MOVs) to open is considered the same. Suppose that θ_1 and θ_2 represent the parameters of two physically distinct but identical MOVs: because this discussion assumes that all such MOVs have the *same* parameter, it is necessary to set $\theta_1 = \theta_2$. Moreover, because the analyst's state of knowledge is the same for the two valves, it follows that $f^{\theta_1}(\theta_1) = f^{\theta_2}(\theta_2)$. Thus, $f^{\theta_1}(\theta_1)$ and $f^{\theta_2}(\theta_2)$ must be regarded as being equal probability density functions and treated as completely dependent probability density functions".

kinds of (possibly unknown) objective and epistemic dependences among the BEs of a FT. Finally, the Distribution Envelop Determination (DEnv) method has been proposed by [Berleant and Goodman-Strauss, 1998; Berleant and Zhang, 2004a, b; Berleant et al., 2003 and 2008] to model unknown dependences between correlated uncertain variables.

6.1.3 Research developed: methodological and applicative contributions

In this Section, the research developed in the present thesis within the fields of uncertainty modeling and quantification (Axis 1) is synthetically overviewed. In particular: (i) the methodological and applicative contributions of my research activity to the four challenges presented before are summarized; (ii) on the basis of the critical literature survey reported in Section 6.1.2 and of the research results obtained so far, specific techniques are recommended for tackling each of the four issues: precise guidelines on the recommended use of the techniques in practical reliability analysis and risk assessment are finally provided.

In the presentation of these contributions and recommendations, reference will be made only to the most relevant works (mainly journal papers) realized by the candidate and his collaborators, within the PhD and Master theses activities.

6.1.3.1 Issue 1: Quantitative modeling and representation of uncertainty coherently with the information available on the system

As highlighted in Section 6.1.2.1, numerous imprecise probability-based theories have been recently introduced for uncertainty quantification: however, they have not yet been broadly accepted for use in the risk assessment community. Till now, the development effort made on these subjects has mostly had a mathematical orientation: thus, no established framework presently exists for practical risk assessment based on these alternative theories [Aven and Zio, 2010]. In this context, the primary objective of my research has been to assess the capabilities of these novel (non-fully probabilistic) techniques with respect to classical purely probabilistic approaches, in reliability and risk analysis applications.

In [Pedroni and Zio, 2012; Pedroni et al., 2013a], we have systematically *compared* the effects of the probabilistic and non-probabilistic *representations* of the epistemically-uncertain parameters of (aleatory) probability distributions in a “two-level” uncertainty modeling framework. In the comparisons, several non-probabilistic approaches have been considered for the description of epistemic uncertainty (including intervals, probability boxes, Dempster-Shafer structures, possibility distributions and fuzzy numbers). These analyses have been carried out with reference to different risk assessment problems, in particular: (i) examples involving straightforward analytical functions, to keep the analysis simple and retain a clear view of each step of the comparison

[Pedroni and Zio, 2012]; (ii) a model for the risk-based design of a flood protection dike [Pedroni et al., 2013a] (Paper I in the Appendix). In each case study different numerical indicators (e.g., cumulative distributions, exceedance probabilities, quantiles, etc.) have been considered to perform a fair and quantitative comparison between the approaches and evaluate their rationale and appropriateness in relation to risk assessment. With respect to that, it is worth mentioning that the "driving criterion" chosen to assess and compare the approaches has been the "*conservatism*" of the results (i.e., of the risk estimates) produced by them. The motivation has been the acknowledgement that being conservative represents an advantage in decision making processes related to the risk assessment of complex, safety-critical components, systems and infrastructures, in particular when the information available on these systems is scarce and/or imprecise: in such cases, being conservative allows to be *"safely"-coherent* with the (scarce and/or imprecise) information available and, thus, to take more reliable and robust decisions.

The comparisons have shown that in general *different* results are obtained in correspondence of *different* representations of epistemic uncertainty. As a consequence, embracing one approach or another may change the outcome of a decision making process based on a risk assessment involving uncertainties. In more detail, non-probabilistic representations of epistemic uncertainty have been shown produce *more conservative* results than a probabilistic one in the presence of scarce, vague and/or imprecise information. In particular, the results have highlighted that selecting a *single*, *precise* probability model to describe a critical random variable of interest without the support of proper experimental evidence may lead to *significant underestimations* of risk: for example, the 95-th quantile of that variable could be underestimated even by a factor 5-10 (see also papers by [Baraldi et al., 2012; Pedroni et al., 2012] for additional quantitative examples of this statement in risk assessment applications). Thus, making *inappropriately precise* assumptions represents a dangerous behavior in decision making processes related to the risk assessment of complex, safety-critical components, systems and infrastructures under uncertainties. These considerations and results can lead to the recommendation of using non-probabilistic representations of epistemic uncertainty in engineering risk assessment, to be "safely" coherent with the (possibly scarce and imprecise) information available.

In more detail, on the basis of the results obtained from the comparisons mentioned above the Fuzzy Random Variable (FRV) approach is recommended for uncertainty modeling and representation [Baudrit et al., 2008]. In such a framework, aleatory uncertainty is classically represented by *probability* models (e.g., probability distributions), whereas epistemic uncertainty in the internal parameters of the aleatory models is described by *possibility* distributions (or fuzzy numbers). This recommendation is motivated by the following facts. First, a possibility function

defines a *family* of probability distributions (see Section 6.1.2.1): this allows describing, in a *faithful* and *objective* way, those situations where the knowledge available does *not* enable to precisely assign a *single* (subjective) probability distribution to an epistemically-uncertain parameter. Second, possibility theory is strongly connected with fuzzy sets and fuzzy logic, as conceptualized and put forward by [Zadeh, 1978]: actually, in his original view possibility distributions were meant to provide a graded semantics to *natural language statements*, which makes them particularly suitable for quantitatively translating (possibly vague, qualitative and imprecise) *expert opinions*. Finally, a possibility distribution also defines a *set* of *nested confidence intervals* for the parameter of interest (see Section 6.1.2.1). Correspondingly, it can be argued that a FRV defines a *set* of *nested* (aleatory) probability models, each of which *contains* the "true" probability model with a given *confidence level* (1 – α). Figure 7 shows an example of FRV. Variable Y is described by a Normal (aleatory) probability distribution with known standard deviation $\sigma = 100$ and epistemically-uncertain mean μ represented by the possibility function $\pi^{\mu}(\mu)$ of Figure 7, left. For each possibility (resp., confidence) level α (resp., 1 – α) in [0, 1], a *family* of CDFs for Y, namely $\{F^Y(y \mid \mu, \sigma)\}_\alpha$, can be constructed by letting μ range within A_α^μ, i.e., $\{F^Y(y \mid \mu, \sigma)\}_\alpha = \{F^Y(y \mid \mu, \sigma) : \mu \in A_\alpha^\mu, \sigma = 100\}$ (i.e., *different* Normal CDFs for Y are obtained in correspondence of the *different* values that the mean μ can assume within the interval A_α^μ). This family of CDFs (of level α) is bounded above and below by the upper and lower CDFs, $\overline{F}_\alpha^Y(y)$ and $\underline{F}_\alpha^Y(y)$, defined as $\overline{F}_\alpha^Y(y) = \sup_{\mu \in A_\alpha^\mu} \{F^Y(y \mid \mu, \sigma = 100)\}$ and $\underline{F}_\alpha^Y(y) = \inf_{\mu \in A_\alpha^\mu} \{F^Y(y \mid \mu, \sigma = 100)\}$, respectively. This *set* of *nested pairs* of CDFs $\{(\underline{F}_\alpha^Y(y), \overline{F}_\alpha^Y(y)) : 0 \le \alpha \le 1\}$ bounds the "true" CDF $F^Y(y)$ of Y with confidence larger than or equal to (1 – α), i.e., $P[\underline{F}_\alpha^Y(y) \le F^Y(y) \le \overline{F}_\alpha^Y(y)] \ge 1 - \alpha$, with $0 \le \alpha \le 1$ [Baudrit et al., 2008]. For illustration purposes, Figure 7 right shows the bounding upper and lower CDFs of Y, $\overline{F}_\alpha^Y(y)$ and $\underline{F}_\alpha^Y(y)$, built in correspondence of the α-cuts of level $\alpha = 0$ (solid lines), 0.5 (dashed lines) and 1 (dot-dashed line) of the possibility distribution $\pi^{\mu}(\mu)$ of parameter μ (Figure 7, left). For further technical details the interested reader is referred to Paper I [Pedroni et al., 2013a] reported in the Appendix.

Finally, notice that the works [Baraldi et al., 2012; Pedroni et al., 2013a] under this research line have been done mainly within the Master thesis of Elisa Ferrario (M.Sc. 1 in Section 4.3).

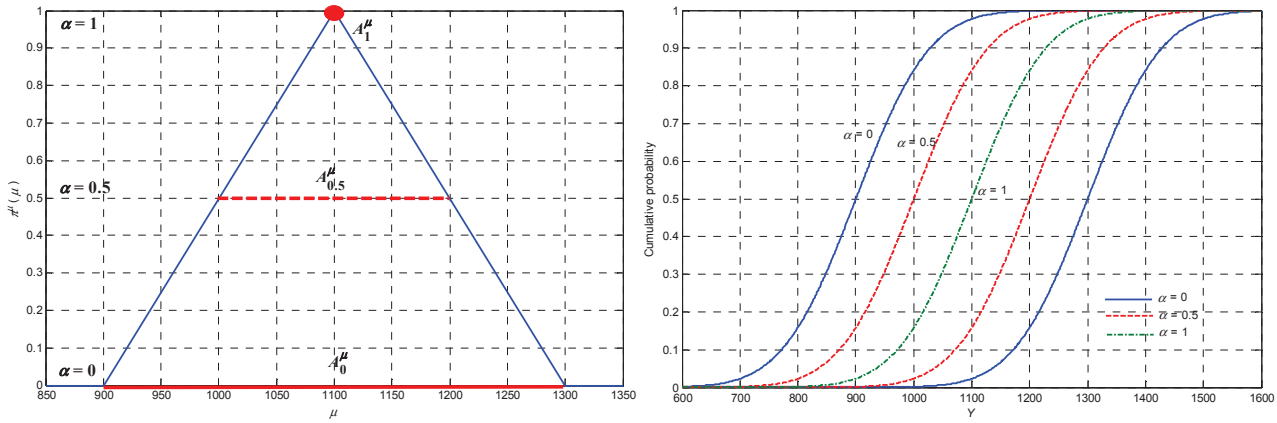


Figure 7. Exemplary Fuzzy Random Variable (FRV). Left: possibility function $\pi^{\mu}(\mu)$ for the mean μ of variable Y. Right: bounding upper and lower CDFs of Y, $\overline{F}_{\alpha}^{Y}(y)$ and $\underline{F}_{\alpha}^{Y}(y)$, built in correspondence of the α-cuts of level α = 0 (solid lines), 0.5 (dashed lines) and 1 (dot-dashed line) of $\pi^{\mu}(\mu)$

A pictorial representation of the methods considered and compared to address Issue 1 of research Axis 1 is given in Figure 8, together with the corresponding applications and recommended approaches.

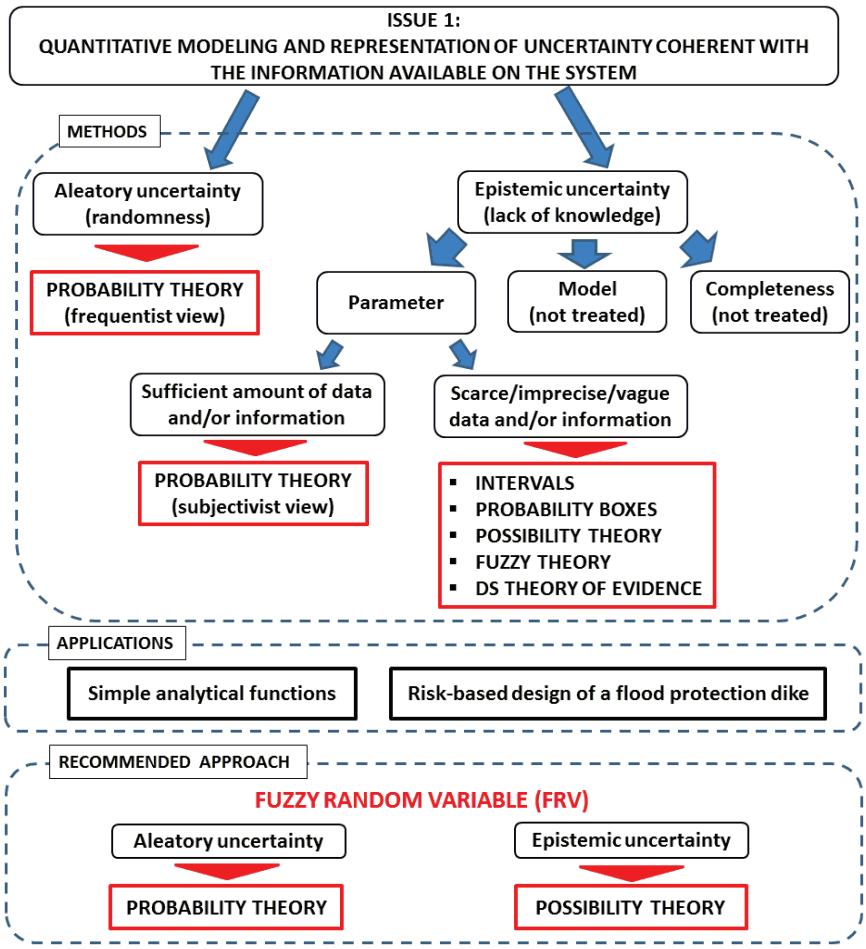


Figure 8. Methods here considered and compared to address Issue 1 of research Axis 1, together with the corresponding applications and recommended approaches

6.1.3.2 Issue 2: Propagation of uncertainty to the output of the system model

In [Baraldi et al., 2012; Pedroni et al., 2012; Pedroni and Zio, 2012; Pedroni et al., 2013a], we have *compared* different techniques for the propagation of uncertainty from the inputs to the output of a system model in a "two-level" setting. In the comparisons, *different* approaches have been considered in correspondence of *different* frameworks adopted for representing epistemic uncertainty (including double-loop MC, interval analysis, MC-based DS-IRS and MC-FIA techniques). The same case studies mentioned in Section 6.1.3.1 have been considered in the comparisons. By way of example, in the application concerning the risk-based design of a flood protection dike [Pedroni et al., 2013a] the output of interest is represented by the yearly maximal water level of a river in proximity of a residential area. It is computed as a function of four inputs, namely the yearly maximal water flow, the upstream and downstream riverbed levels and the Strickler friction coefficient between the river water and the riverbed.

The results have shown that the choice of the uncertainty propagation method is *not* so *critical* (in risk-informed decisions) *only* when the objective of the analysis is the computation of a couple of *extreme bounding* upper and lower CDFs (i.e., a probability box) for the model output of interest: actually, in this case the curves produced by the double MC, hybrid MC-FIA and the MC-based DS-IRS approaches are *almost identical*. However, the analysis of other relevant quantitative indicators (e.g., a given *quantile* of the model output) shows that the hybrid MC-FIA method produces *more conservative* and more reliable results than the double-loop MC and the MC-based DS-IRS approaches. In addition, this higher conservatism is particularly evident in the range of *extreme* probabilities (i.e., around 0 and 1) and quantiles that are of paramount importance in realistic risk assessment applications involving *highly reliable* engineering components, systems and infrastructures. For example, it has been shown that in several situations the choice of double-loop MC or MC-based DS-IRS can lead to serious underestimations (e.g., up to 36%) of the values of high (e.g., 95-th, 99-th, etc.) quantiles of the model output. These findings and considerations confirm the recommendation of adopting the hybrid MC-FIA approach for uncertainty propagation in a "two-level" framework. For further technical details the interested reader is still referred to Paper I [Pedroni et al., 2013a] reported in the Appendix.

A pictorial representation of the here considered and compared to address Issue 2 of research Axis 1 is given in Figure 9, together with the corresponding applications and recommended approaches.

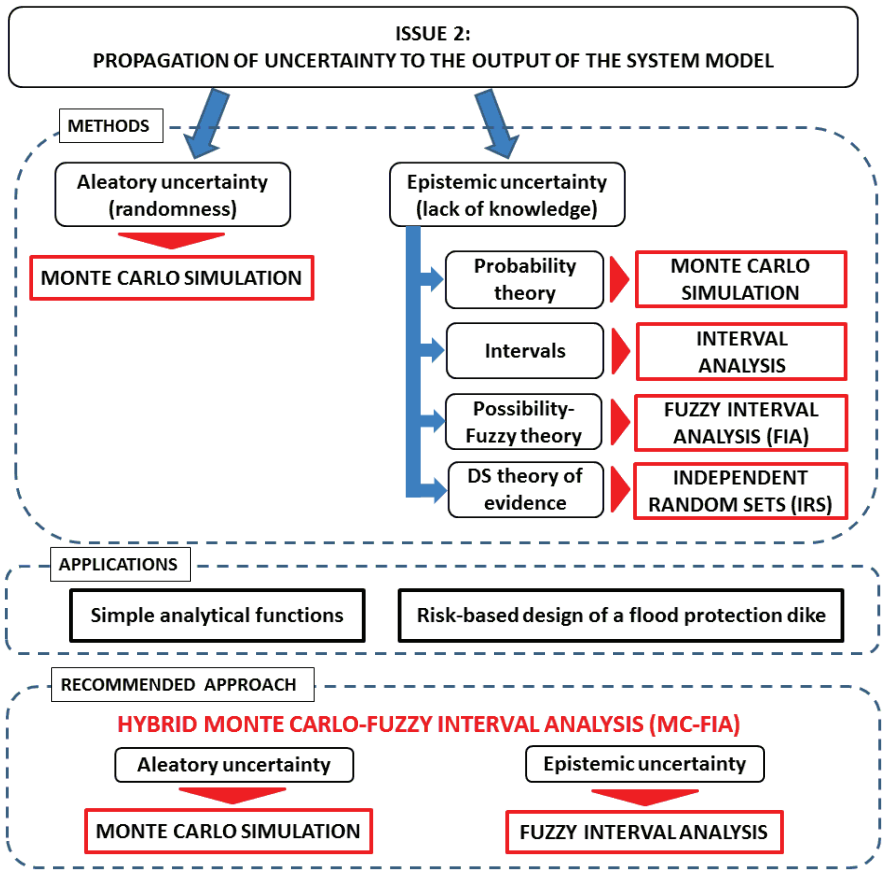


Figure 9. Methods here considered and compared to address Issue 2 of research Axis 1, together with the corresponding applications and recommended approaches

6.1.3.3 Issue 3: Updating as new information becomes available

Coherently with the recommendations provided in Section 6.1.3.1, in [Pedroni et al., 2015] we have adopted possibility distributions to describe epistemic uncertainty and have addressed the issue of updating, in a Bayesian framework, the *possibilistic* representation of the epistemically-uncertain parameters of (aleatory) probability distributions by means of *data*.

We have considered two approaches of literature (see Section 6.1.2.3): the first is based on the purely possibilistic Bayes' theorem by [Dubois and Prade, 1997; Lapointe and Bobee, 2000]; the second is represented by the hybrid (probabilistic and possibilistic) method proposed by [Beer, 2009a; Stein and Beer, 2011; Stein et al., 2013; Beer et al., 2014a]. The objective (and the main contribution of the paper) has been to systematically *compare* the effectiveness of the two methods. To keep the analysis simple and retain a clear view of each step, the investigations have been carried out with respect to a literature case study involving the risk-based design of a flood protection dike.

The findings of the work have shown that in general adopting different methods may generate different results and possibly different decisions in risk problems involving uncertainties: this is of paramount importance in systems that are critical from the safety viewpoint, e.g., in the civil, nuclear, aerospace, chemical and environmental fields. In particular, on the basis of the results

obtained, it seems advisable to suggest the use of the purely possibilistic approach (instead of the hybrid one) for the following reasons:

i. its *strength* in reducing epistemic uncertainty is significantly *higher*, in particular when the amount of available data is *small* (e.g., when only 5-10 pieces of data have been collected): this is important in decision making processes since reducing epistemic uncertainty significantly *increases* the analyst *confidence* in the decisions;
ii. the computational *time* required is consistently *lower* (even by 2-3 orders of magnitude).

In the light of these findings and results, the purely possibilistic approach has been applied by the candidate and some of his collaborators also for updating the epistemic uncertainty in the parameters of the Event Tree (ET) and Fault Tree (FT) models used in the Seismic Probabilistic Risk Assessment (SPRA) of Nuclear Power Plants (NPPs) [Lo et al., 2014a and b].

However, it has to be remarked that the construction of a possibilistic likelihood required by the purely possibilistic method, although recently tacked in the literature [Denoeux, 2014], still represents an issue to be *further* investigated from both the theoretical and practical viewpoint in order to avoid introducing biases in the analysis and to suggest the application of the approach for real risk assessment problems. With respect to that, future research should be devoted to the investigation of additional methods developed to this aim: see, e.g., [Masson and Denoeux, 2006; Mauris, 2008; Hou and Yang, 2010; Serrurier and Prade, 2011].

Finally, in [Pedroni and Zio, 2015b] we have introduced a *novel* approach for updating, by means of data, the epistemic uncertainty in the non-probabilistic (interval-valued) parameters of the aleatory probability distributions of random variables. It is worth mentioning that this method has been developed in response to the Multidisciplinary Uncertainty Quantification Challenge (MUQC) proposed by the NASA Langley Research Center (LaRC) [Crespo et al., 2014]. In the developed approach, first a p-box for the random variable of interest is built by means of the empirical data available: to this aim, a non-parametric approach based on the well-known Kolmogorov-Smirnov (KS) confidence limits has been considered [Ferson and Tucker, 2006; Ferson et al., 2003, 2007 and 2010]. Then, the updated (i.e., reduced) intervals of the epistemically-uncertain parameters are optimally determined as those that do *not* "contradict" the experimental evidence available: in practice, we retain *only* those parameter values that produce aleatory probability distributions which are "*contained*" within the KS bounds constructed on the basis of data. This method (originally developed for updating interval-valued parameters) can be easily *extended* to possibilistic parameters: actually, it can be repeatedly applied to *each* α-cut interval of a possibility function.

Finally, notice that the works [Lo et al., 2014a and b] under this research line have been done mainly within the Ph.D. thesis of Chung-Kung Lo (Ph.D. 4 in Section 4.3).

A pictorial representation of the here considered and compared to address Issue 3 of research Axis 1 is given in Figure 10, together with the corresponding applications and recommended approaches.

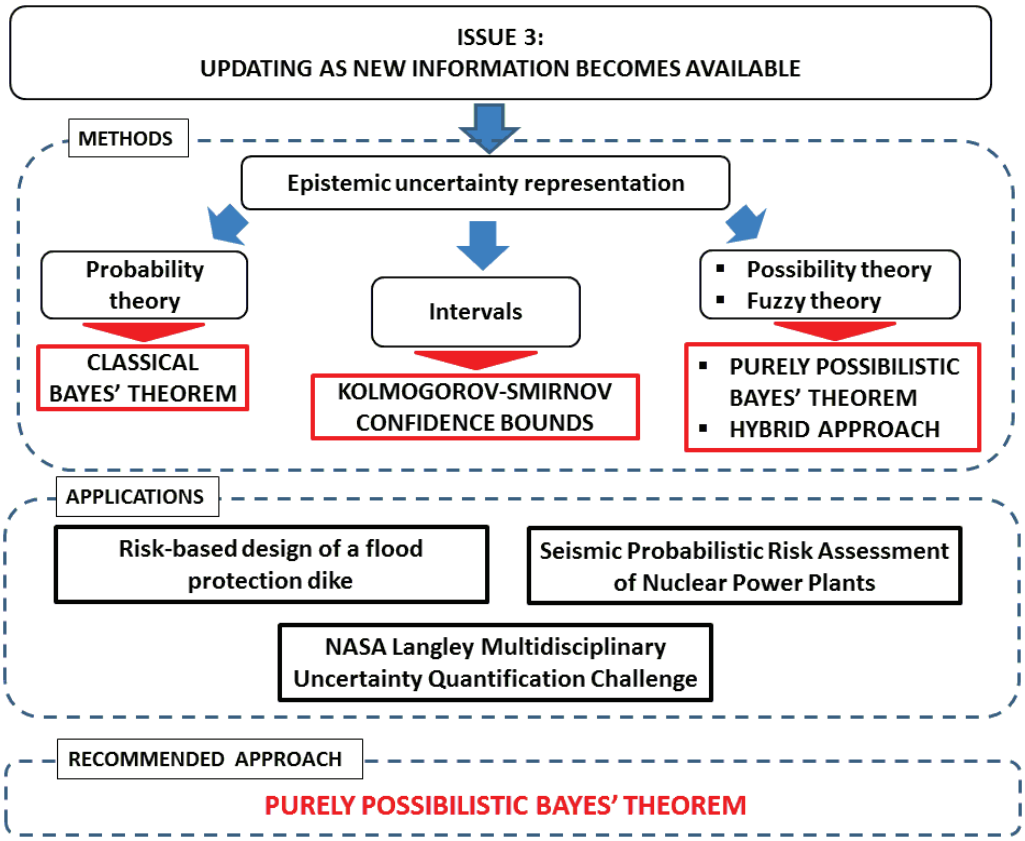


Figure 10. Methods here considered and compared to address Issue 3 of research Axis 1, together with the corresponding applications and recommended approaches

6.1.3.4 Issue 4: Dependences among input variables and parameters

In [Pedroni and Zio, 2013] (Paper II in the Appendix), we have systematically analyzed and quantified the effects of objective (aleatory) and state-of-knowledge (epistemic) dependences between the Basic Events (BEs) of a Fault Tree (FT) on the Top Event (TE) probability. In more details, the following analyses have been performed:

i. the study of the *effects* of different states of *objective dependence* between the BEs, when the state of *epistemic dependence* between the BE probabilities is *defined* (in particular, the states of independence and of perfect, opposite, positive, negative and unknown objective dependence have been explored);

ii. the study of the *effects* of different states of *epistemic dependence* between the BE probabilities when the state of *objective dependence* between the BEs is *given* (in particular,

the states of independence and of perfect and unknown epistemic dependence have been considered).

To keep the analysis simple and thus retain a clear view of each step, the investigations have been carried out with respect to an example involving a FT with six BEs; different numerical indicators (e.g., exceedance probabilities, quantiles, etc.) have been considered to perform a fair and quantitative comparison between different states of objective and epistemic dependence and evaluate their effects on the TE probability.

The results have shown that:

i. the treatment of objective dependences among random BEs is *very critical* since they have a *dramatic impact* on the system risk measure (i.e., the TE probability), in particular if the corresponding BE probabilities are *small* (e.g., of the order of 10^{-3}–10^{-2}): this poses serious concerns in the risk assessment of complex, safety-critical systems where the components are *highly reliable* and, thus, characterized by very small failure probabilities. For example, neglecting a state of positive objective dependence between two BEs (i.e., the occurrence of one event favors the occurrence of the other) could lead to *underestimating* the TE probability even by 1-2 *orders of magnitude*. In this view, in absence of precise information, for the sake of conservatism *unknown* (or, at least, *positive*) objective dependence should be assumed among random events;

ii. the conditions of epistemic dependence should *not* be *neglected*, in particular when *small probabilities* and *extreme quantiles* have to be estimated: for example, neglecting the state of perfect epistemic correlation between two BE probabilities could lead to underestimating the TE probability by a factor 1.5-2. With respect to that, in absence of precise information, *unknown* (or, at least, *perfect*) epistemic dependences should be assumed in order to obtain conservative estimates of the TE probability. On the other hand, notice that if objective dependences are *also* present, the effects of epistemic dependence are likely to be *overwhelmed* by those of objective dependence, since they are *quantitatively less relevant* and *critical*.

In the light of these results, for the sake of *conservatism*, the use of Fréchet bounds [Ferson et al., 2004; Fréchet, 1935; Frank et al., 1987; Sadiq et al., 2008] and of the Distribution Envelop Determination (DEnv) [Berleant and Goodman-Strauss, 1998; Berleant and Zhang, 2004a, b; Berleant et al., 2003 and 2008] methods is strongly recommended to account for *all* kinds of (possibly *unknown*) objective and epistemic dependences, respectively. For further technical details the interested reader is referred to Paper II [Pedroni and Zio, 2013] reported in the Appendix.

A pictorial representation of the methods here considered and compared to address Issue 4 of research Axis 1 is given in Figure 11, together with the corresponding applications and recommended approaches.

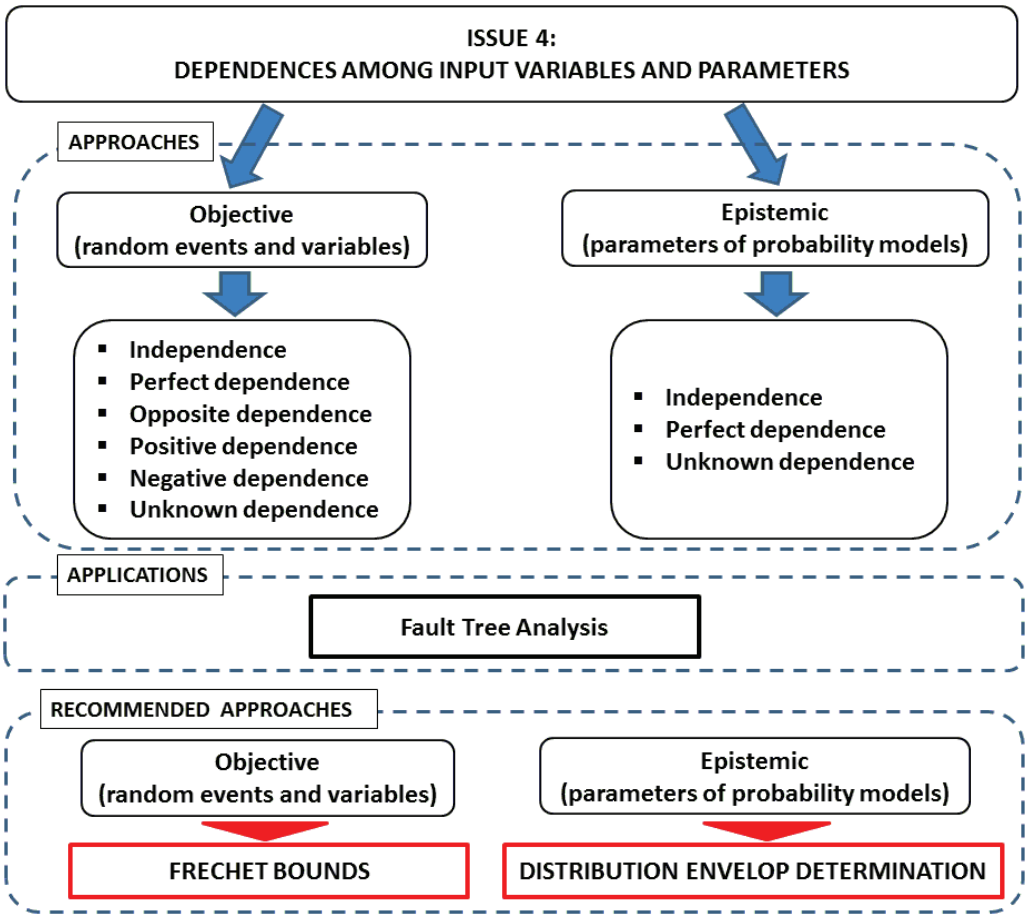


Figure 11. Methods here considered and compared to address Issue 4 of research Axis 1, together with the corresponding applications and recommended approaches

As a closing comment, it is important to notice that although in most of the analyses above conservatism has been evoked as the main criterion of comparisons, we do *not* intend to *overstate* the benefits of conservatism *in itself*. Actually, (i) being conservative just for the sake of conservatism can lead to misallocation of resources; (ii) excessive conservatism can bring the results of an entire analysis into question, as it makes the analysts appear to lack appropriate understanding of the problem under consideration (of course, the same holds for analyses based on inappropriately precise assumptions); (iii) there may be situations where a conservative assumption affecting one result in an analysis turns out to be a non-conservative assumption with respect to another result of the same analysis. Overly conservative assumptions can be as damaging to good decision making as overly optimistic assumptions (i.e., not objectively "anchored" to the available information). In an analysis performed to support an important decision, the appropriate goal is to be neither overly optimistic nor overly pessimistic in the assumptions used, but rather to provide a

full, *objective* and *faithful* description of the uncertainties that are present in the analysis and its results (actually, this is the main, driving reason for resorting to non-probabilistic approaches).

6.2 Axis 2 – Safety-Critical Systems and Infrastructures: Advanced Methods for Modeling, Simulation and Analysis Considering Uncertainties

This Section provides a complete overview on the research activities carried out under Axis 2. It starts by analyzing the problems to be addressed when assessing the risk, vulnerability and resilience of complex safety-critical systems and infrastructures in the presence of uncertainties (Section 6.2.1); then, it points out some conceptual and practical research issues associated to the modeling, simulation and analysis of their behavior and it critically surveys the corresponding possible solution approaches (Section 6.2.2); finally, it briefly summarizes the methodological and applicative contributions of the present work to each of the issues addressed (Section 6.2.3).

6.2.1 Problem statement

In Section 6.2.1.1, we synthetically summarize the main features of complex safety-critical systems and infrastructures and point out why these characteristics pose problems with respect to the assessment of relevant quantities, such as their associated risk, vulnerability and resilience (defined in the following Section 6.2.1.2).

6.2.1.1 Safety-Critical Systems and Infrastructures

Safety-critical industrial systems (e.g., nuclear and chemical plants) and infrastructures (e.g., civil, transportation, electric power, water, gas and communication systems) are *complex* systems composed by a *multitude* and *variety* of *heterogeneous* 'elements', that is, physical hard components (e.g., road, railway, pipelines, pumps, etc.), soft components (e.g., SCADA, information and telecommunication systems) and human and organizational components. The welfare of modern society relies on the continuous operation of such systems and infrastructures that are essential in providing goods (such as energy, water, data) and services (such as transportation, banking and health care) across local, regional and national boundaries [Gheorghe and Schlapfer, 2006; Kröger and Zio, 2011].

These systems and infrastructures are getting more and more *automated*, highly *interconnected* and mutually *dependent* in *complex* ways, due to their increasing *extension* on *large scales* and the progressive advances in *Information and Communication Technology (ICT)*. For example, "today's ability to run largely distributed power networks with a variety of generation technologies, e.g., nuclear, thermo, hydro etc., is only possible through the intense use of information and

communication systems" [Gheorghe and Schlapfer, 2006]. These elements lead to significant *structural complexity*.

In addition, these systems and infrastructures also present a considerable *dynamic complexity*:

i. they *evolve* and *adapt* themselves responding to environmental changes to continue providing for their functionality. Actually, *self-organization* and *adaptive learning* are dynamic properties of complex systems, which allow them to adjust its architecture and behavior into a stable coherent pattern under external pressures, using long-term memory experience feedback to anticipate future unfavorable changes in system functioning [NECSI 2005]. In the electric power grid, for example, adaptive learning is a challenge-response property, which results from the trade-off between consumer involvement and control by the central authority in the energy management process: on one side, intense consumer involvement can initiate chaotic behavior in the electrical system; on the opposite side, strong control by the central authority renders the system rigid, missing opportunities for service efficiency and for exercising system resilience and adaptation capacity.

ii. they show *emergent* behavior. Indeed, the *overall*, "*macro*" behavior emerges from the *interactions* among *single parts* of a complex system: in other words, *synergies* emerge from the interactions among these components and the whole critical system or infrastructure is more than the sum of its parts [Seth, 2008]. Electric power grids have also shown emergent behavior in the past, where local failures have evolved into unexpected cascade failure patterns with transnational, cross-industry effects.

What emerges from the considerations above is the typical construct of a System of Systems (SoS), in which the systems forming the collaborative set of the SoS fulfill their purposes and are managed for their own purposes and the purposes of the whole SoS [Eusgeld et al. 2011; Zio and Sansavini 2011b]. On one hand, these advanced, complex and dynamic configurations have *increased* the *efficiency* of such systems and infrastructures (e.g., the massive use of ICT systems provides better measurements, allows quicker operations, more powerful control schemes and broad access to data [Gheorghe and Schlapfer, 2006]); on the other hand, they have created *new vulnerabilities* to component failures, natural and manmade events. For example, recent incidents have shown that ICT systems can be vulnerable to cyber-attacks and that such attacks can lead to disruption of physical systems and networks [Peng et al., 2013; Netkachov et al., 2014]. In addition, a failure in *one* critical system or infrastructure can propagate to the *others*, possibly provoking (*cascading*) *failures* that generate *large consequences* well beyond the initial impact zone [Weron and Simonsen, 2006; Hines et al., 2009; Helbing, 2013]. Moreover, such failures may be triggered by *multiple* and *diverse* sources of *hazards* associated to exogenous and endogenous stressors that may

target the *various heterogeneous* parts of the complex system: e.g., natural events, terrorism, criminal activities, malicious behavior, market and policy factors, human factors and technical random failures of hard components [Amin, 2001; Zio, 2009].

Finally, such complex systems are affected by large *uncertainties* in the characterization of the failure and recovery behavior of their components, their interconnections and interactions: this makes the corresponding analysis a challenging task, because it requires to quantify the uncertainty and to predict how it propagates throughout the system [Apostolakis, 1990; Helton and Pilch, 2011; Aven and Zio, 2010; Zio and Aven, 2011].

In summary, the safety-critical systems and infrastructures of interest to the present dissertation show several common characteristics (Figure 12) that make them:

i. difficult to model and analyze: as Zio (2007) and Kröger (2008) point out, in order to address the structural and dynamic complexities of these systems under uncertainties, new methods for their modeling, simulation and analysis are needed, since "…the current quantitative methods of risk, vulnerability and resilience analysis seem not to be fully equipped to deal with the level of complexity inherent in such systems" [Zio, 2007, p. 505];
ii. difficult to control or operate reliably and efficiently [Amin, 2001], which raises concerns with respect to the *risk*, *vulnerability* and *resilience* properties characterizing such systems.

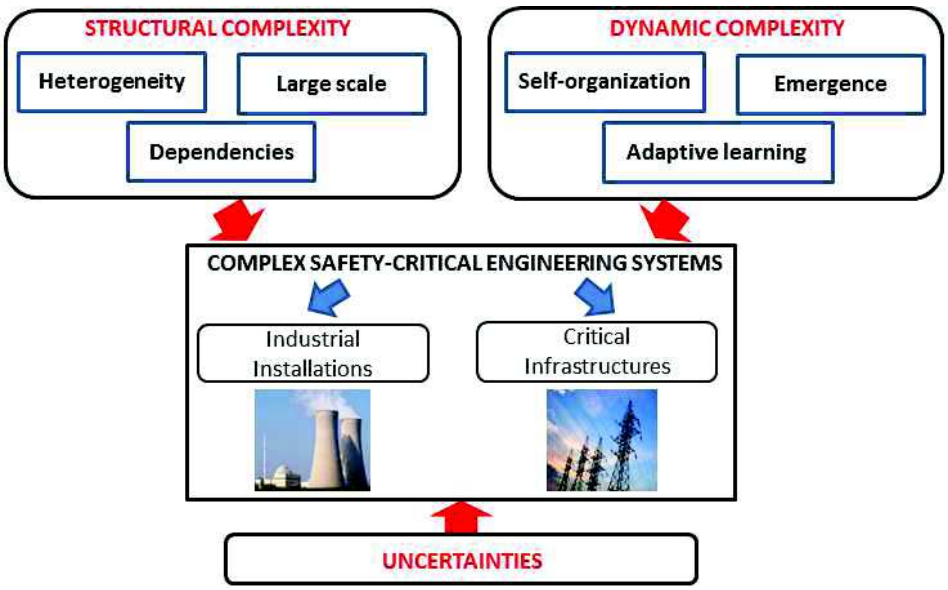


Figure 12. Main characteristics of the safety-critical systems and infrastructures of interest to the present dissertation, and the corresponding related issues

6.2.1.2 Risk, vulnerability and resilience

Risk (and systemic risk)

In general terms, risk describes the (future) *consequences* potentially arising from the operation of our systems and from our activities, and the associated *uncertainty*. Consequences are usually seen

in negative, undesirable terms with respect to the planned objectives. Accident *scenarios* are a relevant part of risk, in that they are those combinations of events potentially leading to the undesired consequences. The recent definition of risk in the glossary of the specialty group on "Foundations of Risk Analysis" of the Society for Risk Analysis (SRA), refers to the consequences of a future activity, e.g. the operation of a CI, where the consequences are with respect to something that humans value. The consequences are often seen in relation to some reference values (planned values, objectives, etc.) and the focus is normally on negative, undesirable consequences. There is always at least one outcome that is considered as negative or undesirable [SRA, 2015].

A classical metric adopted to describe Risk (R) is the following set of triplets [Kaplan and Garrick, 1981]:

$$R = \{\langle S_i, P_i, X_i \rangle\}, \tag{2}$$

where S_i denotes i-th specific (mostly undesired/adverse) *event* or *scenario* leading to loss, damage or injury; P_i denotes the *probability* (*frequency*) of occurrence of that scenario; and X_i denotes the *extent* of the resulting *consequences*. These quantities (and their associated uncertainties) are considered as being numerically quantifiable [Kröger and Zio, 2011]: e.g., for CIs, risk can be computed as the loss of service with its resulting consequences for the people concerned. However, recent research and discussions on the foundational issues of risk assessment and management have led to a broader and more complete description of risk. This includes, besides the triplets of elements reported in (2), also the uncertainty U_i in the probabilities (frequencies) P_i and consequences X_i, in the light of the analyst's (lack of) knowledge (K) on the problem and the system at hand (see previous Section 6.1). Then, the quantification of risk in (2) could be rewritten as:

$$R = \{\langle S_i, P_i(U_i), X_i(U_i) \rangle | K\}. \tag{3}$$

For thorough practical and conceptual discussions on the definition and quantification of risk the reader is referred to, e.g., [Aven, 2012a and b; SRA, 2015] among many others.

Today's critical systems and infrastructures are challenged by the disruptive influences of a complex mix of manmade and naturally occurring threats and hazards, including terrorist attacks, accidents, natural disasters, and other emergencies. With respect to this, *systemic risk* is the risk of having not just statistically independent failures, but interdependent, cascading failures in a network of interconnected system components [Helbing, 2013]. In such cases, a localized initial failure ('perturbation') could spread to other parts of the system and have disastrous effects and cause, in principle, unbounded damage. Large scale outages resulting from systemic risks on real-world CI systems are well documented; examples include blackouts in power grids [US-CA, 2004; UCTE, 2007; Pidd, 2012], telecommunication outages [Newman et al., 2002], financial bankruptcy [Battiston et al., 2007], and catastrophic failures in socio-economic systems [Zhao et al., 2011;

Kempe et al., 2003]. This is strong motivation for investigating the global dynamics of systemic risks.

Vulnerability

Vulnerability is a concept that is used in many areas, but its definition is often ambiguous and sometimes misleading [Buckle et al., 2000; Dilley and Boudreau, 2001; Weichselgartner, 2001; Haimes, 2006]. The term vulnerability has been introduced as the hazard-centric perception of disasters for which the representation in terms of risk appears too limited. A hazard of low intensity could have severe consequences on a system, while a hazard of high intensity could have negligible consequences: the level of vulnerability of the system makes the difference.

In the glossary of the specialty group on "Foundations of Risk Analysis" of the SRA, vulnerability of a system is referred to the *degree* to which a the system can be affected by a *given specific* risk source or agent [SRA, 2015]. Along this line, many definitions explicate vulnerability as the system's overall *susceptibility* to *loss* due to a *given* negative, i.e., the *magnitude* of the *damage given* a specific *strain*. In this view, vulnerability can be interpreted as a *flaw* or *weakness* in the design, implementation, operation and/or management of an infrastructure system or its elements, that: (i) renders it *susceptible* to destruction or incapacitation when exposed to a hazard or threat, or (ii) *reduces* its *capacity* to resume new stable conditions. In order for the vulnerability to be meaningful, it must be related to *specific hazard exposures* (see, e.g., [Dilley and Boudreau, 2001]). A system might thus be vulnerable to certain hazard exposures but robust to others [Hansson and Helgesson, 2003]. Then, the assessment of the *overall* vulnerability of a system requires an evaluation of the exposure to *different* kinds of hazards (e.g., intentional, random internal and natural) [Zio et al., 2012]: an *all-hazard* approach encompassing a general view on the hazards targeting a given system is, thus, needed [Pollet and Cummings, 2009; Waugh, 2005].

In the light of the definitions given above, the concept of vulnerability can be viewed mainly from *two perspectives*:

1. the first perspective is related to a *global technical system property*, where the goal is the evaluation of the *extent* of adverse effects caused by the occurrence of a specific hazardous event (e.g., [Aven, 2007; Johansson and Hassel, 2010; Kröger and Zio, 2011]). For example, the vulnerability of an electric power system might be specified in terms of: (i) changes of network characteristics following attacks on nodes and the scale (e.g., number of nodes/lines lost) or the duration of the associated loss, or (ii) the frequency of major blackouts (number per year) and the associated severity, measured either in power lost or energy unserved (MW or MWh);

2. the second perspective is related to *critical parts* or *components* of a system (e.g., [Apostolakis and Lemon, 2005; Latora and Marchiori, 2005]): in this view, a component *is* a vulnerability of a system if its failure causes large negative consequences to that system [Johansson and Hassel, 2010].

In this dissertation, we define vulnerability as "the consequences that arise when a system is exposed to a hazardous event of a given type and magnitude" and we adopt both the above two perspectives for vulnerability analysis (see details in Section 6.2.3.1).

Resilience

In recent years, lessons learned from some catastrophic accidents have extended the focus on the ability of safety-critical systems and infrastructures to withstand, adapt to and rapidly *recover* from the effects of a disruptive event and, thus, the concept of resilience [Moteff 2012; Obama 2013]. The outcomes of the 2005 World Conference on Disaster Reduction (WCDR) confirmed the significance of the entrance of the term resilience into disaster discourse and gave birth to a new culture of disaster response [Cimellaro et al., 2010]. As a result, systems should not only be reliable (i.e., have an acceptably low failure probability), but also be able to recover from disruptions of the nominal operating conditions [Zio, 2009]. Government policy has also evolved to encourage efforts that would allow assets to continue operating at some level, or quickly return to full operation after the occurrence of disruptive events [Moteff, 2012]. As a consequence, resilience is nowadays considered a fundamental attribute for safety-critical systems and infrastructures that should be guaranteed by design, operation and management.

Resilience comes from the Latin word "resilio" that literary means "to leap back" and denotes a system attribute characterized by the ability to recover from challenges or disruptive events. The Merriam-Webster dictionary defines resilience as "the ability to recover from or adjust easily to misfortune or change". A recent definition of resilience is given in the glossary of the specialty group on "Foundations of Risk Analysis" of the SRA, in terms of: (i) the *ability* of the system to *sustain* or *restore* its *basic functionality* following a risk source or an event (even unknown); (ii) the *sustainment* of system's *operations* and associated *uncertainties*, following a risk source or an event (even unknown) [SRA, 2015]. Various other definitions of "resilience" have been proposed for infrastructure and economic system analysis in the past decades with specific focus on diverse fields of application, such as seismic engineering and structural systems, ecological systems, economics and financial systems, service systems, telecommunication systems, urban infrastructures, disaster analysis for avoidance and recovery (see, e.g., [Bruneau et al., 2003; Reed et al., 2009; Cimellaro et al., 2010; Aven, 2011b; Henry et al., 2012] for some relevant examples): all these diverse

definitions conceptually refer to the *ability* of a system or an organization to *react* and *recover* from unanticipated disturbances and events.

A more "operationalized" definition of resilience is instead given by McDaniels et al. (2007). This definition points out *two* key *properties* of resilience, namely *robustness* and *rapidity*. Robustness refers to a system's ability to *withstand* a certain amount of *stress* with respect to the *loss of functionality* of the system, or as Hansson and Helgesson (2003) defines it: "the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations". In this view, robustness can be seen as the antonym of the term vulnerability. Rapidity on the other hand refers to a system's ability to *recover* from an undesired event with respect to the *speed of recovery*. Both aspects will be considered and quantified in the present dissertation.

From a synthetic disaster management perspective, Figure 13 conceptually illustrates all the concepts mentioned (i.e., risk, vulnerability, robustness and resilience) and their characteristics with reference to the functionality curve $\Phi(t)$ of a safety-critical system or infrastructure. Notice that $\Phi(t)$ could be represented by different metrics depending on the type of analysis (e.g., the amount of flow or services delivered, the availability of critical facilities, the number of customers served, or the enabling potential of economic activities for infrastructure systems): for a power transmission network $\Phi(t)$ may represent the amount of electricity delivered to the demand nodes as a function of time. In the Figure, as said before, S_i denotes a risk scenario (e.g., a disruptive event, such as an earthquake or a terroristic attack) happening at time t_e, P_i denotes the probability (frequency) of that scenario, X_i is the resulting consequence (functionality loss) and U_i is the uncertainty associated with P_i and X_i.

In this conceptualization, the vulnerability ($V(U_i)$) of the system, defined as "*the consequences that arise when the system is exposed to a hazardous event of a given type and magnitude*", can then be represented precisely by the uncertain variable

$$V(U_i) = \{X_i(U_i)\}. \tag{4}$$

Notice that the extent of the consequence is measured between the time t_e, where the disruptive event happens, and the time t_d, where the system reaches the minimal functionality.

Another uncertain variable $RB(U_i)$ denotes the *robustness* (defined as "*the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations*") of the system under scenario S_i. It is the *residual* functionality right after the disruptive event and can be represented by the following relation:

$$RB(U_i) = \{\Phi(t_0) - X_i(U_i)\} \tag{5}$$

On the post-disruption recovery process (between times t_d and t_r), $T_{RE}[\Phi(t_r), U_i]$ denotes the interval of time required for the system to recover a stable, target functionality level $\Phi_{TG} = \Phi(t_r)$ (notice that $\Phi(t_r)$ may be lower than the initial, optimal functionality $\Phi(t_0)$): this element represents the "temporal" dimension of resilience (*recovery time*). On the contrary, $\Phi_{RE}(t_r, U_i)$ refers to the "amount" of system functionality that has been *actually restored* at time t_r: this element represents the so-called "spatial" dimension of resilience (*functionality recovery*). Therefore, the resilience $RE(U_i)$ can be in all generality expressed as a "function" of the following couple:

$$RE(U_i) = \{T_{RE}[\Phi(t_r), U_i], \Phi_{RE}(t_r, U_i)\}. \tag{6}$$

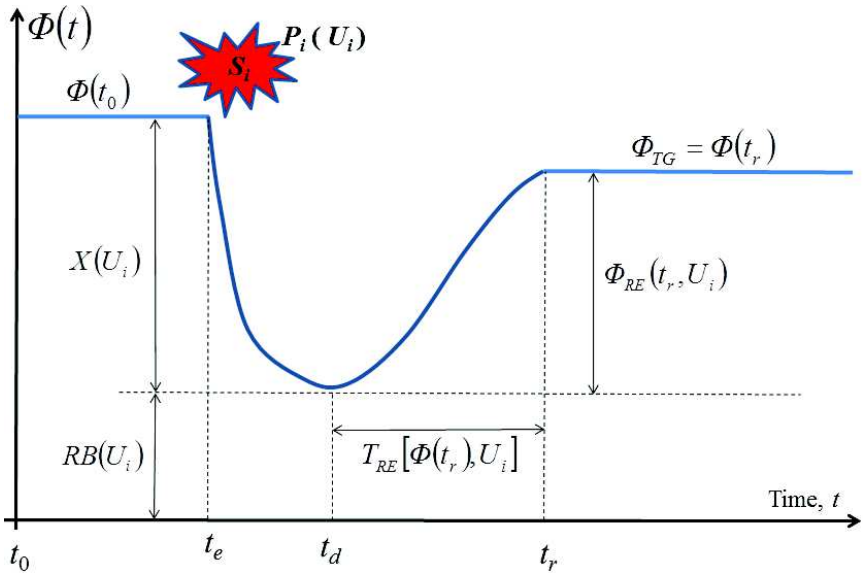


Figure 13. Illustration of the concepts of risk, vulnerability, robustness and resilience with reference to the functionality curve Φ(t) of a safety-critical system or infrastructure

6.2.2 Issues and possible solution approaches: a critical literature survey

The quantities (2)-(6) described in the previous Section 6.2.1 must be *accurately* and *precisely* assessed in order to take rational *decisions* on the utilization of resources for *protecting* the safety-critical systems and infrastructures of interest (possibly from different types of hazards), for reducing their associated risk and vulnerability and improving their safety and resilience. In general, the tasks outlined above are carried out by the following main steps (see Figure 1):

1. Representation of the real system to capture its *main features* and provide a picture of the information needed to answer relevant questions.
2. Mathematical modeling of the system (and corresponding implementation in a *computer code*) to provide: (i) an *approximate* description of the behavior of the real system dependent on a number of (input) *hypotheses* and *parameters*; (ii) the numerical *outputs* of interest (i.e., in this case the relevant risk, vulnerability and resilience metrics).

3. Simulation of the behavior of the system under various conditions of interest (e.g., operational transitions and accident scenarios) and quantitative *evaluation* of the corresponding critical *outputs* of interest (i.e., risk, vulnerability and resilience).
4. Risk-informed decision making processes to (optimally) determine a set of protective actions to be taken in order to effectively reduce (resp., increase) the level of risk and vulnerability (resp., resilience) of the safety-critical systems under consideration.

In the present dissertation, these steps have been analyzed under three research lines/issues:

1. the first concerns the development of innovative methods of *representation* and *modeling* of Critical Infrastructures (CIs) (in particular, for energy production and transmission), for the analysis of their *vulnerability* and *resilience* (Section 6.2.2.1);
2. the second deals with the design and implementation of innovative algorithms for the *efficient risk assessment* and/or *reliability evaluation* of *highly-reliable* engineered systems and infrastructures (in particular, for energy production and safety) (Section 6.2.2.2);
3. the third is about the development of innovative *decision making* approaches for the *multi-criteria vulnerability analysis* of safety-critical systems and infrastructures (in particular, for energy production) under uncertainty (Section 6.2.2.3).

A pictorial representation of the three research issues explored under Axis 2 is given in Figure 14.

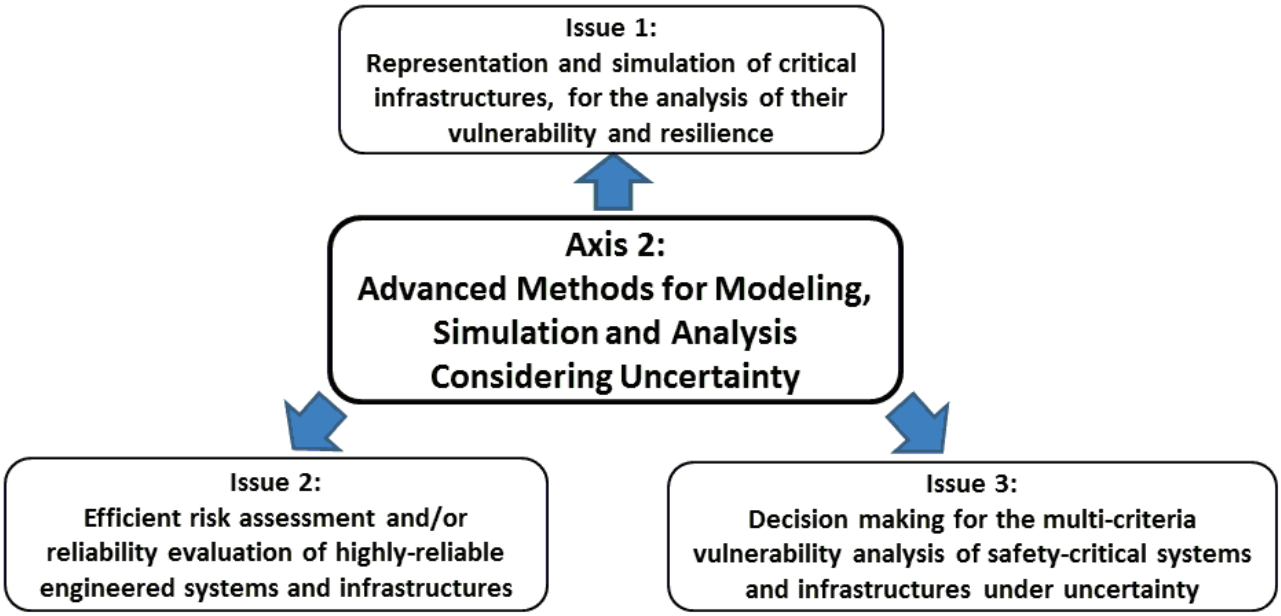


Figure 14. Three conceptual and practical issues addressed under research Axis 2

6.2.2.1 Issue 1: Development of innovative methods of representation and simulation of Critical Infrastructures (CIs), for the analysis of their vulnerability and resilience

A broad spectrum of approaches exists for representation and modeling of Critical Infrastructures (CIs), for the analysis of their vulnerability and resilience. However, as previously highlighted in Section 6.2.1.1, the analysis of these CIs cannot be carried out *only* with classical methods of system decomposition and logic analysis, which seem not to be fully equipped to deal with the level of complexity inherent in such systems (see Figure 12). Thus, a framework is needed to *integrate* a number of methods capable of viewing the problem from *different perspectives* under the existing uncertainties [Zio, 2014b]. The main perspectives include [Zio, 2014b]:

- Logical methods based on system analysis, hierarchical and logic trees, etc.; these methods are capable of capturing the logic of the functioning/disfunctioning of a complex system, and of identifying the combinations of failures of elements (hardware, software and human) which lead to the loss of the system function.
- Structural/topological methods based on system analysis, graph theory, statistical physics, etc.; these methods are capable of describing the connectivity of a complex system and analyzing its effects on the system functionality, on the cascade propagation of a failure and on its recovery (resilience), as well as identifying the elements of the system which must be most robustly controlled because of their central role in the system.
- Flow methods, based on detailed, mechanistic models (and computer codes) of the processes occurring in the system; these methods are capable of describing the physics of system operation, its monitoring and control.
- Phenomenological/Functional methods, based on transfer functions, state dynamic modeling, input-output modeling and control theory, agent-based modeling etc.; these methods are capable of capturing the dynamics of interrelated operation between elements (hardware, software and human) of a complex system and with the environment, from which the dynamic operation of the system itself emerges.

A brief literature survey on these approaches is given in what follows.

Logical methods

Several types of system representation and modeling approaches exist in literature and they rely mainly on a *hierarchy* or *graph* structure.

Hierarchical Modeling has been often adopted to represent and model complex systems, since many organizational and technology-based systems are hierarchical in nature. This approach can be based on different perspectives, e.g., functional, technical, organizational, geographical, political, etc., and

can allow simplifying the modeling process and the ultimate management of the system as a whole [Haimes, 2012].

Hierarchical functional models include Goal Tree Success Tree (GTST) – also combined with Master Logic Diagram (MLD) – and Multilevel Flow Modeling (MFM). The GTST is a *functional hierarchy* of a system organized in levels starting with a *goal* at the top; the MLD, developed and displayed hierarchically, instead shows the "*structural*" *relationships* among independent *parts* of the systems: the combined GTST – MLD provides a powerful *functional-structural* description method. Finally, the dynamic version of the approach, namely the GTST – Dynamic MLD (GTST-DMLD), allows describing also the temporal behavior of the systems [Hu and Modarres, 2000]. Notice that the GTST-DMLD has been considered and applied also in the present thesis (for details, see Section 6.2.3.1 and Paper III [Ferrario et al., 2015a] in the Appendix). Multilevel Flow Models, developed in the field of artificial intelligence, have been proposed for qualitative reasoning, i.e., for representing and structuring knowledge about physical phenomena and systems. They consider cause-effect relations and facilitate the reasoning at different levels of abstraction on the basis of "means-end" and "whole-part" decomposition and aggregation procedures. Goals, functions and flow of material, energy and information are connected to form a hyper graph. They are mainly used for measurement validation (e.g., for checking the measurement of a mass or energy flow), alarm analysis (e.g., for the identification of primary and secondary alarm), and fault diagnosis (i.e., for the identification of the consequences and the root causes of a disturbance in the system functioning) [Lind, 2011 and 2012].

This "logical" perspective includes also: (i) risk analysis approaches that evaluate the result of adverse events affecting a system by means of the potential negative consequences and their associated likelihoods, and it provides suggestions on how to reduce vulnerability, improve resilience and mitigate consequences, and (ii) probabilistic modeling adopted for the characterization of CIs. Risk analysis is carried out by qualitative [Moore, 2006; Piwowar et al., 2009] and quantitative assessments [Apostolakis and Lemon, 2005; Flammini et al., 2009] with the further goal of ranking system components on the basis of their criticality [Koonce et al., 2008]. Traditional methods for risk analysis, e.g., Fault and Event Tree methodology and core methods of Probabilistic Risk Assessment (PRA), have been applied to the vulnerability analysis of CIs for protecting the systems against malevolent actions [Piwowar et al., 2009]. These hierarchical trees are commonly used to identify: (i) the initiating causes of a pre-specified, undesired event or (ii) the accident sequences that can generate from a single initiating event. These approaches comprise step-by-step processes typical of PRA [Kröger and Zio, 2011]. However, they imply drawbacks for use on safety-related issues of large-scale infrastructures due to: "i) the high complexity and

interconnectedness of modern CIs that cannot be adequately modeled; ii) all kinds of human factors and the full spectrum of threats, including malicious behavior and attacks that cannot be taken into account; iii) the dynamic or even the non-linear behavior of systems that cannot be easily handled; and iv) independence from contextual factors that has to be assumed" [Kröger, 2008]. Probabilistic modeling approaches include Markov Chains, Markov/Petri nets and Bayesian networks. The first two rely on the definition of transition probabilities of the system components among their reachable states. An achieved configuration of the component states determines the system state. A limitation of these methods is the exponential growth of the possible configuration of the system when the number of components increases and/or the number of states for each component is high. Bayesian networks can be used for modeling and predicting the behavior of a system, based on observed stochastic events. Drawbacks of this methodology arise from its complexity that leads to significant efforts in logic modeling and quantification, and from the limited capability of providing an exhaustive analysis.

Structural/topological methods

This class of approaches models the interdependent CIs on the basis of their *topologies* under different types of hazards [Ouyang, 2014]. They represent CIs by *graphs* (actually, they are *network*-based approaches) where the *nodes* are the components and the *links* are the physical and relational connections among them. These topology-based methods consider two possible states for the components (failed and functioning), and can measure the *strength* of the connections by including *weighted* links. For network theoretical studies of CIs, *only* the most fundamental parts of the infrastructure are usually modelled, i.e., the *structural properties* of the system that facilitates the physical transportation of the services they provide. On the contrary, in general *no* or *limited functional* aspects of the network are modelled. Topological analysis based on complex network theory can unveil relevant properties of the structure of a network system [Albert et al., 2000; Strogatz, 2001] by: (i) highlighting the role played by its components, (ii) making preliminary vulnerability assessments based on the simulation of faults (mainly represented by the removal of nodes and arcs) and the subsequent re-evaluation of the network topological properties and (iii) guiding and focusing further detailed analyses of critical areas [Crucitti et al., 2006; Zio et al., 2008]. Notable studies concerned with the structural analysis and assessment of the vulnerability among the CIs sector include structural vulnerability of urban transport networks [Masucci et al., 2009], vulnerability of power grids [Bompard et. al., 2009; Crucitti et al. 2005; Holmgren 2006; Hines and Blumsack, 2008; Eusgeld et al., 2009] and the Internet links [Latora and Marchoiri, 2005]. Although simple graph models are common ways to represent and analyze CI networks,

parts of physical properties can also be incorporated into the structure representation of realistic CI systems (e.g., electrical power infrastructure) [Hines and Blumsack, 2008; Cotilla-Sanchez et al., 2012]. Many performance metrics can be quantified, e.g., number of normal or failed components, connectivity loss, fraction of costumers affected, lost service hour, and they can be used to evaluate interdependent effects to facilitate the assessment of mitigation actions and cascading failure consequences [Ouyang, 2014].

In real CI networks another importance dimension to add to the vulnerability characterization is the *dynamics* (i.e., processes going on within networks) of flow of the physical quantities in the network. This entails considering the interplay between structural characteristics and dynamical aspects, which makes the modeling and analysis very complicated since the load and capacity of each component and the flow through the network are often highly variable quantities both in space and time [Kröger and Zio, 2011]. This is particularly relevant in the study of cascading failures. Several models have been developed to capture the *basic* dynamic features of CI networks within a (weighted) topological analysis framework (see, e.g., [Watts, 2002; Motter and Lai, 2002; Holme et al., 2002; Motter, 2004; Crucitti et al., 2004; Kenney et al., 2005; Li et al., 2013]). Among these approaches, the well-known Motter-Lai (ML) model will be considered and applied in the present dissertation (for details, see Section 6.2.3.1 and Paper IV [Fang et al., 2015b] in the Appendix). In all these approaches, the dynamics of cascading is *only* related to statistical *topological* (structural) properties of the networks (e.g., the network *connectivity*). Nevertheless, these abstract modelling paradigms allow a *preliminary* analysis the system response to cascading failures and can be used to *guide* a *successive* more *detailed* simulation focused on the most relevant physical processes and network components. Despite their apparent simplicity, these models provide indications on the elements *criticality* for the propagation process [Zio and Sansavini, 2011a] and on the *actions* that can be performed in order to prevent or mitigate the undesired effects [Motter, 2004]. In addition, they have the advantage of modelling cascading dynamics with *few parameters*, so that their application to realistic, large-scale systems is *feasible* and certainly *computationally cheap*. On the other hand, they abstract the physical laws regulating the flows in the system: in other words, they *cannot* give sufficient information about the *flow performance* of the system, which is instead analyzed by flow-based methods.

Flow-based methods

This class of approaches models the interdependent CIs on the basis of their *flow patterns* under different types of hazards [Ouyang, 2014]: in other words, explicit consideration is given to the mathematical *equations* governing the physical flows of electricity, gas, water, data, etc., through

the CI connections. As the structural/topological methods, they represent CIs by networks (they are network-based approaches too). These methods can be based on uniform network descriptions [Lee et al., 2007], physical rules that provide a more realistic modeling on interdependencies [Ouyang et al., 2009], oriented stochastic modeling methods [Bobbio et al., 2010], dynamic functional model [Trucco et al., 2012], maximum flow model [Nozick et al., 2005], and others [Ouyang, 2014]. They capture the flow characteristics of interdependent CIs, identify critical component, and suggest improvement for the emergency protection; however, their *computational cost* can be *prohibitive* when the components and links are described in detail [Ouyang, 2014].

Of particular interest to the present thesis are the physics-based flow models of cascading failures. There are many models of cascading failure selecting and approximating a modest subset of the many physical and engineering mechanisms of the system under study. Taking the study of cascading failures in electrical power grids as an example, the so-called Manchester model [Nedic et al., 2006] is a fairly detailed blackout model based on AC power flow simulation. The Hidden failure model [Wang and Thorp, 2001] is based on the hidden failure theory and tends to simulates hidden relay failures probabilistically, taking into account the DC power flow constraint of the network. In addition, some researchers [Iyer et al., 2009; Wang et al., 2012] provide Markov-transition models for cascading failure in power grids, where the transition probabilities among states are derived from a stochastic model for line overloading using a stochastic flow redistribution model based upon DC power-flow equations. However, the state space of Markov-based model is large, as it requires tracking the functionality status of transmission lines and power flow information; in addition, due to the analytical complexity of the time-varying transition probabilities, the analytical and asymptotic characterization of probabilistic metrics (such as the blackout probability and distribution of the blackout size) is not possible. Finally, researchers at Oak Ridge National Laboratory (ORNL), Power System Engineering Research Center (PSerc) of Wisconsin University, and Alaska University (Alaska) have proposed a landmark study for blackout modelling in power grids, called the ORNL-PSerc-Alaska (OPA) model [Dobson et al., 2001]. The OPA model is built upon the Self-Organized Criticality (SOC) theory and DC power flow attributes. It contains two different time scale dynamics, i.e., power flow dynamics and power grid growth dynamics, and reveals the complexity and criticality of power systems. The OPA model seeks to faithfully describe the *dispatching dynamics* of the power flows during the evolution of the failure propagation following the initial disturbances, by explicitly incorporating the standard DC power flow equations and minimizing generation costs and load shedding [Dobson et al., 2001]. Till now, only ideal cases (such as tree networks) and real networks with a small number of nodes (~ 100) have been treated by means of the OPA model [Carreras et al., 2002]. Large networks and the

influence of the topology on the dynamics of the model have not been studied yet. Notice that also the OPA model will be considered and applied in the present dissertation (for details, see Section 6.2.3.1 and Paper IV [Fang et al., 2015b] in the Appendix).

Finally, notice that embracing these more physical descriptions (and solving the corresponding constrained optimization functions associated to the model) results in a significant increase in the *computational burden*, rendering practical application extremely difficult for realistic networks with large numbers of elements [Sun and Han, 2005].

Phenomenological/Functional methods

This category of methods includes i) agent based model, ii) system dynamic model, iii) economic-based approaches, iv) others (e.g., dynamic control system theory and high level architecture).

Agent based modeling is a simulation methodology coming from the field of complexity science. It is used to evaluate the dynamic operational behavior of infrastructure network and its associated economic entity. An agent based model is composed by three elements: i) agents, i.e., technical and non-technical components, ii), environment, i.e., abstract space where the agents can interact, and iii) rules, i.e., behavior patterns for the agent and the environment, they can include physical law. The behavior of the infrastructure emerges from the behaviors of the individual agent and their interactions [Kröger and Zio, 2011]. The main advantages of the agent based modeling are the possibility of representing heterogeneous components and capturing all types of interdependencies among CIs, capturing the emerging behavior, create a space where the agents interact according to distance, provide a scenario-based what-if analysis and the effectiveness assessment of different control strategies, and can be also integrated with other modeling technique to provide more comprehensive analysis [Borshchev and Filippov, 2004]. However, two main limitations are with respect to i) the challenge of calibrating the simulation parameters due to the lack of significant data and the difficulties in model the agent behavior, and ii) the dependence of the quality of the simulation on the assumptions made that are difficult to justify theoretically and statistically [Ouyang, 2014].

System dynamic models take a top-down analysis for interdependent CIs to characterize their functions such as production, transmission and consumption. It uses a series of differential equations to describe the system level behaviors of the CIs. The key concepts are i) feedback loops to indicate connection and direction of effects between CIs components, ii) stocks to represent the states of the system and iii) flow rates between stocks. Several are the advantages of this approach: for example, it allows capturing important causes and effects under disruptive scenarios, providing investment recommendations, and including multi-attribute utility functions to compare protection

strategies. On the contrary, they cannot analyze component-level dynamics (such as change of infrastructure topologies), it is difficult to calibrate parameters (huge amount of data are needed) and perform a validation of the model [Ouyang, 2014].

Economic-based approaches include two types of economic theories employed to model CIs interdependencies: input-output model and computable general equilibrium. The first one is based on a static and linear model whose output is interpreted as the risk of inoperability of a CI, i.e., its inability to perform its function. It is based on the large-scale databases and measures the interdependencies among infrastructure sectors by economic relationships. The input-output model allows analyzing the propagation of perturbations between interdependent infrastructures and, thus, implementing effective mitigation strategies; in addition, it can provide analytical solutions that facilitate the sensitivity analysis of parameters [Ouyang, 2014]. However, it cannot analyze the interdependencies at component levels and it can give a good approximate result only when the disturbances have small impact on the economic sectors (since the interdependent matrix is derived from economic database and its elements measure the interdependent strength in normal economic operations), otherwise it will provide large errors [Ouyang, 2014]. The computable general equilibrium is an extension of the input-output model to capture nonlinear connections among CIs.

Other approaches exist like dynamic control system theory [Casalicchio et al., 2011] and high level architecture that integrate all the other methods (e.g., agent based modeling) [Eusgeld et al., 2011; Wang et al., 2011].

These phenomenological approaches have not been taken into account in the present dissertation.

6.2.2.2 Issue 2: Design and implementation of innovative algorithms for the efficient risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures

Once a representation and a mathematical model of the safety-critical engineered system and/or infrastructure of interest is available (previous Section 6.2.2.1), its behavior has to be *simulated* under various conditions (e.g., operational transitions and accident scenarios) and the corresponding critical *outputs* of interest (i.e., risk/reliability, vulnerability and resilience) have to be quantitatively *evaluated*. In practice, as highlighted in Section 6.2.1.1, real-world engineered systems and infrastructures are: (1) *dynamic*, i.e., their state changes (deterministically and/or stochastically) in time; (2) *hybrid*, i.e., they are characterized by both discrete and continuous variables (e.g., components' discrete states, like functioning, failed, standby, and continuous physical quantities, like temperatures, pressures and flow rates); (3) *complex*, i.e., they are described by a large number of components, variables and parameters related by highly nonlinear dependences and interconnections.

These real-world system features *rarely* allow solving the models for risk assessment and reliability evaluation with uncertainty propagation *analytically*. On the other hand, Monte Carlo Simulation (MCS) methods offer a feasible means [Zio, 2013]. The basic idea is to:

i. randomly generate a large number of possible system evolutions, including the undesired chains/sequences of events (*scenarios* S_i, $i = 1, 2, \ldots$) possibly leading to system disturbance and/or failure. Correspondingly, quantify the extent of the undesired consequences X_i of the accident scenarios S_i, $i = 1, 2, \ldots$;
ii. estimate the corresponding probabilities (frequencies) P_i as the fraction of the number of simulations that end in a (failure) scenario/state of interest.

While MCS makes it possible to assess the risk and/or reliability of a complex system or infrastructure, it presents some drawbacks (Figure 15):

1. The necessity to introduce the *time dimension* into the analysis leads to a dramatic increase in the *size* of the system state space (and, thus, in the number of possible scenarios), which makes its thorough exploration impossible in practical cases of real, complex systems characterized by hundreds of (discrete-state) components and associated (continuous) physical quantities.
2. When an accident scenario of interest is *very rare*, a large number of simulations of the complex system must be carried out to estimate the probability of that scenario with sufficient statistical *accuracy* and *precision* [Schueller, 2009]: this is a typical situation when dealing with *highly-reliable* engineered systems and with *extreme* events or "black swans" [Zio, 2014a; Aven, 2013 and 2015; Aven and Krohn, 2014].
3. The *computational cost* associated to the simulation of the complex system behavior can be very high, e.g., it may take hours or even days to run *one single* scenario in some particular applications: typical examples are represented by Finite Element Models (FEMs) used in structural reliability analysis, by the computer code RELAP5-3D used to describe the thermal-hydraulic behavior of nuclear systems and by the detailed power flow models employed to simulate the behavior of electrical power networks [Fong et al., 2009; Perez et al., 2011; Dobson et al., 2001].
4. If the simulation of the behavior of the system of interest requires the propagation of *hybrid* (aleatory and epistemic) uncertainty through the mathematical model, then the computational burden is increased even more dramatically: actually, in such a case *families* of probability models have to be propagated for *each* uncertain model input parameter (see Section 6.1).

These problematic features call for advanced simulation techniques that allow performing *efficient* and *robust* (i.e., accurate and precise) risk assessments and/or reliability evaluations for highly-reliable engineered systems and infrastructures, while *reducing* the associated *computational cost*.

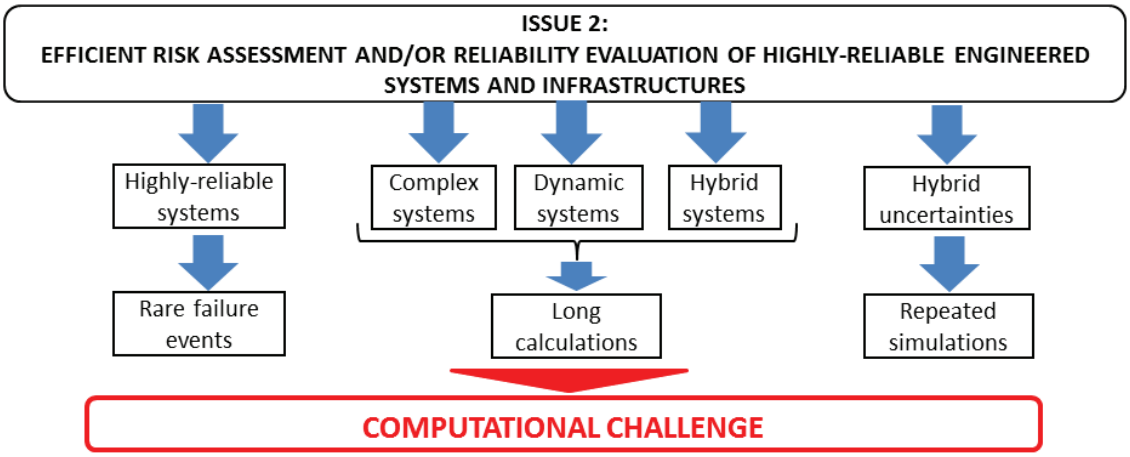


Figure 15. Problems related to the efficient risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures (Issue 2, Axis 2)

In this dissertation, the above mentioned computational challenge is tackled in two different ways: from one side, *efficient random sampling techniques* are employed to perform robust estimations with a limited number of input samples drawn (and associated low computational time); from the other side, *fast-running*, *surrogate regression models* (also called response surfaces or meta-models) are used to replace the long-running system model code in the risk assessment and reliability analysis. A critical literature survey on these two classes of methods is reported in what follows.

Advanced random sampling methods

The computational hurdles described in the previous Section can be tackled from one side by resorting to efficient simulation techniques that perform accurate and precise estimations of the (small) *probabilities* of *rare failure events* and *scenarios* associated to highly-reliable systems and infrastructures with a *limited number* of random samples.

To this aim, the Importance Sampling (IS) method has been introduced, whereby a suitable Importance Sampling Density (ISD) is chosen so as to favor the MC samples to be near the failure region, thus forcing the rare failure event/scenario to occur more often [Au and Beck, 2003a; Au, 2004]. In this regard, it is possible to show that there exists an optimal ISD so that the variance of the MC estimator is zero. Unfortunately, this optimal ISD is not implementable in practice, since its analytical expression depends on the unknown failure probability itself. With respect to that, several techniques in various fields of research have been proposed to reduce some distances between the

instrumental ISD and the optimal one: see, e.g., the Adaptive Kernel (AK) [Au and Beck, 1999; Morio, 2012], the Cross-Entropy (CE) [Rubinstein and Kroese, 2004; De Boer et al., 2005; Botev and Kroese, 2008], the Variance Minimization (VM) [Asmussen and Glynn, 2007] and the Markov Chain Monte Carlo-Importance Sampling (MCMC-IS) [Botev et al., 2013b] methods.

Another possible approach is Stratified Sampling [Helton and Davis, 2003; Munoz Zuniga et al., 2011]. This technique requires dividing the sample space into several non-overlapping subregions (referred to as "strata") and calculating the probability of each subregion; the (stratified) sample is then obtained by randomly sampling a predefined number of outcomes from each stratum [Helton and Davis, 2003; Cacuci and Ionescu-Bujor, 2004]. By so doing, the full coverage of the sample space is ensured while maintaining the probabilistic character of random sampling. A major issue related to the implementation of Stratified Sampling lies in defining the strata and calculating the associated probabilities, which may require considerable a priori knowledge. As a remark, notice that the widely used event tree techniques in nuclear reactor PRA can be seen as defining and implementing Stratified Sampling of accident events and scenarios [Cacuci and Ionescu-Bujor, 2004].

A popular compromise between plain random sampling (i.e., standard MCS) and Importance/Stratified Sampling is offered by Latin Hypercube Sampling (LHS), which is commonly used in PRA [Morris, 2000] for efficiently generating random samples [Helton and Davis, 2003; Sallaberry et al., 2008]. The effectiveness of LHS, and hence its popularity, derives from the fact that it provides a dense stratification over the range of each uncertain variable, with a relatively small sample size, while preserving the desirable probabilistic features of simple random sampling; moreover, there is no necessity to determine strata and strata probabilities like in Stratified Sampling [Helton and Davis, 2003]. For these reasons LHS is frequently adopted for efficiently propagating uncertainties in PRA problems [USNRC, 1990; Hofer et al., 2002; Krzykacz-Hausmann, 2006; Helton and Sallaberry, 2009]. On the other hand, LHS is very efficient for estimating mean values and standard deviations in complex reliability problems [Olsson et al., 2003], but only slightly more efficient than standard MCS for estimating small failure probabilities [Pebesma and Heuvelink, 1999], like those expected for complex, safety-critical engineered systems and infrastructures.

In the Subset Simulation (SS) approach, the small probability of an extreme failure event/scenario is expressed as a product of *conditional* probabilities of some chosen intermediate and thus *more frequent* events [Au and Beck, 2001; Au and Beck, 2003b; Ching et al., 2005; Au et al., 2007; Zio and Pedroni, 2009b and 2010b; Cadini et al., 2012; Au and Wang, 2014]. The problem of evaluating the small probabilities is thus tackled by performing a *sequence* of simulations of more

frequent events in their conditional probability spaces; the necessary conditional samples are generated through successive Markov Chain Monte Carlo (MCMC) simulations [Metropolis et al., 1953], in a way to gradually populate the intermediate conditional regions until the final failure region is reached. A similar concept is exploited by the so called splitting methods [Botev and Kroese, 2012; Botev et al., 2013a; Murray et al., 2013].

In the Line Sampling (LS) method, *lines* (instead of random points) are used to probe the failure domain of the high-dimensional system state space under analysis [Schuëller and Pradlwarter, 2007; Zio and Pedroni, 2009c, 2010a,b; Valdebenito et al., 2010]. An "important direction" is optimally determined to point towards the failure domain of interest and a number of conditional, one-dimensional problems are solved along such direction, in place of the high-dimensional problem [Pradlwarter et al., 2005]. The approach has been shown to perform significantly better than standard MCS in a wide range of risk assessment and reliability analysis applications in the structural, nuclear and aerospace fields [Koutsourelakis et al., 2004; Schueller et al., 2004; Pradlwarter et al., 2005 and 2007; Schueller and Pradlwarter, 2007; Valdebenito et al., 2010; Zio and Pedroni, 2009c; 2010a, b; 2012].

The above mentioned algorithms have shown to provide outstanding performances in *static* problems, whereas their *applicability* to complex *dynamic* systems is not fully demonstrated. Methods explicitly designed for dynamic reliability analysis and risk assessment have been proposed in the literature [Labeau, 1996], and consistently developed through years [Labeau et al., 2000]. In particular, Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) is currently employed to take into account *time-dependences* in the evolution of the dynamic system and to probe the corresponding event sequence space for identifying *unknown unreliability*, *unexpected scenarios* and *critical configurations* [Zio, 2014a]. In this context, in [Zhu et al., 2006] advancements in the dynamic reliability field have been brought by including software behavior into the analysis and using an entropy-driven criterion to *intelligently guide* and *force* the simulation of scenarios of interest. [Hu et al., 2004] proposed methods that focus the exploration efforts, i.e. the simulations, on those scenarios having more uncertain outcomes (i.e., a higher number of end states). For this purpose, they exploited a function based on *negative entropy* for assessing the uncertainty in the simulation outcomes and a Bayesian scheme for updating the knowledge gathered by the simulations [Hu, 2005]. [Čepin and Mavko, 2002] and [Rao et al., 2009] evaluate system failure probabilities by resorting to dynamic fault trees. A method exploiting Dynamic Event Tree (DET) and Monte Carlo simulation is proposed in [Li et al., 2010 and 2011] to *force* the stochastic system simulation to a failure state and to retrieve the corresponding probability by means of a

biasing approach similar to that of Importance Sampling. In [Catalyurek et al., 2010] and [Aldemir, 2013] an efficient framework is proposed for the exploration of the state space of dynamic, hybrid and complex systems and the assessment of the corresponding state probabilities; however, an acceptance threshold on the probabilities is introduced to avoid an explosion of the number of system analysis, making these approaches prone to neglect events with small failure probabilities. Finally, Sequential Monte Carlo simulation has recently captured the attention of many researchers due to its rigorous consistent mathematical formulation and its possibility of dealing with rare events [Cérou et al., 2012] and large hybrid dynamic systems [Blom et al., 2006; Cassandras and Lygeros, 2006].

Fast-running surrogate regression models (or meta-models)

Another viable approach to overcome the computational burden associated to the risk assessment and reliability analysis of highly-reliable safety-critical systems and infrastructures is that of resorting to fast-running, surrogate regression models, also called response surfaces or meta-models, to approximate the input/output function implemented in the long-running system model code, and then *substitute* it in the system analysis [Storlie et al., 2008]. Because calculations with the surrogate model can be performed *quickly*, the problem of long simulation times is circumvented.

The construction of such a surrogate model entails running a *reduced* number of expensive simulations (e.g., few hundreds) for specified "exemplary" system operating conditions and collecting the corresponding system response. Then, statistical techniques are employed for "fitting" the response surface to the "exemplary" data generated in the previous step: by so doing, the meta-model is "*trained*" to reproduce the behavior of the original long-running computer model. Several examples can be found in the open literature concerning the application of surrogate meta-models in risk assessment and reliability analysis problems. In [Bucher and Most, 2008; Liel et al., 2009; Bai et al., 2014], polynomial Response Surfaces (RSs) are employed to evaluate the failure probability of structural systems, whereas in [Arul et al., 2009; Fong et al., 2009; Mathews et al., 2009], they are employed for performing the reliability analysis of emergency passive safety systems in advanced nuclear reactors. In [Deng, 2006; Hurtado, 2004 and 2007; Cardoso et al., 2008; Cheng et al., 2008], learning statistical models such as Artificial Neural Networks (ANNs), Radial Basis Functions (RBFs) and Support Vector Machines (SVMs) are trained to provide local approximations of the failure domain in structural reliability problems. In [Zio et al., 2010; Pedroni et al., 2010] ANNs are used for the estimation of the failure probability of emergency safety systems in nuclear reactors.

In the same line of research, Gaussian process models and kriging are very promising. They *assume* that the computer model behaves as a realization of a Gaussian random process whose parameters are estimated from the available computer runs [Bichon et al., 2008; Picheny et al., 2010; Bect et al., 2012]. Applications of Gaussian meta-models to realistic risk assessment problems in several engineering domains can be found, e.g., in [Marrel et al., 2009, 2015a and b; Volkova et al., 2008].
In addition, Polynomial Chaos Expansion (PCE) and Stochastic Collocation (SC) methods expand the system response as a truncated series of properly selected basis functions, "calibrated" by means of the available computer experiments [Ng and Eldred, 2012]. In particular, PCE surrogates the original, long-running computer model with a series of orthonormal polynomials that are chosen in coherency with the probability distributions of the uncertain model input parameters [Ghanem and Spanos, 1991; Sudret, 2008; Blatman and Sudret, 2010; Kersaudy et al., 2015; Schobi et al., 2015; Sudret and Mai, 2015]. Instead, SC is a stochastic expansion method which constructs multidimensional interpolation polynomials over the system responses evaluated at a structured set of collocation points [Babuska et al., 2007; Ng and Eldred, 2012].
On the other hand, notice that the approximation of the system output provided by an empirical regression model introduces an additional source of (*model*) uncertainty, which needs to be evaluated, particularly in safety critical applications like those of interest to the present dissertation. One way to do this is by resorting to bootstrapped regression models [Efron and Thibshirani, 1993], i.e., an *ensemble* of regression models constructed on different data sets bootstrapped from the original one [Zio, 2006; Storlie et al., 2009]. The bootstrap method is a *distribution-free* inference method which requires *no* prior *knowledge* about the distribution function of the underlying population [Efron and Thibshirani, 1993]. The basic idea is to generate a "bootstrapped data set" by random sampling with replacement from the original set of input-output examples available [Efron and Thibshirani, 1993]: *each* of these bootstrapped data sets is used to build a bootstrapped regression model which is used to calculate the quantities of interest (e.g., in this case the risk and/or reliability associated to the safety-critical system of interest). This allows quantifying, e.g., in terms of *confidence intervals*, the (model) uncertainty associated to the estimates provided by the meta-models [Efron and Thibshirani, 1993].

Finally, it is worth mentioning that other effective strategies combining advanced MCS methods with metamodeling have been proposed in the literature for reducing the computational efforts related to the assessment of the probabilities of rare events/scenarios: in such approaches the meta-model is typically constructed and iteratively refined (by means of samples intelligently generated by the advanced MC scheme) until a desired level of accuracy in the failure probability estimate is

achieved: see, e.g., [Romero et al., 2004; Echard et al., 2011 and 2013; Bourinet et al., 2011; Balesdent et al., 2013; Dubourg et al., 2013; Dubourg and Sudret, 2014; Fauriat and Gayton, 2014; Cadini et al., 2014a, b and 2015].

6.2.2.3 Issue 3: Development of innovative decision making approaches for the multi-criteria vulnerability analysis of safety-critical systems and infrastructures under uncertainty

As highlighted in the previous Sections, a broad spectrum of approaches has been proposed for the (efficient) assessment of the risk, vulnerability and resilience associated to safety-critical systems and infrastructures. Once these estimates are available, an "informed" Decision Making (DM) process has to be carried out to:

i. *compare* the performances of *different* systems, *rank* them and possibly *identify* the *preferred* ones (for example, in the context of interest to the present dissertation the objective would be to identify the less risky/vulnerable and/or more resilient system configurations);
ii. *optimally* determine *sets* of *protective actions* that can improve the overall situation, i.e., that can effectively reduce (resp., increase) the level of risk and vulnerability (resp., resilience) of the (group of) safety-critical systems or infrastructures under consideration.

In this Section, we will be mainly concerned with the vulnerability of safety-critical systems and infrastructures and use it as the driving criterion for the DM process.

In order to perform activities (i) and (ii) listed above, several issues need to be addressed (Figure 16):

1. DM problems typically present *multiple* and *conflicting* objectives (e.g., minimizing system vulnerability while minimizing protective actions costs);
2. DM problems typically present *multiple attributes* and *criteria* to be considered for the evaluation and ranking of the alternative system configurations available and the selection of the preferred ones (e.g., the vulnerability of a power production site to a malevolent external attack could be evaluated on the basis of several attributes like the number of accesses to the site, the level of control at the entrance, the preparedness of the workers, the level of redundancy in the safety and security systems, etc.);
3. as highlighted in Section 6.2.1.2, the assessment of the *overall* vulnerability of a safety-critical system requires an evaluation of the exposure to *different kinds* of hazards: i.e., malevolent acts, accidental and natural occurrences should be *all* considered [Waugh, 2005; Pollet and Cummins, 2009; Zio et al., 2012]. Yet, these different hazards require a *different* analytical *treatment*. Random accidents, natural failures and unintentional man-made

hazards are typically known and categorized by emergency planners. Their occurrence can be typically modeled within a probabilistic framework typical of classical risk assessment approaches. Conversely, *terrorism* is a hazard that eludes quantification by probability theory due to the *intentional* and *malevolent* planning it implies [Zio et al., 2012];

4. in the case of intentional hazards due to malevolent acts, two additional issues need to be taken into account: (a) terroristic attacks are typically characterized by *important consequences* but *low probabilities* (frequencies): thus, the (very *scarce* and *diverse*) 'pieces of data' available on such events cannot be used for a sound, classical statistical analysis; (b) the occurrence of malevolent acts brings issues related to the *large uncertainty* due to behaviors of *different rationality*.

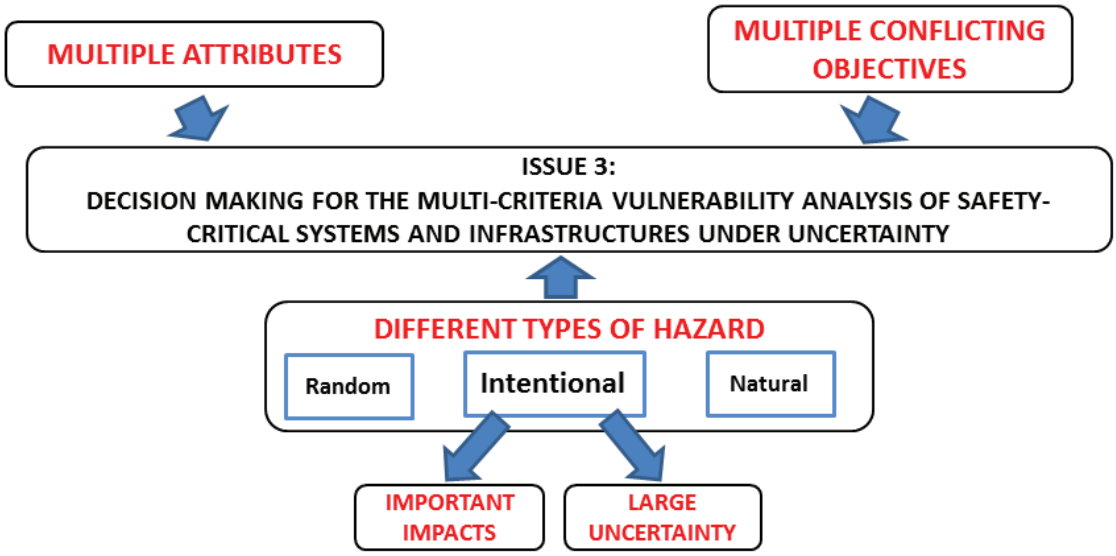


Figure 16. Problems related to decision making process for the multi-criteria vulnerability analysis of safety-critical systems and infrastructures under uncertainty (Issue 3, Axis 2)

As a result of issues 1.-4. listed above, classical risk analysis approaches can be very difficult to apply: in such cases, alternative methods should be sought. Multi-Criteria Decision Aid (MCDA) can provide a formal procedure for the assessment. Indeed, significant advances in MCDA over the last three decades constitute a powerful *non-parametric* alternative methodological approach for *ranking*, *prioritization* and *classification* problems, which can be adopted also for the vulnerability assessment of complex systems under uncertainty [Belton and Stewart, 2002].

In all generality, MCDA aims at constructing a systematic view of the decision maker preferences consistent with a certain set of assumptions, so as to give coherent guidance to the decision maker in the search for the preferred solution (for example, in the context of interest to the present dissertation, the less/more vulnerable system configuration). This is achieved by constructing a model to represent the decision maker preferences and value judgements. The model contains two primary elements, viz.:

1. preferences in terms of each individual criterion, i.e., models describing the relative importance or desirability of achieving different levels of performance for each identified criterion;
2. aggregation scheme, for allowing inter-criteria comparisons, in order to combine preferences across criteria.

Then, according to the nature of the DM problem, the policy of the decision maker and the overall objective of the decision, four different analyses can be performed to:

1. identify the best (i.e., less vulnerable) alternative or select a limited set of the best alternatives;
2. rank-order the alternatives from best (i.e., less vulnerable) to worst ones (i.e., more vulnerable);
3. classify the alternatives into pre-defined homogenous groups (e.g., in the context here of interest, assign them to specified vulnerability categories);
4. identify distinguishing features (i.e., attributes, physical characteristics, etc.) of the alternatives and perform their description based on these features.

Finally, on the basis of the outcomes of (some of the) analyses 1.-4. above, the decision maker needs to "do something" about one or more situations which are found *unsatisfactory* in some way. The DM problem then constitutes much more than simply the evaluation and comparison of alternatives. It involves also an in-depth consideration of what is "unsatisfactory", and the creative *generation* of possible courses of *actions* to address and *improve* the situation (e.g., select protective actions to reduce vulnerability) [Belton and Stewart, 2002]. In an MCDA context, this last step is often termed "*inverse* multi-criteria classification problem": the objective is to identify the *changes* that should be made to the *features* of a given group of alternatives (i.e., the safety-critical systems or infrastructures of interest) so that the group can be "classified" into a more desirable category (i.e., into a lower vulnerability class) [Aggarwal et al., 2010; Li et al., 2012].

A number of examples of applications of MCDA approaches to the assessment, ranking, prioritization of the vulnerability of safety-critical systems exist. [Apostolakis et al., 2005] and [Patterson and Apostolakis, 2007] focus on the identification of critical locations in infrastructures: these are seen as geographical points that are exposed to intentional attacks. Critical locations are not limited to individual infrastructures, but may affect multiple infrastructures: for example, water and electrical distribution systems may occupy the same service tunnels. The vulnerabilities and their ranking according to potential impacts are obtained by Multi-Attribute Utility Theory (MAUT) [Keeney and Raiffa, 1976; Keeney, 1993; Morgan et al., 2000]. In particular, decision makers focus

initially on seeking improvements to what is perceived to be the *most important* (operationally meaningful and measurable) *criterion*. In effect, available alternatives are systematically eliminated until, in the view of the decision maker, a satisfactory level of performance for this criterion has been ensured. At this point, attention shifts to the next most important criterion, and the search continues amongst the remaining alternatives for those which ensure satisfactory performance on this criterion. [Konce, 2008] has proposed a methodology for ranking components of a bulk power system with respect to its risk significance to the involved stakeholders. The likelihood and the extent of power outages when components fail to perform their designed functions are analyzed; the consequences associated with the failures are determined by considering the type and number of customers affected. [Johansson and Hassel, 2010] have proposed a framework for considering structural and functional properties of interdependent systems and have developed a predictive model in a vulnerability analysis context. [Piwowar et al., 2009] have proposed a systemic analysis which accounts for malevolence, i.e., the willingness to cause damage. [Cailloux and Mousseau, 2011] have proposed a framework to evaluate and compare the threats and vulnerabilities associated with territorial zones according to multiple criteria (e.g., industrial activity, population, etc.) by using an *outranking* approach called ELimination Et Choix Traduisant la REalité (ELECTRE). In this approach an alternative is said to "outrank" or "dominate" another one if there is "sufficient" evidence to justify the conclusion that the first alternative is at least as good as the other, taking *all* the measurable *criteria* into account (*not* only one at a time, *sequentially* like in MAUT) [Roy, 1996; Roy and Bouyssou, 1993; Brans et al., 1985 and 1986].

6.2.3 Research developed: methodological and applicative contributions

In this Section, we synthetically overview the methodological and applicative contributions of the present work to the modeling, simulation and analysis of safety-critical systems and infrastructures under uncertainties (Axis 2). In the presentation of the contributions, reference will be made only to the most relevant works (mainly journal papers for brevity) realized by the candidate and his collaborators, within the PhD and Master theses activities.

6.2.3.1 Issue 1: Development of innovative methods of representation and simulation of critical infrastructures, for the analysis of their vulnerability and resilience

In [Ferrario et al., 2015a], we have looked at the *robustness* and *recovery* properties of a System of Systems (SoS) consisting of two interdependent Critical Infrastructures (CIs) (gas and electric power networks), and a Supervisory Control And Data Acquisition (SCADA) system connected to the gas network, all affected by both aleatory and epistemic uncertainties [Nozik et al., 2005].

To provide quantitative measures of the robustness $RB(U_i)$ (5) and recovery capacity (i.e., resilience) $RE(U_i)$ (6) of the SoS, we have evaluated: (i) the steady-state probability distributions of the *supply* of gas and electricity at the demand nodes (which represents the indicator $\Phi(t)$ of the SoS functionality, as defined in Section 6.2.1.2); and (ii) the *time* $T_{RE}[\Phi(t_r), U_i]$ needed to recover the system from the worst condition to the initial functionality level $\Phi(t_0)$ in which all the demand nodes are satisfied, i.e., to obtain $\Phi(t_r) = \Phi(t_0)$.

We have proposed a *hierarchical* model description of the system *logic* and *functionality* by Goal Tree Success Tree – Dynamic Master Logic Diagram (GTST-DMLD) (Section 6.2.2.1), originally *extending* its representation characteristics to evaluate the *physical flows* of gas and electricity through the interdependent infrastructures. In particular, we have introduced new concepts in order to model in the diagram *not only* the *dependency* relations between the components, but also the ways in which the *flows* of gas and electricity are partitioned into the network on the basis of: (i) the *importance* of the demand nodes, (ii) the *amount* of product necessary to satisfy each demand, (iii) the *constraints* of the arc capacities and (iv) the *information* provided by the SCADA system.

For a more realistic representation, we have utilized a *multi-state* model for consideration of the different degrees of damage that the individual components may experience. Transitions between different states of damage occur stochastically (aleatory uncertainty) and epistemic uncertainty affects the associated transition probabilities (frequencies) due to insufficient knowledge and information on the components degradation behavior. Indeed, safety-critical CIs are highly reliable and, thus, undergo few degradation states to failure, so that it is difficult to estimate damage levels and transition probabilities. We have adopted *intervals* to describe the epistemic uncertainty in the probabilities (frequencies) of transition between different components states and in the mean values of the holding time distributions: then, we have used interval analysis to calculate the (uncertain) probabilities (frequencies) of the states of all the components of the CIs. Finally, we have employed Monte Carlo Simulation (MCS) for the probabilistic evaluation of the system performance, i.e., of the robustness and resilience indicators mentioned above.

The framework has shown the capability of representing, modeling and quantitatively accounting for i) the dependencies and interdependencies among the components of a critical infrastructure and between different CIs, respectively, ii) the stochastic variability in the states of the components, and iii) the epistemic uncertainty in the transition probabilities between different components states. The results and insights obtained can help to improve the global SoS performance, e.g., by improving the structural response of specific arcs that more easily turn into damage states or by developing a more redundant network that allows the supply of the product from different paths. For further technical details the interested reader is referred to Paper III [Ferrario et al., 2015a] reported in the

Appendix at the end of the manuscript.

In [Ferrario et al., 2015b], we have proposed a Hierarchical Graph (HG) representation to evaluate the robustness $RB(U_i)$ (5) of interdependent CIs, here measured as its *capability* to deliver the required amount of product (e.g., energy, water, etc.) to the demand nodes of the infrastructure. In doing so, we have taken into account the fact that the demand nodes may have *different importance*, which establishes possibly different priorities in the partitioning of the product through the connections and elements of the CI. The representation consists of a *graph* structured in hierarchical levels that allows highlighting critical arcs and supporting the quantitative robustness evaluation by assigning different priorities to the demand nodes.

For illustration purpose, a case study has been considered that is adapted from the IEEE 123 node test feeders [IEEE, 2000] and includes a large electricity distribution network. As a measure of the robustness of the system, we have evaluated the steady-state probability distributions of the product (i.e., electricity) delivered to the demand nodes. The quantitative evaluation of the system robustness has been performed by MCS. In addition, an unsupervised spectral *clustering* algorithm has been also employed in combination with HG, in order to analyze the CI at *different levels* of detail and to make its *size manageable* [Fang and Zio, 2013]. The results have shown that the HG can be adopted together with hierarchical clustering to provide *approximate* results by analyzing clustered networks instead of the entire large-sized, real network. This can be useful in a first *preliminary* phase of design of the CIs, in order to have satisfactory, physically coherent results with relatively low computational cost.

In [Fang et al., 2015b and c], we have been mainly concerned with power transmission networks and we have addressed the problem of optimally (re)designing some characteristics of these infrastructures in order to reduce (resp. improve) their vulnerability (resp., robustness/resistance) to cascading failures (started by both intentional attacks and random failures).

In details, in [Fang et al., 2015c] we have proposed a methodology for the optimal *allocation* of the *links* connecting generators and distributors in a power transmission network for obtaining high resistance (i.e., low vulnerability $V(U_i)$ (4)) to cascading failures, while keeping the investment costs low. In practical cases, the cost of knocking down an existing network and reconstructing it from scratch is prohibitive, especially for CIs like the power transmission network: a more practicable alternative is to *reconfigure* parts of the network *topology*, e.g., by *reallocation* of the links which connect production facilities to consumers. In most circumstances, low vulnerability and low cost are *conflicting* objectives and cannot be achieved simultaneously. For instance, a highly connected network can be very resistant (or robust) to cascading failures; on the other hand,

increasing the number of connecting links obviously increases costs. Formulated as a large-scale, nonlinear and combinatorial *multi-objective* optimization problem, the facility allocation problem has been solved by a heuristic method, i.e., the Non-dominated Sorting Binary Differential Evolution (NSBDE) algorithm. The search by the NSBDE requires: (i) the construction of a *model* to describe the cascading failure process in the network of interest, and (ii) the *repeated* evaluation of the model for every possible generators-distributors configuration proposed by the algorithm during the search. With respect to that, we have embraced a *topological* cascading failure model (namely, the Motter-Lai – ML – model) (Section 6.2.2.1) to exploit is *rapidity* of calculation. Notice that under the topological ML model, network vulnerability $V(U_i)$ has been quantified by the fraction of network "*connectivity*" *lost* in the cascading failure.

For exemplification, we have applied the method to the 400kV French Power Transmission Network (FPTN400) [EDF, 2013; RTE, 2013], under the objectives of minimizing network vulnerability $V(U_i)$ to cascading failures and minimizing investment costs. The results of the case study have shown that generator-distributor allocation can be optimized to improve the cascading resistance/robustness of a realistic power transmission network system at an acceptable cost.

Then, we have tackled the problem of the *physical* significance of the *topological* optimization results obtained. For this reason, a more detailed, physics-based flow model (namely, the ORNL-Pserc-Alaska – OPA – model) (Section 6.2.2.1) has been embraced. Notice that under this physics-based flow model, network vulnerability $V(U_i)$ has been classically quantified by the system *load shedding*. The OPA model has been performed on five network topologies selected from the Pareto optimal front found by the topological optimization process, in order to *validate a posteriori* the optimal configurations obtained. The ranking of the five selected networks with respect to their vulnerability to both intentional attacks and random failure has been found to be *consistent* with that of the ML model; in addition, the *computational time* required by the ML approach has been shown to be 6 times lower than that of the OPA approach. This has verified: (i) the *physical meaningfulness* of the topological optimization solutions, and (ii) the *practical usefulness* of abstract cascading models in network optimization tasks.

As a further step in the comparison between topological and flow-based models, in [Fang et al., 2015b] we have tackled the problem of searching for the most favorable *pattern* of link *capacity* allocation for a CI power network with the objective of resisting to cascading failures with limited investment costs. As before, low vulnerability and low cost are conflicting objectives: for instance, a network whose components have high capacity can be highly resistant to failures; however, this type of components is often characterized by high costs. The problem has been formulated within a multi-objective optimization framework and has been solved by an evolutionary algorithm, namely

the Non-dominated Sorting Genetic Algorithm II (NSGA-II). The optimization has been carried out using two different approaches to cascade failure modelling: the computationally-cheap topological ML model and the more detailed, flow-based OPA model. Notice that differently from [Fang et al., 2015c], *both* the ML *and* OPA models have been *directly embedded* within the search algorithm for optimally solving the problem of capacity resource allocation.

The approaches have been compared on the FPTN400. Again, the analysis of the behavior of the link capacity patterns of the optimal solutions found has shown that the results provided by the ML and OPA models are *consistent* and *highly correlated*: this means that links with low capacity in ML tend to have low capacity in OPA, and links with high capacity in ML also tend to have high capacity in OPA. This consistency is not insignificant since it demonstrates that one improved pattern of capacity allocation optimized by the ML model is also of higher resistance (i.e., lower vulnerability) if measured by the more realistic OPA model. For further technical details the interested reader is referred to Paper IV [Fang et al., 2015b] reported in the Appendix.

In [Fang et al., 2015a and d], we have instead addressed the problem of *optimization* of system *resilience* $RE(U_i)$ (6). In [Fang et al., 2015a], firstly we have reviewed different definitions of system resilience and different metrics to evaluate it in the context of systems engineering, especially for infrastructure network systems. Then, we have proposed a *novel time-dependent* metric of system resilience focusing on the *post-disaster recovery process*. It has been defined as the *cumulative system functionality* that has been restored at time t, normalized by the *target* cumulative performance as if the system were not affected by disruption during this time period. In details, referring to Figure 13 and to the corresponding notation of Section 6.2.1.2, the time-dependent resilience $RE(t, U_i)$ of a safety-critical system under accident scenario S_i (and affected by uncertainty U_i) has been mathematically defined as:

$$RE(t,U_i)=\frac{\int_{t_d}^{t}[\Phi(\tau,U_i)-\Phi(t_d,U_i)]d\tau}{\int_{t_d}^{t}[\Phi_{TG}(\tau)-\Phi(t_d,U_i)]d\tau}, \tag{7}$$

where $\Phi_{TG}(\tau)$ is the *target* system performance, which is generally evolving in time due to the dynamic nature of service demand in infrastructure systems. For simplicity, it can be assumed that $\Phi_{TG}(\tau)$ equals the initial system performance $\Phi(t_0)$ and remains invariant. This metric is consistent with the basic meaning of resilience and it is able to quantify how a system "*bounces back*" from a disrupted state to an accepted performance, while capturing *at the same time* both the *magnitude* and *rapidity* of the system recovery action (i.e., both the "spatial" and "temporal" dimension of resilience: see Section 6.2.1.2). In addition, notice that the system performance function $\Phi(\cdot)$ in (7)

could be represented by *different* metrics (e.g., the amount of flow or services delivered, the availability of critical facilities, the number of customers served, or the enabling potential of economic activities for infrastructure systems), depending on which dimension (i.e., technical, organizational, social and economic) of resilience the analysis focuses on. This study has concentrated on the *technical* dimension of resilience and has utilized the amount of flow delivered to the demand nodes of a network as the performance level metric.

Based on this resilience definition, the study has provided a framework for considering the role of *recovery decisions* and *actions* in the resilience optimization of infrastructure networks. Specifically, a project-oriented perspective has been applied to plan the process of network's connections recovery after a disruptive event: that is, a *set* of *link repair actions* must be scheduled in an optimal way so as to *maximize* the network resilience over the recovery time. This Resilience Optimization Problem (ROP) has been formulated within a Mixed Integer Programming (MIP) framework. On the other hand, the time required to solve the MIP formulation may impair its application for effective restoration activities after extreme events affecting large-scale infrastructure networks. Therefore, a *heuristic* dispatching rule that integrates fundamental concepts from *network flows* and *project scheduling* has been finally proposed: it seeks to determine the *set* of *link repair tasks* that maximizes the *ratio* between the improvement in system resilience and the *cost* of restoring the set of links.

The application on a case study concerning the FPTN400 has shown that the proposed dispatching rule is able to obtain *high-quality* sub-optimal (and optimal in some cases) solutions to the ROP (actually, the difference with respect to the real, global optimum does not exceed 5%); in addition, the associated computational cost is *much lower* with respect to that of widely adopted commercial MIP solvers (actually, it can be reduced by a factor 5-15).

Finally, based on the new resilience definition in (7), in [Fang et al., 2015d] we have proposed two metrics, i.e. the optimal repair time and the resilience reduction worth, to measure the *criticality* (or the importance) of the components of a network system from the perspective of their *contribution* to system *recovery* or *resilience* after a disruptive event. Specifically, the two metrics quantify: (i) the *priority* with which a failed component should be repaired and re-installed into the network, and (ii) the *potential loss* in the optimal system resilience due to a *time delay* in the recovery of a failed component, respectively. Given the stochastic nature of disruptive events on infrastructure networks, a Monte Carlo-based method is proposed to generate probability distributions of the two metrics for all the components of the network; then, a stochastic ranking approach based on the Copeland's pairwise aggregation is used to rank components importance. The results obtained on the IEEE 30 Bus test system [IEEE, 2014] by the proposed measures have been compared to those

produced by classical topology-based importance measures used in network reliability analysis (e.g., betweenness centrality indices): the difference in the results have shown that classical measures are *not* appropriate to help implement resilience planning because they do *not* take into account system *recovery time*. Instead, the two measures proposed provide insights useful for practical restoration activities of infrastructure networks after suffering a disruptive event.

Finally, notice that the works [Ferrario et al., 2015a and b] under this research issue have been done within the PhD thesis of Elisa Ferrario (Ph.D. 1 in Section 4.3); instead the works [Fang et al., 2015a-d] have been done within the PhD thesis of Yi-Ping (Ph.D. 2 in Section 4.3).

A pictorial representation of the methods here considered and compared to address Issue 1 of research Axis 2 is given in Figure 17, together with the corresponding applications.

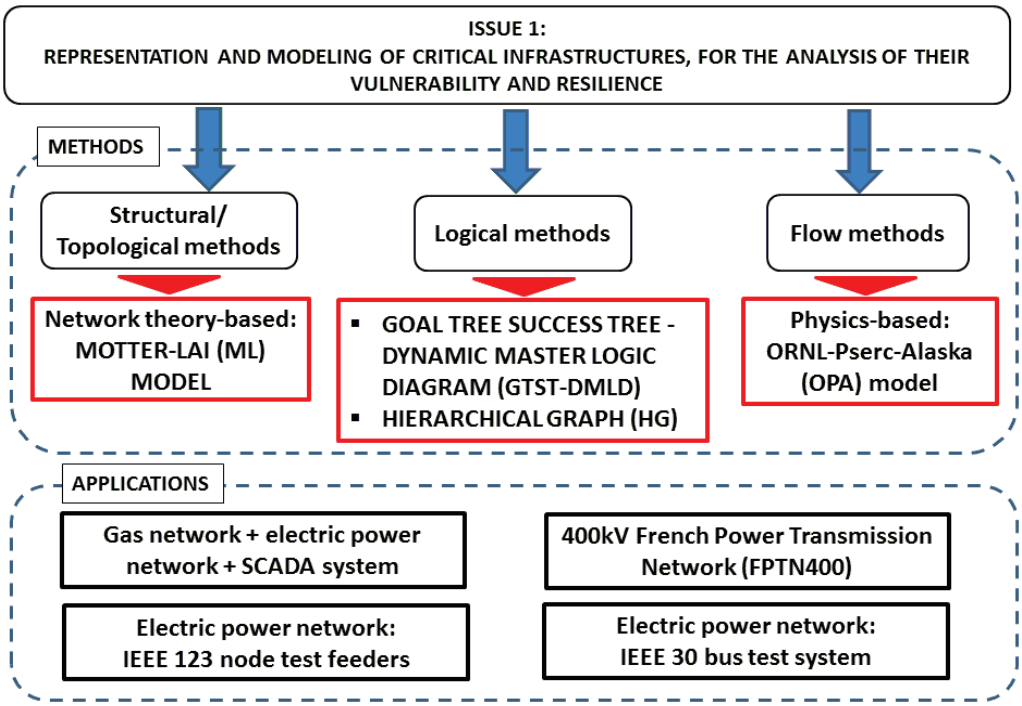


Figure 17. Methods here considered and compared to address Issue 1 of research Axis 2, together with the corresponding applications

6.2.3.2 Issue 2: Design and implementation of innovative algorithms for the efficient risk assessment and/or reliability evaluation of highly-reliable engineered systems and infrastructures

Many of the papers under this research line have been developed during my PhD studies (see [Zio and Pedroni, 2009a-c and 2010a; Pedroni et al., 2010; Zio et al., 2010]): therefore, these works will not be analyzed in details in the present Section. Instead, I will briefly summarize only the content of some works carried out after my PhD (i.e., since 2010).

In the review paper by [Zio and Pedroni, 2011], the outcomes and results of the works cited above have been critically analyzed and synthesized: the objective has been to show how the computational issues associated to the evaluation of the reliability (resp., failure probability) of highly-reliable *emergency passive safety systems* in nuclear reactors can be effectively handled, and to correspondingly provide advices and recommendations[8]. *Different* computational methods have been recommended for efficiently tackling the *different* phases of the reliability assessment of nuclear passive systems: in particular, the optimized Line Sampling (LS) method originally proposed by the author in [Zio and Pedroni, 2010a] has been recommended for small failure probability estimation, whereas the use of Subset Simulation (SS) and bootstrapped meta-models (in particular, Artificial Neural Networks-ANNs) has been suggested for uncertainty propagation and sensitivity analysis in the presence of long-running system model codes. These recommendations have been arrived at on the basis of: (i) a critical review of the methods available in the literature on the subject; (ii) the experience of the authors in nuclear passive systems reliability assessments [Zio and Pedroni, 2009a-c; 2010a and 2012; Pedroni et al., 2010; Zio et al., 2010]; (iii) a thorough comparison of the above mentioned approaches with benchmark methods of literature. For further technical details the interested reader is referred to Paper V [Zio and Pedroni, 2011] reported in the Appendix.

As a further development along this research line, in [Pedroni and Zio, 2015a] we have proposed a *novel* approach, namely, the Adaptive Metamodel-based Subset Importance Sampling (AM-SIS) method, which originally combines the powerful features of three existing techniques, i.e., MCMC-IS, SS and ANNs (see Section 6.2.2.2). The method consists of the following main steps:

1. an estimator of the optimal ISD is constructed in two stages: (a) the SS technique is adopted to generate a population of samples *approximately distributed* according to the optimal Importance Sampling Density (ISD). In order to reduce the computational effort associated to this step, the original long-running system model is replaced by an ANN meta-model, properly *constructed* and *adaptively refined* in *proximity* of the failure region of interest by means of the samples *iteratively* generated by SS; (b) the population thereby created is 'fitted' by means of a proper Probability Density Function (PDF) to obtain an estimator for the optimal ISD: in this paper, a fully nonparametric PDF based on the well-known Gibbs Sampler is employed to this aim;

[8] Notice that emergency safety systems are called "passive" if they do not need external input (especially energy) to operate: on the contrary, they rely on the intelligent use of physical phenomena (e.g., radiation, natural circulation, etc.) to perform their safety function (e.g., the removal of the decay heat in a nuclear reactor after a loss of coolant accident). In this view, passive systems are expected to be highly reliable and to improve the safety of nuclear power plants because of simplicity and reduction of both human interactions and hardware failures.

2. the IS method is applied, in which the ISD estimator constructed at step (1) above is used as an ISD to evaluate the small failure probability (resp., high reliability) of the engineered system of interest.

The performance of the AM-SIS method in the estimation of small failure probabilities (i.e., around 10^{-7}) has been assessed with a very *small* number of samples drawn, i.e., of code evaluations (e.g., of the order of few tens or hundreds): this is important for practical cases in which the computer codes require several hours to run a single simulation. Also, the computational efficiency of AM-SIS has been extensively and systematically compared to that of several probabilistic simulation methods of literature (namely, standard MCS, LHS, IS, AK-IS, SS and optimized LS). The results have shown that AM-SIS outperforms the other approaches in terms of:

i. *accuracy* and *precision* of the failure probability estimates: for example, the standard deviation of the estimator can be 1-3 *orders of magnitude* lower than that of the other methods;
ii. *reduced* overall *computational burden* (i.e., reduced number of random samples drawn and, correspondingly, of expensive system model evaluations): in summary, only *few hundreds* of code runs (i.e., around 400) were necessary for 'completing' the two phases of ISD construction (by ANN and SS) and of failure probability (10^{-7}) evaluation.

The investigations have been carried out with regards to a case study dealing with the reliability analysis of a passive, natural convection-based decay heat removal emergency safety system of a Gas-cooled Fast Reactor (GFR) (modified from [Pagani et al., 2005]).

For what concerns the analysis of highly-reliable *dynamic* and *hybrid* systems, in [Turati et al., 2015a] we have considered the REpetitive Simulation Trials After Reaching Thresholds (RESTART) method, an advanced MCS technique taking its root in *splitting* theory. The approach has shown promising performance in the analysis of dynamic, *discrete* systems [Villén-Altamirano and Villén-Altamirano, 1991; Villén-Altamirano and Villén-Altamirano, 1994], and can be potentially extended to dynamic, *hybrid* systems. The method is based on the random generation of many possible realizations of the life of the dynamic system. Such trajectories are *split* (i.e., "multiplied") when they get close to "interesting" regions of the system state space (i.e., the failure region); on the contrary, the trajectories are *stopped* if they tend to go far from the failure region. This way of proceeding, coupled with a proper weight assigned to each path, allows a more efficient exploration of the system state space and, thus, a reduction of the variance of the corresponding failure probability estimator [Villén-Altamirano and Villén-Altamirano, 2002]. The indication of which trajectories should be split (i.e., of which regions of the state space should be explored more

deeply) is given by a properly selected scalar Importance Function (IF) that results, thus, crucial for the overall performance of the method [Villén-Altamirano and Villén-Altamirano, 2006; Amrein and Künsch, 2011]. In particular, the possibility of embedding the *discrete* and *continuous* variables typically describing a hybrid system within a single scalar importance function has attracted our interest toward this method.

In this view, the objective of the paper has been to show how this widely applied technique can be efficiently employed for hybrid, dynamic, highly reliable systems. For this reason, we have applied the RESTART method to evaluate the failure probability of two systems of literature, whose mathematical models contain both discrete and continuous time-dependent variables: the first is a control system of a liquid hold-up tank [Marseguerra and Zio, 1996] and the second is a system composed by a pneumatic valve and a centrifugal pump subject to degradation [Lin et al., 2015]. The systems have been modeled via Piecewise Deterministic Markov Processes (PDMPs). Although suggestions and guidelines for the construction of proper Importance Functions (IFs) for discrete dynamic systems are given in literature [Villén-Altamirano, 2007; Villén-Altamirano, 2010b; Villén-Altamirano, 2014], *no* indications have been given yet with reference to *hybrid* systems: this has represented the main contribution of our work. The new IFs introduced have been shown capable of considering the *dependences* between the degradation of the process components of the systems: by so doing, the performance of the RESTART has been found to be close to the *optimal theoretical* one derived in [Villén-Altamirano and Villén-Altamirano, 2002].

In [Turati et al., 2015b], we have addressed the problem of thoroughly and intelligently exploring the state space of hybrid dynamic safety-critical systems. In this context, the paper has contributed to IDPSA by proposing an efficient framework for: (i) analyzing, under the constraint of *limited* computational effort (i.e., of a fixed number of available simulations to run), the *possible evolutions* of hybrid dynamic systems; and (ii) identifying those event sequences (i.e., scenarios S_i) that can bring the systems in *unexpected* and/or *extreme* conditions (e.g., in those end states that are *more safety-critical* and/or *rare*).

In particular, we have proposed a method that relies on two phases:

1. in the first, the exploration efforts (i.e. the simulations) are focused on those scenarios having *more uncertain* outcomes (i.e., a higher number of end states for the system). For this purpose, we have exploited a function based on *negative entropy* for assessing the uncertainty in the outcomes and a Bayesian scheme for updating the knowledge gathered by the simulations [Turati et al., 2015c]. As a result, scenarios that can reach a *larger* number of end states are explored more frequently and thoroughly;

2. on the basis of the results of step 1., *new* driving functions are introduced in order to embed into the search the analyst's (acquired) *knowledge* and *preferences*, such as his/her interest for specific scenarios or end states (e.g., those that are *more rare/unexpected* and/or that lead to *more severe consequences*): by so doing, the *guided* exploration of the "interesting" portions of the state space is *deepened* and *refined*.

The performance of the proposed *adaptive semi-automatic guided* exploration framework has been verified on a simple, but representative, case of a dynamic system made by a gas transmission pipe (actively controlled by a valve), which is connected in series to two pipes in parallel: all the components are subject to stochastic failures described by proper probability distributions. The effectiveness of the method has been also compared to that of crude Monte Carlo Sampling and that of a simple, entropy-based search scheme [Turati et al., 2015c]: the results have shown its superiority in *efficiently* and *intelligently* probing and evenly "covering" the system state space. In addition, it has been highlighted that the guided exploration phase (step 2. above) allows running a large number of simulations that lead to the extreme events/scenarios of interest, thus favoring the retrieval of *critical features* and *time dependences* characterizing those events: this can aid analysts and designers to prevent and mitigate dangerous and/or unexpected consequences.

Notice that the works [Turati et al., 2015a-c] under this research issue have been done within the PhD thesis of Pietro Turati (Ph.D. 5 in Section 4.3).

A pictorial representation of the methods here considered and compared to address Issue 2 of research Axis 2 is given in Figure 18, together with the corresponding applications.

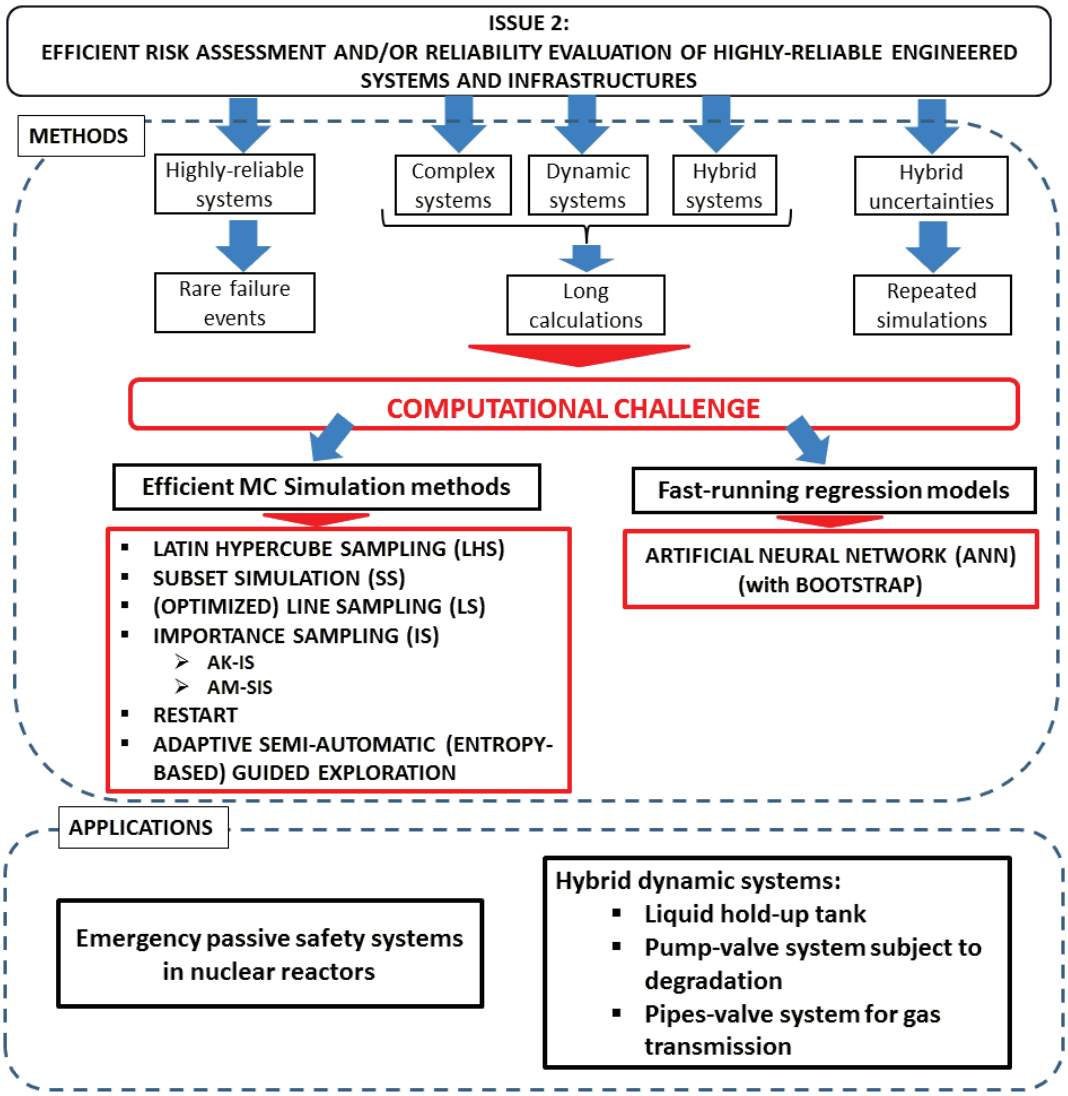


Figure 18. Methods here considered and compared to address Issue 2 of research Axis 2, together with the corresponding applications

6.2.3.3 Issue 3: Development of innovative decision making approaches for the multi-criteria vulnerability analysis of safety-critical systems and infrastructures under uncertainty

In [Wang et al., 2015b], we addressed the issue of evaluating the vulnerability of (a fleet of) safety-critical systems (in particular, Nuclear Power Plants-NPPs) to malevolent intentional acts. With respect to that, due to the specific features (low frequency but important effects) of intentional hazards (characterized by significant *uncertainties* due to behaviors of different rationality) the analysis is difficult to perform by traditional risk assessment methods (see Section 6.2.2.3). For this reason, we have proposed to tackle the problem within a Multi-Criteria Decision Aid (MCDA) framework relying on *empirical classification*. In particular, we have adopted a classification model based on the Majority Rule Sorting (MR-Sort) method [Leroy et al., 2011] to assign an alternative of interest (i.e., a safety-critical system) to a given (vulnerability) class (or category). The MR-Sort classification model contains a group of (adjustable) parameters that have to be calibrated by means

of a set of empirical classification *examples* (also called *training set*), i.e., a set of alternatives with the corresponding pre-assigned vulnerability classes.

Due to the *finite* (typically *small*) size of the set of training classification examples usually available in the analysis of real complex safety-critical systems, the performance of the classification model can be impaired. In particular:

i. the classification *accuracy* (resp., error), that is, the expected fraction of patterns correctly (resp., incorrectly) classified, is typically reduced (resp., increased);
ii. the classification process is characterized by significant uncertainty, which affects the *confidence* of the classification-based vulnerability model: in our work, we define the confidence in a classification assignment as in [Baraldi et al., 2011], that is, as the probability that the class assigned by the model to a given (single) pattern is the correct one.

A quantitative assessment of the performance of the classification model (in terms of *accuracy* and *confidence* in the assignments) is thus needed. This issue has been addressed by three different approaches, namely, the model-retrieval-based method [Leroy et al., 2011], the bootstrap method [Efron and Thibshirani, 1993] and the leave-one-out cross-validation technique [Baraldi et al., 2011]. From the results obtained in a case study involving NPPs it has been concluded that although the model retrieval-based approach may be useful for providing an upper bound on the error rate of the classification model, the *bootstrap* method seems to be *advisable* for the following reasons: (i) it makes use of the training data set available from the particular case study at hand, thus characterizing the uncertainty intrinsic in it; (ii) for each alternative (i.e., safety-critical system) to be classified, it is able to assess the confidence in the classification by providing the probability that the selected vulnerability class is the correct one. This is of paramount importance in the decision making processes involving the vulnerability assessment of safety-critical systems, since it provides a tool to quantify the 'robustness' of a given decision. For further technical details the interested reader is referred to Paper VI [Wang et al., 2015b] reported in the Appendix.

An additional issue related to empirical classification is represented by the fact that the examples provided by the *experts* for the construction of the classification model may contain *contradictions*: thus, a validation of the *consistency* of the data set is opportune. With respect to that, in [Wang et al., 2015a] two approaches have been used to tackle this problem: the inconsistencies in the data examples have been "resolved" by *deleting* or *relaxing*, respectively, some constraints in the process of model construction [Leroy et al., 2011]. The approaches have been successfully tested on a case study involving the assessment of the overall level of safety-related criticality of a group of NPPs.

Finally, in [Wang et al., 2015c and d] the base model developed in [Wang et al., 2015b] has been extended to address the *inverse classification problem* [Aggarwal et al., 2010; Li et al., 2012; Mousseau and Slowinski, 1998] of (optimally) determining a set of *protective actions* that can effectively reduce the level of vulnerability of a safety-critical system, taking into account a specified set of constraints (e.g., budget limits) [Aven and Flage, 2009]. Mathematically speaking, the aim is to identify how to modify some *features* of the input patterns (i.e., the attributes of the safety-critical system under analysis) such that the resulting class is changed as desired (i.e., the vulnerability category is reduced to a desired level).

In [Wang et al., 2015d], *sensitivity indicators* have been originally introduced as measures of the *variation* in the vulnerability class that a safety-critical system is *expected* to undergo after the application of a given set of protective actions. These indicators form the basis of an algorithm to *rank* different combinations of actions according to their effectiveness in reducing the safety-critical systems vulnerability.

In [Wang et al., 2015c], the problem has been instead tackled within an *optimization framework*: the set of protective actions to implement is chosen as the one minimizing the *overall* level of vulnerability of the *group* of safety-critical systems of interest. Three different optimization approaches have been explored: (i) *one single* classification model is built to evaluate and minimize system vulnerability; (ii) an *ensemble* of compatible classification models, generated by the bootstrap method, is employed to perform a "robust" optimization, taking as reference the "*worst-case*" scenario over the group of models; (iii) finally, a *distribution* of classification models, still obtained by bootstrap, is considered to address vulnerability reduction in a "*probabilistic*" fashion (i.e., by minimizing the "expected" vulnerability of the fleet of systems).

The developed methods have been applied fictitious and real NPPs. From the results obtained, it has been concluded that a combination of protective actions can be still obtained using only a single classification model (approach i. above); however, this set of actions is *not robust* with respect to the uncertainty of the classification model. The robust optimization may, then, be used for obtaining a *more conservative* set of actions, coping with model uncertainty. Eventually, the probabilistic optimization seems *most practical* for *real cases*, for the following reasons: (i) as for the robust case, it handles the uncertainty coming from the finite data set available and the compatible models; (ii) by minimizing the *expected value* of the (bootstrapped) probability distribution of the overall vulnerability of the fleet of NPPs, some "extreme" models of the bootstrapped ensembles are "neglected", which is reasonable and more realistic.

Finally, notice that the works [Wang et al., 2015a-d] under this research issue have been done within the PhD thesis of Tai-Ran Wang (Ph.D. 3 in Section 4.3).

A pictorial representation of the methods here considered and compared to address Issue 3 of research Axis 2 is given in Figure 19, together with the corresponding applications.

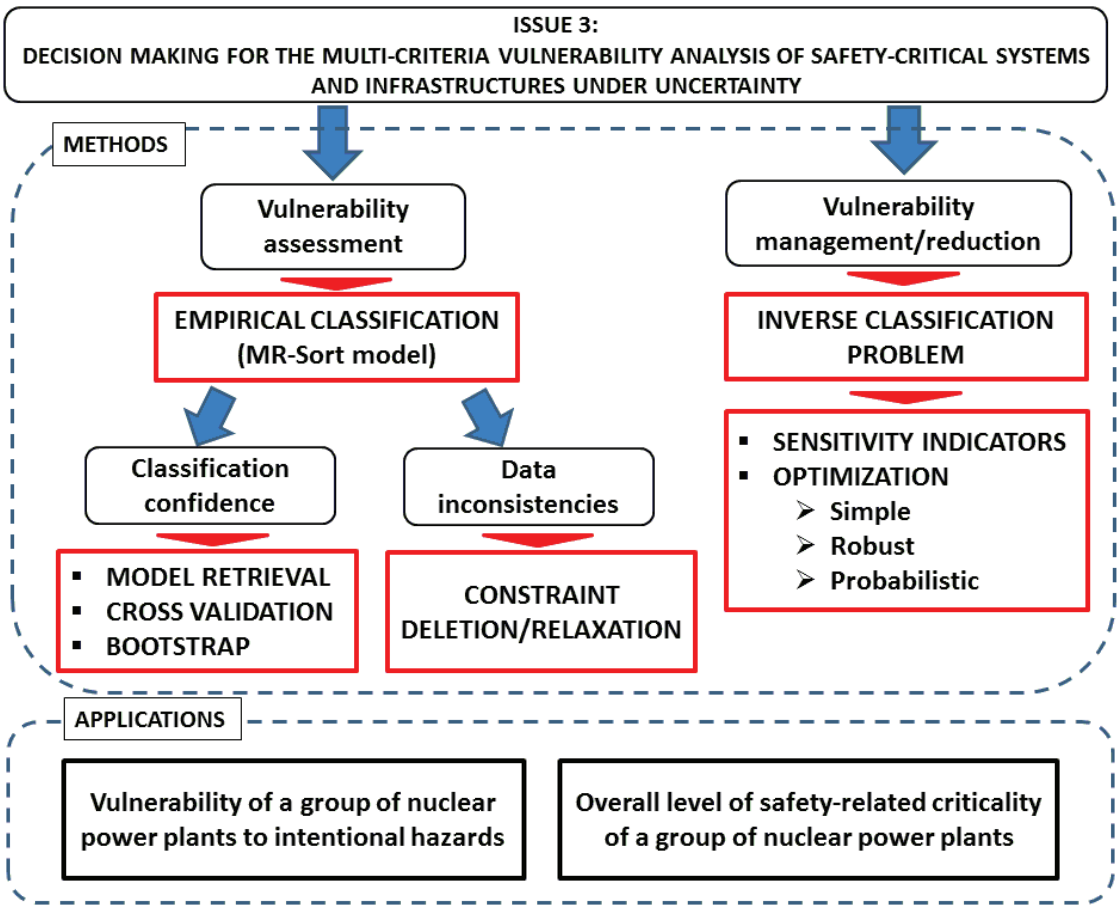


Figure 19. Methods here considered and compared to address Issue 3 of research Axis 2, together with the corresponding applications

7 Detailed presentation of the future research activities

(Présentation détaillée de projet de recherche)

Protection of individual and national interests relies, in part, on our collective capacity to sustain safe, reliable and efficient operation of safety-critical systems (such as nuclear and chemical plants) and infrastructures (such as electric grids, energy and water supplies, communication systems and transport routes). However, there exist many challenges to the fulfillment of these objectives: (i) *increase* in *population* and *weather extremes* (e.g., flooding) now cause unprecedented stress on our aging systems and infrastructures; (ii) *pressure* to work ever more efficiently in a privatized, open market remains a primary factor of risk in such systems; (iii) *security threats* create additional serious challenges to operators; (iv) *technology* continues to evolve, and risks must be dynamically assessed to integrate the potential disruptive power of *new* forms of *attacks* that exploit the technological advancements, e.g., cybercrime and micro Unmanned Aerial Vehicles (UAVs) flying over sensitive facilities; (v) systems and infrastructures have become highly *interconnected*. Risks and vulnerabilities are compounded by systems interdependency in a way that is difficult to understand and address effectively.

Within this broad context, my future research will concern both relevant research *themes* (Section 7.1) and *methods* (Section 7.2).

7.1 Research themes

My future research will be carried out around three main *themes* that are currently credited by many as among the most relevant for the analysis and management of the risk and vulnerability of complex, safety-critical systems and infrastructures:

1. Modeling and analysis of (*extreme*) *external natural events* and the corresponding quantitative assessment of the *robustness* and *resilience* of safety-critical systems and infrastructures with respect to this class of threats and hazards;
2. Integration of the risks and vulnerabilities coming from *cyber attacks*, given that modern industrial installations and infrastructures currently rely on the massive and still increasing use of "soft components", such as Supervisory Control And Data Acquisition-SCADA, information and telecommunication systems;
3. Management of *multiple* risks coming from heterogeneous '*contributors*' (e.g., *different* types of *hazard*, like internal failure events, fires, cyber attacks, earthquakes, floods, etc.) and different '*locations*' (e.g., *different* power production *units* on the same site), for their *aggregate evaluation* according to different and possibly conflicting (safety-related,

environmental, economical, etc.) *criteria*. It is evident how this third theme naturally "envelops" and includes also issues 1. and 2. reported above.

These three *themes* are developed in more details in what follows:

1. It is a recognized fact that *extreme events* and *weather conditions* can cause natural disasters that can impact safety-critical systems (such as nuclear and chemical plants) and infrastructures (such as electric grids, energy and water supply systems, communication systems and transport routes), at the same time putting a strain on emergency and crisis response capabilities, and trigger accidents simultaneously at *several* installations. In addition, *multiple hazards* may develop at the *same time* (e.g., heavy winds and precipitation) or one hazard may trigger others (e.g., an earthquake followed by a tsunami, as in the dramatic catastrophe of Fukushima).

   Furthermore, recent studies predict that climate change will lead to more frequent and more intense natural disasters, also in areas where there are industrial facilities and infrastructures. Under these premises, an increasingly preferable approach to describe and manage systemic risk is to explore and defend against *catastrophic accident* scenarios, on top of the usual consideration given to *reasonably probable* scenarios.

   In this newly arising context of extreme conditions assessment, one of the specific issues that I will address is the *seismic risk assessment* for *nuclear systems* and *components* with adequate treatment of the associated uncertainties. The goal is the quantitative assessment of the (failure) behavior of nuclear systems and components under the occurrence of a seismic event: in more detail, the response of structural systems subject to seismic risk will be studied and the structure fragility curves will be identified, representing the conditional probability of failure of a nuclear component for any given level of seismic excitation. The specific objectives of the research are the following:

   a) the study and development of robust and efficient methods to treat the available (scarce) information of different types, e.g., numerical simulations, expert judgement, real data, etc.;
   b) the quantification and efficient propagation of the (aleatory and epistemic) uncertainties through the (long-running) computer codes (i.e., Finite Element Models-FEMs) typically used to simulate the behavior of structural systems, by advanced simulation techniques and meta-models;
   c) the development of a methodology that is robust enough to be included in a general framework of seismic probabilistic risk assessment for nuclear power plants.

This topic will be the subject of a PhD thesis in collaboration with the Électricité de France (EdF) R&D Department of "Mechanical and Acoustic Analyses" from October 2015 to October 2018.

Another branch of this research theme will regard the probabilistic risk assessment of future *electric power systems*, exposed to natural hazards and extreme weather conditions. These systems are critical for our everyday's life, as they reach virtually every home, school, hospital, office, factory and institution. They are complex systems made of a large number of spatially distributed, interconnected elements (wires and machines), which link the electricity generators to the customers, for satisfaction of their diverse needs.

The *existing* power generation and distribution systems have been developed to meet the requirements of conventional single direction power delivery from centralized high-capacity generation units (e.g. thermal plants, nuclear power plants, etc.) to various end-user loads (e.g. industry, commerce, residence, etc.). However, the energy challenges faced by Europe and the rest of the world are changing the landscape of power systems. For example, originally developed as loosely interconnected networks of local systems, electric power grids have now extended on *large scales*, across regional and national boundaries. In addition, *distributed resources*, mostly in the form of small power generators based on renewable energies (such as photovoltaic panels and wind turbines), that are often geographically separated from the traditional power sources, are being increasingly connected to the existing backbone. The extent of the interconnectedness, the number and variety of power sources and generators, of controls and loads make electric power grids among the most complex engineered systems.

Besides the above mentioned technological challenges, a number of emerging issues are daunting the electric power grid systems and increasing the stress of the environments in which these are to be operated. These are: (a) the deregulated energy market, which has resulted in the systems being operated closer to their capacity and limits, i.e., with reduced safety margins, and consequently in the need for new and balanced business strategies; (b) the prospected demand for electricity in the next 25–50 years, which results in the need to technically respond by increased capacity and efficiency; (c) the sensed increase in the exposure to malevolent attacks that are no longer only hypothetical, which calls for effective protection to a different type of hazard/threat, much more difficult to predict than random failures. In the light of these elements, security and reliability are major concerns for power production and distribution systems.

Actually, a comprehensive evaluation of the risk associated with these systems must consider *contingencies* under *normal* environmental conditions and also *extreme* ones. Environmental conditions can strongly influence the operation and performance of future generation and distribution systems for several reasons. First, the growing shares of renewable-energy generators installed inject considerable amounts of *(aleatory) uncertainty* into power system operation: actually, owing to the *inherently random* nature of the corresponding natural resources, renewable-energy generators behave quite differently from conventional ones. In addition, these systems employ relatively *new technologies*, and this introduces a significant amount of *(epistemic) uncertainty* due to lack of knowledge and/or data on the physical phenomena involved and/or to limited or (possibly) null operating experience of the corresponding components or systems over the wide range of conditions encountered during operation. Finally, several *intrinsically stochastic* environment-related *contingencies* (e.g., high winds, thunderstorms, heavy snows, or even earthquake and flooding events) can damage or deeply degrade the components of the power grid [Rocchetta et al., 2015]. The presence of all these uncertainties puts pressure on decision makers in two directions: (1) to robustly assess the risk associated to the modern power production and distribution systems; (2) to identify by sensitivity analysis those (uncertain) "internal" system elements and "external" environmental contingencies that contribute the most to system risk, with the objective of properly driving resource allocation for uncertainty reduction and consequent confidence gain for design, maintenance and operation decision making.

Differently from classical power system reliability assessments that focus on the evaluation of quantities such as System Average Interruption Duration Index (SAIDI), System Average Interruption Frequency Index (SAIFI) and Expected Energy Not Supplied (EENS) to reflect the ability to supply adequate electric service over the long term, we will embrace a Probabilistic Risk Assessment (PRA) framework for a systemic analysis of system-scale scenarios, and to estimate the probability (or frequency) of such scenarios of disturbance to power system operation and their consequences [McCalley et al., 2004]: these elements are the constituents of risk. As for the boundary of the analysis, the extreme events and weather conditions can also significantly affect system risk by increasing the frequency of failures of the power components and/or inducing severe damage [McCalley et al., 2005]. In addition, the large *spatial scale* of these *distributed* CIs introduces an additional important aspect to consider in the risk analysis: that of the global impact of spatially local hazards [Wilkinson et al., 2012]. Indeed, whereas the spatially local hazards threaten relatively small-scale

systems whose components are located in the hazard influence area, these relatively small-scale systems are usually a part of much larger or national scale systems, and then the impact of localized natural hazards can extend to the large-scale systems they are embedded in. Examples can be found in [Hong et al., 2015] concerning the Chinese railway system under flood hazards and in [Poljansek et al., 2012] with respect to the seismic risk analysis of the European gas and electricity networks. Recently, some works on localized failures have been made by scholars by resorting to a topological approach in the field of complex network theory: see [Shao et al., 2015; Berezin et al., 2015]. However, these purely topology-based studies usually produce the risk results with weak correlations to those results obtained when the infrastructure system flow properties are considered [Cavalieri and Franchin, 2014; Ouyang, 2013; Ouyang et al., 2014].

In order to address these issues related to the *distributed* nature of these power systems on very *large spatial scales*, I plan to put forward a *multi-level* analysis framework, based on two successive stages [Eusgeld et al, 2009]: (i) a *screening analysis* for identifying the parts of the critical infrastructure most relevant with respect to its risk and (ii) a *detailed modeling* of the operational dynamics of the identified parts for gaining insights on the causes and mechanisms responsible for the associated risk. In particular, I will evaluate the potentials of: (i) using *network analysis* based on measures of *topological interconnection* and *reliability efficiency*, for the screening task; (ii) using *object-oriented/agent-based* modeling as the simulation framework to capture the detailed dynamics of the operational scenarios involving the most vulnerable parts of the critical infrastructure as identified by the preceding network analysis. With regards to object-oriented/agent-based modeling, objects/agents can be used to model both technical components such as generators, and non-technical components such as grid operators. The different objects interact with each other directly (e.g., generator dispatch) or indirectly (e.g., via, the physical network). Each object is modeled by attributes, e.g., physical constraints on technical components such as thermal limits of transmission lines, and by rules of behavior, which include both deterministic and stochastic time-dependent processes, each triggered by an input from the object environment. A deterministic process is for instance the outage of a component when its condition reaches a failure threshold, while stochastic processes are probabilistic component failure modes, changing load levels or operator reactions in case of (extreme) contingencies [Eusgeld et al, 2009].

One of the major advantages of an object-oriented approach for modeling and simulating critical infrastructures, is the possibility to include *physical laws* into the simulation and to

emulate the behavior of the infrastructure as it *emerges* from the behaviors of the individual objects and their interactions. In other words, the overall system behavior results from the interactions among the multiple single objects of different kinds which make up the system. This modeling achieves a closer representation of the system behavior by integrating the spectrum of different stochastic phenomena which may occur, thus generating a multitude of representative stochastic, time-dependent event chains. On the other hand, this simulation-based approach becomes *highly computer intensive* for complex realistic infrastructures such as the power generation and distribution systems here of interest. The challenge in this respect is to reduce the computational burden, e.g., making use of rare event simulation techniques or by substituting some objects with empirical meta-models, while quantifying the uncertainty introduced in the approximation of the empirical models (see details below). Eventually, the problem of *optimally designing* these future power generation and distribution systems (possibly including renewable generation sources) in the face of extreme events and conditions will be also tackled in the long term.

2. As mentioned above, critical infrastructures are getting more and more automated, and strongly interconnected due to their increasing extension on large scales and the progressive advances in information technology. For example, today's ability to run largely distributed power networks with a variety of generation technologies (e.g., nuclear, thermo, hydro, etc.) is only possible through the intense use of information and communication systems. Systems that rely on the tight integration of physical processes, computational resources, and communication capabilities are called *cyber-physical systems*. If, on one hand, these advances and interdependences have increased their efficiency (e.g., provide better measurements, allow quicker operations, more powerful control schemes and broad access to data), on the other hand, they have created *new vulnerabilities* to component failures, natural and manmade events. Recent studies and real-world incidents have demonstrated the inability of existing security methods to ensure a safe and reliable functionality of cyber-physical infrastructures against unforeseen failures and, possibly, external attacks [Sridhar et al., 2012]. Actually, Critical Infrastructure Protection (CIP) has gained great importance in all nations, with particular focus being placed traditionally on physical protection and asset hardening [Lewis, 2006]. Proofs of this statement are represented by: (i) the directives of the Department of Homeland Security in the USA [Bush, 2002; Bush, 2003; Clinton, 1998]; (ii) the Thematic Area launched by the European Reference Network for Critical Infrastructure

Protection (ERNCIP) to address the CIP problem systematically; and (iii) the numerous European Union projects on the subject [Klein et al., 2011].

Concerns about security of control systems are not new [Basseville and Nikiforov, 1993; Ding, 2008]. Cyber-physical systems, however, suffer from *specific* vulnerabilities for which appropriate detection, identification and assessment techniques need to be developed. For instance, the reliance on communication networks and standard communication protocols to transmit measurements and control packets increases the possibility of intentional and worst-case (cyber) attacks against physical plants. On the other hand, information security methods (such as authentication, access control, message integrity, and cryptography methods) appear inadequate for a satisfactory protection of cyber-physical systems. Indeed, these security methods do not exploit the *compatibility* of the *measurements* with the underlying *physical process* and *control mechanism*, which are the ultimate objective of a protection scheme [Cardenas et al., 2009]. Moreover, such information security methods are *not effective* against *insider attacks* carried out by authorized entities [Slay and Miller, 2007] and they also fail against attacks targeting directly the *physical dynamics* [De Marco et al., 1996].

This calls for the development of novel methodologies for the assessment of the risk and vulnerability of interdependent critical infrastructures (e.g., power transmission and telecommunication networks) to '*combined*' physical and cyber attacks. The main challenge will be to assess and model the *interactions* between the cyber and the physical security systems to understand the *effects* of cyber technology on *overall* security system effectiveness [SANDIA, 2005; Graves, 2006; Hromada and Lukas, 2012].

This topic will be the subject of a PhD thesis in collaboration with the Électricité de France (EdF) R&D Department of "Measures and Information Systems for Electrical Networks" and the "Research Institute for Smarter Electric Grids" (RISEGrid) from January 2017 to January 2020: the application domain will be that of '*smart grids*', i.e., power transmission networks characterized by an important use of informatics and telecommunication means.

3. Risk aggregation can be defined as the process of combining information on the risk from various: (i) '*contributors*' (i.e., different *types* of hazard – for example, internal failure events, fires, earthquakes, etc.) and (ii) '*locations*' (i.e., different power production units on the same site), in order to provide an overall characterization of risk [EPRI, 2014]. Traditional PRA approaches address these issues respectively as follows: (i) *mean* value contributions to the risk metrics of interest from various hazards are straightforwardly

summed [EPRI, 2014]; (ii) risks from *different* units are considered *separately*, while *dependencies* and *interactions* between the units are introduced *a posteriori*, informally and on an 'ad-hoc' basis [Schroer and Modarres, 2012]. On the other hand, events like the Fukushima nuclear accident mentioned above call for new, more rigorous methods to address multi-hazard, multi-unit site risk. The challenges to the "risk aggregation process" are the following [Yang, 2012; EPRI, 2014; Stutzke, 2014]:

a) The *levels of maturity* of the analyses used in the construction of the PRAs are different for the various hazard groups and for the various units. The principal concern with aggregating the contributions to the risk metrics from the individual contributors to the metrics is the potential for the analysis of the individual contributors to introduce biases and uncertainties that are *not equivalent* across contributors, thus distorting the insights that can be derived from the results. The most commonly cited concern is with the combination of the risk from the various hazard groups by simply adding the mean values for all hazard groups. This concern stems from the acknowledged differences in the capabilities of the methods used to estimate these risk contributions, and the effect this has on the uncertainties in these risk estimates. This is a consequence of the different maturity levels of the methods.

b) Different *degrees of approximations* are made to facilitate the construction of the PRA models for the different hazards and sites. PRA models are a discretized representation of the potential spectrum of accident sequences for a particular plant, and consequently, approximations are a necessary part of creating and quantifying these models. These approximations are made for a number of reasons that include practical considerations, such as the limitation of analytical tools and resource limitations. The degree to which the discretization of the spectrum of accident sequences is developed is to a large extent determined by the level of detail needed to support the purpose of the analysis. In addition, a number of *assumptions* are made during the construction of the model to address the unavailability or limitations of constituent analysis techniques. In some cases, this leads to the use of conservative models and in other cases it leads to the omission of possible risk contributors from the model. This may result in a *non-conservative bias* in the results. Furthermore, it is accepted that a model may necessarily lack certain contributions to risk because they are not known to exist (i.e., the "unknown unknowns"). These approximations and assumptions result in biases on the mean values of risk metrics derived from these PRAs, and their nature is such that the

magnitude of their effects is not easily quantified. These biases are typically, although not always, considered to be conservative. On the other hand, the approximations made when developing the PRA models for different hazard groups result in *differing degrees of bias*; furthermore, the biases will be manifested differently *from analyst to analyst*.

c) The *nature* and *magnitude* of the *uncertainties* associated with the different analyses is extremely varied. The characterization of uncertainty derived from a propagation of *parametric* uncertainties through the PRA models is conditional upon all the assumptions and approximations that have gone into that model. For example, the PRA model for failure events internal to a nuclear power plant is nearly always the basis for the PRA models used to analyze other hazard groups, since it incorporates the potential initiating events and the functions, systems and operator actions required to respond to those initiating events. Common practice is that all other hazard groups are analyzed by determining how a hazard of a specified severity affects the plant in terms of causing an initiating event and causing damage to the structures, systems or components of the plant that support the functions required to respond to the initiating event. There can be significant uncertainties regarding how to model both the frequencies of external hazards and their impacts on the plant. In many cases, the response has been to adopt models that result in a conservative bias on either the frequency of specific hazard events, on their impact on the plant, or both. A "mean" risk estimate derived from a conservative model is clearly not a "true mean" risk value. Furthermore, the existence of *model* uncertainties that are not taken into account explicitly in the evaluation of the mean values implies that there cannot be one single result upon which decisions are made. Rather, there can be several different results, depending on the number of key modeling uncertainties. Finally, *extremely rare* - possibly *never observed* historically - environmental conditions related only to some particular hazards (that have a very high probability of causing significant damage to the plant) may be so uncertain to call into question any classical, probabilistic statistical analysis (and obviously the evaluation of mean values for the risk metrics of interest).

These challenges will be addressed during a PhD work in collaboration with the Électricité de France (EdF) R&D Department of "Industrial Risk Management" from October 2015 to October 2018.

7.2 Research methods

In tackling themes 1.-3. described above, I will contribute to the development of mathematical models of the safety-critical systems and infrastructures of interest for the simulation of their behavior in the presence of uncertainties. In this view, the complexity of the problems and of the systems addressed calls also for further *methodological* research:

1. Novel approaches will be studied and developed that allow dealing with uncertainties in system models with multiple inputs/outputs, which are *functions* of *time* (and possibly of *space*) and show *functional dependencies* and *correlations* between each other. In this broad framework, particular attention will be devoted to the identification by *sensitivity analysis* of those (uncertain) "internal" system elements and "external" environmental contingencies that contribute the most to system risk, with the objective of properly driving resource allocation for uncertainty reduction and consequent confidence gain for design, maintenance and operation decision making [Lamboni et al., 2011; Auder et al., 2012; Gamboa et al., 2013; Collin et al., 2015; Marrel et al., 2015a and b].
2. In order to *reduce* the *computational effort* associated to the risk, vulnerability and resilience assessment of complex safety-critical engineering systems (e.g., in the presence of object-oriented modeling and long-running computer codes), special attention will be devoted to surrogate modeling (meta-modeling), with particular reference to the promising Polynomial Chaos Expansion (PCE) and Stochastic Collocation (SC) techniques. These methods expand (and approximate) the real system response as a truncated series of properly selected basis functions, "calibrated" by means of a *limited-size* set of available computer experiments. In particular, PCE surrogates the computer model with a series of orthonormal polynomials that are chosen in coherency with the probability distributions of the uncertain model input parameters [Ghanem and Spanos, 1991; Sudret, 2008; Blatman and Sudret, 2010; Kersaudy et al., 2015; Schobi et al., 2015; Sudret and Mai, 2015]. Instead, SC is a stochastic expansion method which constructs multidimensional interpolation polynomials over the system responses evaluated at a structured set of collocation points [Babuska et al., 2007; Ng and Eldred, 2012].

   In addition, further efforts will be made in the task of intelligently probing the space of the (undesired) event sequences of the complex, dynamic systems of interest. In particular, I plan to "complement" the research work carried out so far by developing advanced simulation techniques for *scenario analysis*, i.e., methods tailored to the "*creation*" of scenarios of potential future conditions and events of particular interest. In this case, the aim of simulation is *neither* of *completeness nor* of *accuracy* of *estimation*, as in traditional risk

analysis, but rather of enabling the generation of "surprising" scenarios that may provide useful insights about what could happen. Methods of "adjoint" simulation may be of particular interest for generating deductive (anticipatory, backwards) scenarios, where we start from a future imagined event/state of the total system and question what is needed for this to occur. Interpretation of these scenarios by system thinking, to see the holes and interconnections, is critical if one has to identify "black swans" [Aven, 2013; Aven and Krohn, 2014].

A pictorial representation of the themes and methods object of my future research is given in Figure 20.

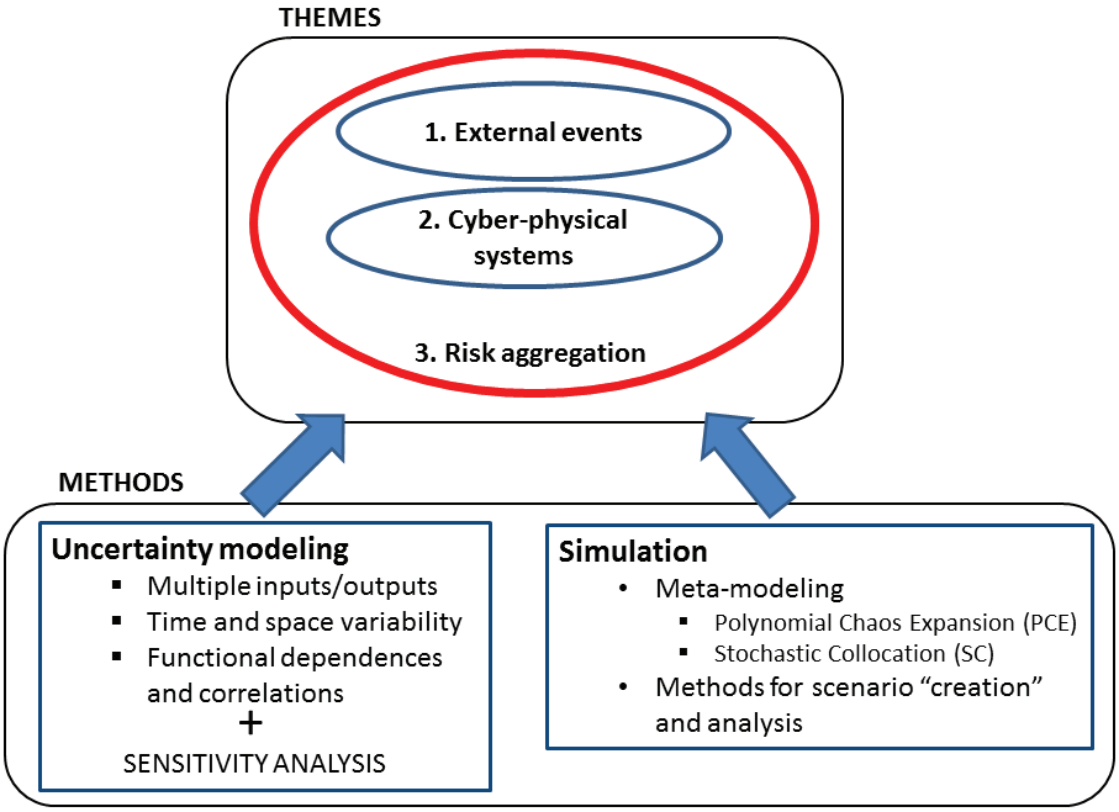


Figure 20. Themes and methods that will be addressed in my future research

The scheduling of the developments of these lines is shown in Table 5. Theme 3 ("risk aggregation") will be the main trunk throughout the coming years because it is *transversal* to different engineering fields and it *envelops* both Theme 1 and 2. There is a preliminary research work that has already started under this Theme by means of the internship of a Master student in collaboration with the EDF R&D department of "Industrial Risk Management": the corresponding Ph.D. will start in October 2015. Themes 1 (2015-2018) and 2 (2017-2019) will at the same time *feed* Theme 3 and *benefit* from its development. In this respect, notice that a Ph.D. in collaboration with the EDF R&D Department of "Mechanical and Acoustic Analyses" has already started in the

field of modeling and analysis of (*extreme*) *external natural events* (Theme 1), with particular emphasis on *seismic risk assessment* for *nuclear systems* and *components*. On the contrary, Theme 2 ("cyber risk") will be launched in 2017 with the expected, more precise definition of the terms of collaboration between the EDF R&D Department of "Measures and Information Systems for Electrical Networks" and the "Research Institute for Smarter Electric Grids" (RISEGrid). The methodological research will be carried out in parallel. Methods for uncertainty and sensitivity analysis (Method 1) and for scenario simulation (Method 2(b)) are obviously needed to support *constantly* the development of *all* the research themes. The use of meta-modeling techniques (Method 2(a)) will be instead particularly useful in the analysis of Theme 1, where I plan to adopt *object-oriented/agent-based* models that are particularly computer intensive.

	Years					
Research	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Themes						
Theme 1: extreme events	**X**	**X**	**X**	**X**		
Theme 2: cyber risk			**X**	**X**	**X**	**X**
Theme 3: risk aggregation	**X**	**X**	**X**	**X**	**X**	**X**
Methods						
Method 1: Uncertainty and sensitivity analysis	**X**	**X**	**X**	**X**	**X**	**X**
Method 2(a): Simulation (meta-modeling)	**X**	**X**	**X**	**X**		
Method 2(b): Simulation (scenario analysis)	**X**	**X**	**X**	**X**	**X**	**X**

Table 5. Planning of the future research activities during 2015-2020

8 Conclusions

From a quantitative point of view, my works include 28 international journal publications (14 on the top journals such as IEEE Systems Journal, Reliability Engineering & Systems Safety, IEEE Transactions on Power Systems, Risk Analysis, IEEE Transactions on Nuclear Science and Computers and Structures), 4 book chapter, 22 communications on the international/national conferences and 5 works published as technical reports of international research institutes. My H-index is 12 on Google scholar, 11 on Scopus and 9 on Web of Science. Many of these publications were co-authored with external academic researchers and industrial partners, justifying our openness and the community recognition from academia and industry. I have co-directed 2 M.Sc. students and 5 Ph.D. students (including 2 pending) evidenced by joint publications. I have participated in 3 international projects or contracts. I have also directed or co-organized 5 sessions or tracks in international conferences. I have exercised numerous scientific reviewing activities for international journals or conferences. Finally, I have been serving as a Guest Editor one international journal (namely, the ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering).

My research activities on advanced models and methods for the risk, vulnerability and resilience assessment of complex, safety-critical engineering components, systems and infrastructures, in the presence of uncertainties were conducted first within the Laboratory of Analysis of Signal and Analysis of Risk (LASAR) of the Energy Department of the Politecnico di Milano (March 2010-February 2013), then within the Chair on System Science and the Energy Challenge (SSEC) (March 2013-present). These activities were initiated by the problems/demands from the national industry applications or from the international academic communities during our participation in various research projects. Particularly, our involvement in the project SINAPS@ (since 2014) and our collaboration contracts with EDF R&D (January 2010-December 2012) and with FonCSI (September 2009-October 2012) have enabled us to enhance our knowledge in connection with other scientific fields and thus develop our scientific themes and build relationships with other European and international universities.

From the teaching viewpoint, I have been co-responsible of the organization and activity of the course “Nuclear Thermo-hydraulics” of an international Master in “Nuclear Energy” at the Commissariat à l'énergie atomique et aux énergies alternatives (CEA)-Institut national des sciences et techniques nucléaires (INSTN) (Saclay, France) for 4 years (2012-2015) and of the course “Managing Uncertainty for Reliability Optimization” of a Research Master at CentraleSupélec for 1 year (2015). In addition to these responsibilities, I have held a large number of lectures during

professional training courses (about 24 hours), Master courses of the Politecnico di Milano (about 25 hours), international Master courses (9 hours), Ph.D. courses offered by the Doctoral School of the Politecnico di Milano (about 30 hours) and international Ph.D. courses (about 17 hours).

All these activities impose a scientific rigor that I can further develop not only in my personal scientific production and in my teaching responsibilities, but also in the doctoral supervision and future works in order to establish our research activity on solid qualitative bases.

I have already obtained the Italian Academic Qualification to be an Associate Professor in the Scientific Disciplinary Area of "Thermodynamics and Nuclear Engineering" in February 2014. However, I have decided to pursue my HDR in France by preparing this thesis because it not only allows me to officially supervise Ph.D. candidates, but it also provides me, through the process of pursuing this qualification, with a deepened understanding of my past, current and future research and an opportunity to improve my articulation and animation abilities. In addition, I want to continue teaching students to transfer as much as possible the results of my research and I also want to take further teaching responsibilities in order to evolve certain teaching activities in line with my research. Finally, the HDR degree will enable me for the qualification of full professor in France which is my career development target for the next 5 years.

9 Bibliography

Aggarwal CC, Chen C, Han JW. The inverse classification problem. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 2010; 25: 458–468.

Albert R, Jeong H, Barabási AL. Error and attack tolerance of complex networks. Nature 2000; 406(6794): 378-382.

Aldemir T. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy 2013; 52: 113-124.

Amin M. Toward self-healing energy infrastructure systems. IEEE Computer Applications in Power 2001; 14(1): 20-28.

Amrein M, Künsch HR. A variant of importance splitting for rare event estimation: Fixed number of successes. ACM Transactions on Modeling and Computer Simulation (TOMACS) 2011; 21(2): Paper n.13.

Anstett-Collin FJ, Goffart J, Mara T, Denis-Vidal L. Sensitivity analysis of complex models: Coping with dynamic and static inputs. Reliability Engineering and System Safety 2015; 134: 268–275.

Apostolakis GE. A commentary on model uncertainty. In: Mosleh A, Siu N, Smidts C, Lui C, Eds. Proceedings of the Workshop on Model Uncertainty: Its Characterization and Quantification; 20-22 October 1993; Annapolis, MD; p. 13-22. Center for Reliability Engineering, University of Maryland, College Park, Maryland; 1993. Also published as Report NUREG/CP-0138. Washington, DC: U.S. Nuclear Regulatory Commission; 1993.

Apostolakis GE. PRA/QRA: an historical perspective. In: 2006 Probabilistic/quantitative risk assessment workshop, 29–30 November 2006, Taiwan.

Apostolakis GE. The concept of probability in safety assessment of technological systems. Science 1990; 250: 1359-1364.

Apostolakis GE. The distinction between aleatory and epistemic uncertainties is important: an example from the inclusion of ageing effects into PSA. Proc. Int. Topl. Mtg. Probabilistic Safety Assessment (PSA '99); August 22-26, 1999; Washington, DC; La Grange Park, Illinois: American Nuclear Society; 1999. p. 135-142.

Apostolakis GE, Kaplan S. Pitfalls in risk calculations. Reliability Engineering 1981; 2(2): 135-145.

Apostolakis GE, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis 2005; 25(2): 361-376.

Apostolakis GE, Piccinelli R, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis 2005; 25: 361–376.

Arul AJ, Iyer NK, Velusamy K. Adjoint operator approach to functional reliability analysis of passive fluid dynamical systems. Reliability Engineering and System Safety 2009; 94: 1917-1926.

Asmussen S, Glynn PW. Stochastic Simulation: Algorithms and Analysis: Algorithms and Analysis, Vol. 57. New York, NY (USA): Springer-Verlag; 2007.

Atwood CL, LaChance JL, Martz HF, Anderson DL, Englehardte M, Whitehead D, Wheeler T. Handbook of Parameter Estimation for Probabilistic Risk Assessment. Technical Report NUREG/CR-6823. Washington, DC: US Nuclear Regulatory Commission. Also published as Technical Report SAND2003-3348P. Albuquerque, New Mexico: Sandia National Laboratories; 2003.

Au SK. Probabilistic Failure Analysis by Importance Sampling Markov Chain Simulation. Journal of Engineering Mechanics 2004; 130(3): 303-311.

Au SK, Beck JL. A new adaptive importance sampling scheme for reliability calculations. Structural Safety 1999; 21: 135-158.

Au SK, Beck JL. Estimation of small failure probabilities in high dimensions by subset simulation. Probabilistic Engineering Mechanics 2001; 16(4): 263-277.

Au SK, Beck JL. Importance sampling in high dimensions. Structural Safety 2003a; 25(2): 139-163.

Au SK, Beck JL. Subset Simulation and its application to seismic risk based on dynamic analysis. Journal of Engineering Mechanics 2003b; 129(8): 1-17.

Au SK, Wang Y. Engineering Risk Assessment with Subset Simulation. Singapore (Singapore): John Wiley & Sons; 2014.

Au SK, Wang ZH, Lo SM. Compartment fire risk analysis by advanced Monte Carlo simulation. Engineering Structures 2007; 29(9): 2381-2390.

Auder B, De Crecy A, Iooss B, Marques M. Screening and metamodeling of computer experiments with functional outputs. Application to thermal–hydraulic computations. Reliability Engineering and System Safety 2012; 107: 122–131.

Aven T. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering & System Safety 2007; 92(6): 745-754.

Aven T. On the Need for Restricting the Probabilistic Analysis in Risk Assessments to Variability. Risk Analysis 2010a; 30(3): 354-360.

Aven T. Some reflections on uncertainty analysis and management. Reliability Engineering and System Safety 2010b; 95: 195-201.

Aven T. Interpretations of alternative uncertainty representations in a reliability and risk analysis context. Reliability Engineering & System Safety 2011a; 96(3): 353-360.

Aven T. On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience Response. Risk Analysis 2011b; 31(5): 693-697.
Aven T. Foundational Issues in Risk Assessment and Risk Management. Risk Analysis 2012a; 32(10): 1647–1656.
Aven T. The risk concept — historical and recent development trends. Reliability Engineering and System Safety 2012b; 99: 33–44.
Aven T. On the meaning of a black swan in a risk context. Safety Science 2013; 57: 44–51.
Aven T. Implications of black swans to the foundations and practice of risk assessment and management. Reliability Engineering & System Safety 2015; 134: 83–91.
Aven T, Flage R. Use of decision criteria based on expected values to support decision-making in a production assurance and safety setting. Reliability Engineering & System Safety 2009; 94: 1491–1498.
Aven T, Heide B. Reliability and validity of risk analysis. Reliability Engineering and System Safety 2009; 94: 1862–1868.
Aven T, Krohn BS. A new perspective on how to understand, assess and manage risk and the unforeseen. Reliability Engineering & System Safety 2014; 121: 1-10.
Aven T, Steen R. The concept of ignorance in a risk assessment and risk management context. Reliability Engineering and System Safety 2010; 95(11): 1117–1122.
Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliability Engineering and System Safety 2010; 96(1): 64-74.
Ayyub BM. Elicitation of Expert Opinions for Uncertainty and Risks. Boca Raton, FL: CRC Press; 2001.
Babuska I, Nobile F, Tempone R. A Stochastic Collocation Method for Elliptic Partial Differential Equations with Random Input Data. SIAM Journal on Numerical Analysis 2007; 45(3): 1005–1034.
Bai YC, Han X, Jiang C, Bi RG. A response-surface-based structural reliability analysis method by using non-probability convex model. Applied Mathematical Modelling 2014; 38(15–16): 3834-3847.
Balesdent M, Morio J, Marzat J. Kriging-based adaptive Importance Sampling algorithms for rare event estimation. Structural Safety 2013; 44: 1–10.
Baraldi P, Pedroni N, Zio E, Ferrario E, Pasanisi A, Couplet M. Monte Carlo and fuzzy interval propagation of hybrid uncertainties on a risk model for the design of a flood protection dike. In: Bérenguer C, Grall A, Guedes Soares C, Eds. Advances in Safety, Reliability and Risk Management. Proceedings of the European Safety and RELiability (ESREL) 2011 Conference; 18-23 September 2011; Troyes, France. London, United Kingdom: Taylor & Francis Group; 2012. p. 2167-2175.
Baraldi P, Razavi-Far R, Zio E. Bagged ensemble of fuzzy c means classifiers for nuclear transient identification. Annals of Nuclear Energy 2011; 38: 1161–1171.
Baraldi P, Zio E. A combined Monte Carlo and possibilistic approach to uncertainty propagation in event tree analysis. Risk Analysis 2008; 28(5): 1309-1325.
Basseville M, Nikiforov IV. Detection of Abrupt Changes: Theory and Application. Englewood Cliffs, NJ (USA): Prentice Hall; 1993.
Battiston S, Delli Gatti D, Gallegati M, Greenwald B, Stiglitz JE. Credit chains and bankruptcy propagation in production networks. Journal of Economic Dynamics and Control 2007; 31(6): 2061-2084.
Baudrit C, Couso I, Dubois D. Joint propagation of probability and possibility in risk analysis: toward a formal framework. Internat. J. Approx. Reasoning 2007a; 45(1): 82–105.
Baudrit C, Dubois D. Comparing Methods for Joint Objective and Subjective Uncertainty Propagation with an example in a risk assessment. In: Cozman FG, Nau R, Seidenfeld T, Eds. Proceedings of the Fourth International Symposium on Imprecise Probabilities and Their Applications (ISIPTA '05); 20/07/2005-23/07/2005; Pittsburgh, PA (USA); 2005a.
Baudrit C, Dubois D. Practical Representations of Incomplete Probabilistic Knowledge. Computational Statistics & Data Analysis 2006; 51(1): 86-108.
Baudrit C, Dubois D, Fargier H. Propagation of uncertainty involving imprecision and randomness. In: Proc. of the International Conference in Fuzzy Logic and Technology (EUSFLAT03); 10/09/2003-12/09/2003; Zittau, Germany; 2003. p. 653-658.
Baudrit C, Dubois D, Guyonnet D. Joint Propagation and Exploitation of Probabilistic and Possibilistic Information in Risk Assessment. IEEE Transactions on Fuzzy Systems 2006; 14(5): 593-608.
Baudrit C, Dubois D, Perrot N. Representing parametric probabilistic models tainted with imprecision. Fuzzy Sets and System 2008; 159(15): 1913-1928.
Baudrit C, Guyonnet D, Dubois D. Joint propagation of variability and imprecision in assessing the risk of groundwater contamination. Journal of Contaminant Hydrology 2007b; 93: 72–84.
Baudrit C, Guyonnet D, Dubois D. Post-processing the hybrid method for addressing uncertainty in risk assessments. Journal of the Environmental Engineering Division, ASCE 2005b; 131(12): 1750–1754.
Bayarri MJ, Berger JO, Paulo R, Sacks J, Cafeo JA, Cavendish J, Lin CH, Tu J. A framework for validation of computer models. Technometrics 2007; 49: 138-154.
Bect J, Ginsbourger D, Li L, Picheny V, Vazquez E. 2012. Sequential design of computer experiments for the estimation of a probability of failure. Stat Comput, 22: 773–93.

Bedford T, Cooke R. Probabilistic Risk Analysis. Foundations and Methods. Cambridge (UK): Cambridge University Publishing Ltd; 2001.
Beer M. Engineering quantification of inconsistent information. Int J Reliability and Safety 2009a; 3(1/2/3): 174–197.
Beer M. Fuzzy probability theory. In: Meyers RA, Ed. Encyclopedia of Complexity and Systems Science - Vol.6. New York (NY): Springer; 2009b. p. 4047–4059.
Beer M, Ferson S. Special issue of Mechanical Systems and Signal Processing "Imprecise probabilities - What can they add to engineering analyses?". Mechanical Systems and Signal Processing 2013; 37(1-2): 1-3.
Beer M, Ferson S, Kreinovich V. Imprecise probabilities in engineering analyses. Mechanical Systems and Signal Processing 2013a; 37(1-2): 4-29.
Beer M, DiazDelaO FA, Patelli E, Au SK. Conceptual comparison of Bayesian approaches and imprecise probabilities. In: Topping BHV, Ivanyi P (eds.). Computational Technology Reviews. Saxe-Coburg Publications; 2014a. Vol. 9, p. 1-29.
Beer M, Kougioumtzoglou IA, Patelli E. Emerging Concepts and Approaches for Efficient and Realistic Uncertainty Quantification. In: Frangopol DM, Tsompanakis Y., eds. Maintenance and Safety of Aging Infrastructure, Book Series "Structures & Infrastructures". Boca Raton, FL; London, UK; New York, NY: CRC Press, Taylor & Francis Group; 2014. Vol 10, Chapter 5, p. 121–154.
Beer M, Zhang Y, Quek ST, Phoon KK. Reliability analysis with scarce information: Comparing alternative approaches in a geotechnical engineering context. Structural Safety 2013b; 41: 1–10.
Belton V, Stewart T. Multiple Criteria Decision Analysis – An Integrated Approach. Berlin, Germany: Kluwer Academic Publishers; 2002.
Berezin Y, Bashan A, Danziger MM, Li D, Havlin S. Localized attacks on spatially embedded networks with dependencies. Scientific reports 2015; 5: Paper n. 8934.
Bergman B. Conceptualistic pragmatism: a framework for Bayesian analysis? IIE Transactions 2009; 41: 86-93.
Berleant D, Anderson G, Goodman-Strauss C. Arithmetic on Bounded Families of Distributions: A DEnv Algorithm Tutorial. In: Hu C et al., Eds. Knowledge Processing with Interval and Soft Computing. London, UK: Springer-Verlag; 2008. p. 183-210.
Berleant D, Goodman-Strauss C. Bounding the results of arithmetic operations on random variables of unknown dependency using intervals. Reliable Computing 1998; 4: 147-165.
Berleant D, Xie L, Zhang J. Statool: a tool for distribution envelope determination (DEnv), an interval-based algorithm for arithmetic on random variables. Reliab Comput 2003; 9(2): 91–108.
Berleant D, Zhang J. Representation and problem solving with Distribution Envelope Determination (DEnv). Reliability Engineering and System Safety 2004a; 85: 153-168.
Berleant D, Zhang J. Using Pearson correlation to improve envelopes around the distributions of functions. Reliable Computing 2004b; 10: 139-161.
Bernardo JM, Smith AFM. Bayesian Theory. Chichester (UK): Wiley; 1994.
Bernardo JM. The concept of exchangeability and its applications. Far East Journal of Mathematical Sciences 1996; 4: 111-121.
Bichon B, Eldred M, Swiler L, Mahadevan S, McFarland J. Efficient global reliability analysis for nonlinear implicit performance functions. AIAA Journal 2008; 46(10): 2459–2468.
Bishop CM. Neural Networks for pattern recognition. New York, NY, USA: Oxford University Press; 1995.
Blatman G, Sudret B. Efficient computation of global sensitivity indices using sparse polynomial chaos expansions. Reliability Engineering and System Safety 2010; 95: 1216–1229.
Blockley D. Analyzing uncertainties: Towards comparing Bayesian and interval probabilities. Mechanical Systems and Signal Processing 2013; 37(1-2): 30-42.
Blom, HAP et al. Stochastic hybrid systems: theory and safety critical applications. Vol. 337. Heidelberg, Germany: Springer-Verlag; 2006.
Bobbio A, Bonanni G, Ciancamerla E, Clemente R, Iacomini A, Minichino M, Scarlatti A, Terruggia R, Zendri E. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. Reliability Engineering & System Safety 2010; 95(12): 1345-1357.
Bompard E, Gao C, Napoli R, Russo A, Masera M, Stefanini A. Risk assessment of malicious attacks against power systems. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 2009; 39(5): 1074-1085.
Borshchev A, Filippov A. From System Dynamics and Discrete Event to Practical Agent Based Modeling: Reasons, Techniques, Tools. Proceedings of the 22nd International Conference of the System Dynamics Society; July 25 - 29, 2004; Oxford, England. p. 45.
Botev ZI et al. Static network reliability estimation via generalized splitting. INFORMS Journal on Computing 2013a; 25(1): 56-71.
Botev ZI, Kroese DP. An efficient algorithm for rare-event probability estimation, combinatorial optimization, and counting. Methodology and Computing in Applied Probability 2008; 10(4): 471-505.
Botev ZI, Kroese DP. Efficient Monte Carlo simulation via the generalized splitting method. Statistics and Computing 2012; 22(1): 1-16.

Botev ZI, L'Ecuyer P, Tuffin B. Markov chain importance sampling with applications to rare event probability estimation. Statistics and Computing 2013b; 23(2): 271-285.
Bourinet JM, Deheeger F, Lemaire M. Assessing small failure probabilities by combined subset simulation and Support Vector Machines. Struct. Saf. 2011; 33: 343–353.
Brans JP, Mareschal B, Vincke P. How to select and how to rank projects: The promethee method. European Journal of Operational Research 1986; 24: 228–238.
Brans JP, Vincke P. A preference ranking organization method: the promethee method for multiple criteria decision-making. Management Science 1985; 31: 647–656.
Breeding RJ, Helton JC, Gorham ED, Harper FT. Summary Description of the Methods Used in the Probabilistic Risk Assessments for NUREG-1150. Nuclear Engineering and Design 1992a; 135(1): 1-27.
Breeding RJ, Helton JC, Murfin WB, Smith LN, Johnson JD, Jow H-N, Shiver AW. The NUREG-1150 Probabilistic Risk Assessment for the Surry Nuclear Power Station. Nuclear Engineering and Design 1992b; 135(1): 29-59.
Brown TD, Breeding RJ, Helton JC, Jow H-N, Higgins SJ, Shiver AW. The NUREG-1150 Probabilistic Risk Assessment for the Grand Gulf Nuclear Station. Nuclear Engineering and Design 1992; 135(1): 117-137.
Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney K, Wallace WA, von Winterfeldt D. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra 2003; 19(4): 733-752.
Bucher C, Most T. A comparison of approximate response function in structural reliability analysis. Probabilistic Engineering Mechanics 2008; 23: 154-163.
Buckle P, Mars G, Smale S. New approaches to assessing vulnerability and resilience. Australian Journal of Emergency Management 2000; 15(2): 8-14.
Buckley JJ. Fuzzy probabilities — new approach and applications. Studies in Fuzziness and Soft Computing - vol.115. Berlin, Heidelberg: Springer-Verlag; 2005.
Bush GW. Homeland Security Presidential Directive-3 (HSPD-3). Washington, DC; 2002.
Bush GW. Homeland Security Presidential Directive-7 (HSPD-7). Washington, DC; 2003.
Cacuci DG, Ionescu-Bujor M. A comparative review of sensitivity and uncertainty analysis of large scale systems – II: Statistical methods. Nuclear Science and Engineering 2004; 147: 204-217.
Cadini F, Avram D, Pedroni N, Zio E. Subset Simulation of a reliability model for radioactive waste repository performance assessment. Reliability Engineering and System Safety 2012; 100: 75-83.
Cadini F, Gioletta A, Zio E. Improved metamodel-based importance sampling for the performance assessment of radioactive waste repositories. Reliability Engineering and System Safety 2015; 134: 188–197.
Cadini F, Santos F, Zio E. An improved adaptive kriging-based importance technique for sampling multiple failure regions of low probability. Reliability Engineering and System Safety 2014a; 131: 109–117.
Cadini F, Santos F, Zio E. Passive systems failure probability estimation by the meta-AK-IS2 algorithm. Nuclear Engineering and Design 2014b; 277: 203–211.
Cailloux O, Mousseau V. Parameterize a territorial risk evaluation scale using multiple experts knowledge through risk assessment examples. Advances in Safety, Reliability and Risk Management. London, UK: Taylor and Francis Group; 2011. p. 2331– 2339.
Cardenas AA, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S. Challenges for securing cyber physical systems. In: Proceedings of the Workshop on Future Directions in Cyber-physical Systems Security; 23 Jul. 2009; Newark, NJ, USA.
Cardoso JB, De Almeida JR, Dias JM, Coelho PG. Structural reliability analysis using Monte Carlo simulation and neural networks. Advances in Engineering Software 2008; 39: pp. 505-513.
Carreras BA, Lynch VE, Dobson I, Newman DE. Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos: An interdisciplinary journal of nonlinear science 2002; 12(4): 985-994.
Casalicchio E, Bologna S, Brasca L, Buschi S, Ciapessoni E, D'Agostino G, Fioriti V, Morabito F. Inter-dependency Assessment in the ICT-PS Network: The MIA Project Results. In: Xenakis C, Wolthusen S, eds. Critical Information Infrastructures Security. Berlin Heidelberg: Springer; 2011. p. 1-12.
Cassandras CG, Lygeros J. Stochastic hybrid systems. Boca Raton, FL: CRC Press, Taylor & Francis group; 2006.
Catalyurek U, et al. Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees. Reliability Engineering & System Safety 2010; 95(3): 278-294.
Cavalieri F, Franchin P. Models for seismic vulnerability analysis of power networks: comparative assessment. Computer-aided civil and infrastructure engineering 2014; 29: 590-607.
Čepin M., Mavko B. A dynamic fault tree. Reliability Engineering & System Safety 2002; 75(1): 83-91.
Cérou F et al. Sequential Monte Carlo for rare event estimation. Statistics and Computing 2012; 22(3): 795-808.
Cheng J, Li QS, Xiao RC. A new artificial neural network-based response surface method for structural reliability analysis. Probabilistic Engineering Mechanics 2008; 23: 51-63.
Ching J, Beck JL, Au SK. Hybrid subset simulation method for reliability estimation of dynamical systems subject to stochastic excitation. Probabilistic Engineering Mechanics 2005; 20: 199-214.
Cimellaro GP, Reinhorn AM, Bruneau M. Framework for analytical quantification of disaster resilience. Engineering Structures 2010; 32(11): 3639-3649.

Clinton W. Presidential Decision Directive PDD-63: Protecting America's Critical Infrastructures. Washington, DC (USA); 1998.
COM. Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism. Brussels, Belgium: Commission of the European Community; 2004.
Cooke R. Experts in Uncertainty: Opinion and Subjective Probability in Science. Oxford, New York: Oxford University Press; 1991.
Coolen FPA, Utkin LV. Imprecise probability: a concise overview. In: Aven T, Vinnem JE, Eds. Risk, reliability and societal safety. Proceedings of the European safety and reliability conference (ESREL) 2007; 25-27 June 2007; Stavanger, Norway; London, UK: Taylor & Francis Group, 2007. p. 1959-66.
Cooper R, Ferson S, Ginzburg L. Hybrid Processing of Stochastic and Subjective Uncertainty Data. Risk Analysis 1996; 16(6): 785-791.
Cotilla-Sanchez E, Hines PD, Barrows C, Blumsack S. Comparing the topological and electrical structure of the North American electric power infrastructure. IEEE Systems Journal 2012; 6(4): 616-626.
Cox LA. Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small? Risk Analysis 2011; 31(10): 1530-1533.
Crespo LG, Kenny SP, Giesy DP. Reliability analysis of polynomial systems subject to p-box uncertainties. Mechanical Systems and Signal Processing 2013; 37(1-2): 121-136.
Crespo LG, Kenny SP, Giesy DP. The NASA Langley Multidisciplinary Uncertainty Quantification Challenge. Proceedings of the 16th AIAA Non-Deterministic Approaches Conference; 13 - 17 January 2014; National Harbor, Maryland (USA). Reston, VA: American Institute of Aeronautics and Astronautics; 2014. pp. 1-10. doi: 10.2514/6.2014-1347.
Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks. Physical Review E 2004; 69(4): paper 045104.
Crucitti P, Latora V, Marchiori M. Locating critical lines in high-voltage electrical power grids. Fluctuation and Noise Letters 2005; 5(02): L201-L208.
Crucitti P, Latora V, Porta S. Centrality measures in spatial networks of urban streets. Physical Review E 2006; 73(3): paper 036125.
Cullen AC, Frey HC. Probabilistic Techniques in Exposure Assessment: A Handbook for Dealing with Variability and Uncertainty in Models and Inputs. New York, NY: Plenum Press; 1999.
De Boer P.-T. et al. A tutorial on the cross-entropy method. Annals of operations research 2005; 134(1): 19-67.
De Finetti B. Theory of Probability. New York, NY: Wiley; 1974.
De Marco CL, Sariashkar JV, Alvarado F. The potential for malicious control in a competitive power systems environment. In: Proceedings of the IEEE Int. Conf. on Control Applications; Dearborn, MI, USA; 1996. p. 462–467.
Dempster AP. Upper and Lower Probabilities Induced by a Multivalued Mapping. Annals of Mathematical Statistics 1967a; 38: 325-339.
Dempster AP. Upper and Lower Probability Inferences Based on a Sample from a Finite Univariate Population. Biometrika 1967b; 54(2-3): 515-528.
Deng J. Structural reliability analysis for implicit performance function using radial basis functions. International Journal of Solids and Structures 2006; 43: 3255-3291.
Dilley M, Boudreau TE. Coming to terms with vulnerability: a critique of the food security definition. Food policy 2001; 26(3): 229-247.
Ding SX. Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools. London, UK: Springer; 2008.
Dobson I, Carreras B, Lynch V, Newman D. (2001). An initial model for complex dynamics in electric power system blackouts. In: Proceedings of the 46th Hawaii International Conference on System Sciences; 7-10 Jan. 2013; Wailea, Maui, HI USA. IEEE Computer Society; 2013. p. 2017-2017.
Dubois D, Guyonnet D. Risk-Informed Decision Making in the Presence of Epistemic Uncertainty. Int. J. General Systems 2011; 40(2): 145-167
Dubois D, Prade H. Bayesian conditioning in possibility theory. Fuzzy Sets and Systems 1997; 92: 223-240.
Dubois D, Prade H. Possibility Theory: An Approach to Computerized Processing of Uncertainty. New York (NY): Plenum Press; 1988.
Dubois D. Possibility Theory and Statistical Reasoning. Computational Statistics and Data Analysis 2006; 51: 47-69.
Dubois D. Representation, propagation and decision issues in risk analysis under incomplete probabilistic information. Risk Analysis 2010; 30: 361–368.
Dubourg V, Sudret B, Deheeger F. Metamodel-based importance samplingfor structural reliability analysis. Probab. Eng. Mech. 2013; 33: 47–57.
Dueñas-Osorio L, Craig JI, Goodno, BJ. Seismic response of critical interdependent networks. Earthquake Engineering & Structural Dynamics 2007; 36(2): 285-306.
Echard B, Gayton N, Lemaire M. AK-MCS: an active learning reliability method combining Kriging and Monte Carlo simulation. Struct. Saf. 2011; 33: 145–154.

Echard B, Gayton N, Lemaire M, Relun N. A combined Importance Sampling and Kriging reliability method for small failure probabilities with time-demanding numerical methods. Reliab. Eng. Syst. Saf. 2013; 111: 232–240.
EDF. En direct de nos centrales, http://france.edf.com/france-45634.html. Retrieved April 2013.
Efron B, Thibshirani RJ. An introduction to the bootstrap. Monographs on statistics and applied probability 57. New York, NY (USA): Chapman and Hall; 1993.
EPRI (Electric Power Research Institute). An Approach to Risk Aggregation for Risk-Informed Decision-Making. Technical Report 3002003116. Palo Alto, CA (USA): Electric Power Research Institute (EPRI); 2015.
Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliability Engineering & System Safety 2009; 94(5): 954-963.
Eusgeld I, Nan C, Dietz S. System-of-systems approach for interdependent critical infrastructures. Reliability Engineering & System Safety 2011; 96(6): 679-686.
Fang YP, Pedroni N, Zio E. Assessment and optimization of the resilience of infrastructure network systems subject to disruptive events. Under first review on IEEE Systems Journal 2015a.
Fang YP, Pedroni N, Zio E. Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network. Accepted for publication on IEEE Systems Journal 2015b, doi: 10.1109/JSYST.2014.2352152.
Fang YP, Pedroni N, Zio E. Optimization of Cascade-Resilient Electrical Infrastructures and its Validation by Power Flow Modelling. Risk Analysis, an International Journal 2015c; 35(4): 594–607.
Fang YP, Pedroni N, Zio E. Resilience-based component importance measures for critical infrastructure network systems. Under second review on IEEE Transactions on Reliability 2015d.
Fang YP, Zio E. Unsupervised spectral clustering for hierarchical modelling and criticality analysis of complex networks. Reliability Engineering & System Safety 2013; 116: 64-74.
Fauriat W, Gayton N. AK-SYS: an adaptation of the AK-MCS method for system reliability. Reliab Eng Syst Saf 2014; 123: 137–44.
Ferdous R, Khan F, Sadiq R, Amyotte P, Veitch B. Fault and Event Tree Analyses for Process Systems Risk Analysis: Uncertainty Handling Formulations. Risk Analysis 2011; 31(1): 86-107.
Ferrario E, Pedroni N, Zio E. Analysis of the robustness and recovery of critical infrastructures by Goal Tree Success Tree – Dynamic Master Logic Diagram, within a multi-state system-of-systems framework, in the presence of epistemic uncertainty. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering (Special Issue on Non-probabilistic Approaches for Handling Uncertainty in Engineering) 2015a; 1(3): paper 031001, 14 pages. doi: 10.1115/1.4030439.
Ferrario E, Pedroni N, Zio E. Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation. Under first review on Reliability Engineering and System Safety 2015b.
Ferson S. Bayesian methods in risk assessment. Technical Report available at: www.ramas.com/bayes.pdf; 2005.
Ferson S. What Monte Carlo methods cannot do. Human and Environmental Risk Assessment 1996; 2: 990–1007.
Ferson S, Burman MA. Correlation, dependency bounds and extinction risks. Biol. Conserv. 1995; 73: 101–105.
Ferson S, Ginzburg LR. Different methods are needed to propagate ignorance and variability. Reliability Engineering and Systems Safety1996; 54: 133–144.
Ferson S, Hajagos JG. Arithmetic with uncertain numbers: rigorous and (often) best possible answers. Reliability Engineering and System Safety 2004; 85: 135-152.
Ferson S, Kreinovich V, Ginzburg L, Sentz K, Myers DS. Constructing probability boxes and Dempster-Shafer structures. Technical Report SAND2002-4015. Albuquerque, New Mexico: Sandia National Laboratories; 2003.
Ferson S, Kreinovich V, Hajagos J, Oberkampf W, Ginzburg L. Experimental Uncertainty Estimation and Statistics for Data Having Interval Uncertainty. Technical Report SAND2007-0939. Albuquerque, New Mewico: SANDIA National Laboratories; 2007.
Ferson S, Long TF. Conservative uncertainty propagation in environmental risk assessments. In: Hughes JS, Biddinger GR, Mones E, Eds. Environmental Toxicology and Risk Assessment - Third Volume, ASTM STP 1218. Philadelphia, PA: American Society for Testing and Materials; 1995. p. 97–110.
Ferson S, Nelsen RB, Hajagos J, Berleant DJ, Zhang J, Tucker WT, Ginzburg LR, Oberkampf WL. Dependence in probabilistic modeling, Dempster-Shafer theory, and probability bounds analysis. Technical Report SAND2004-3072. Albuquerque, New Mexico: SANDIA National Laboratories; 2004.
Ferson S, Tucker WT. Sensitivity in risk analyses with uncertain numbers. Technical Report SAND2006-2801. Albuquerque, New Mewico: SANDIA National Laboratories; 2006.
Ferson S, Van den Brink P, Estes TL, Gallagher K, O'Connor R, Verdonck F. Bounding uncertainty analyses. In: Warren-Hicks WJ, Hart A, Eds. Application of uncertainty analysis to ecological risks of pesticides. Pensacola and Boca Raton (FL): SETAC and CRC Press; ISBN 9781439807347; 2010.
Fetz T. Sets of joint probability measures generated by weighted marginal focal sets. In: de Cooman G, Fine TL, Seidenfeld T, Eds. Proceedings of the Second International Symposium on Imprecise Probability and Their Applications; 26 - 29 June 2001; Cornell University: Ithaca, NY (USA); Maastricht, The Netherlands: Shaker Publishing; 2001. pp. 171-178.

Fetz T, Oberguggenberger M. Propagation of uncertainty through multivariate functions in the framework of sets of probability measures. Reliability Engineering and System Safety 2004; 85: 73-87.
Flage R, Aven T, Zio E. Alternative representations of uncertainty in reliability and risk analysis – review and discussion. In: Martorell S, Guedes Soares C, Barnett J, editors. Safety, reliability and risk analysis - Theory, methods and applications. Proceedings of the European safety and reliability conference 2009 (ESREL 2009); 22–25 September 2008; Valencia, Spain. London (UK): CRC Press; 2009. p. 2081–2091.
Flage R, Baraldi P, Zio E, Aven T. Possibility-probability transformation in comparing different approaches to the treatment of epistemic uncertainties in a fault tree analysis. In: Ale B, Papazoglu IA, Zio E, Eds. Reliability, Risk and Safety. Proceedings of the European Safety and Reliability (ESREL) 2010 Conference; 5-9 September 2010; Rhodes, Greece; London, United Kingdom: Taylor & Francis Group; 2010. ISBN 978-0-415-60427-7. p. 714-721.
Flammini F, Gaglione A, Mazzocca N, Pragliola C. Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. Critical Information Infrastructures Security 2009; 5508: 180-189.
Fong CJ, Apostolakis GE, Langewish DR, Hejzlar P, Todreas NE, Driscoll MJ. Reliability analysis of a passive cooling system using a response surface with an application to the flexible conversion ratio reactor. Nuclear Engineering and Design 2009; 239(12): 2660-2671.
Frank MJ, Nelsen RB, Schweizer B. Best-possible bounds for the distribution of a sum—a problem of Kolmogorov. Probability Theory and Related Fields 1987; 74: 199-211.
Fréchet M. Généralisations du théorème des probabilités totales. Fundamenta Mathematica 1935; 25: 379-387.
Frey HC, Burmaster DE. Methods for Characterizing Variability and Uncertainty: Comparison of Bootstrap Simulation and Likelihood-Based Approaches. Risk Analysis 1999; 19(1): 109-130.
Gamboa F, Janon A, Klein T, Lagnoux A. Sensitivity analysis for multidimensional and functional outputs. Electron. J. Statist 2014; 8(1): 575-603.
Garrick BJ, Gekler WC, Goldfisher L, Karcher RH, Shimizu B, Wilson JH. Reliability analysis of nuclear power plant protective systems. HN-190 USAEC Research and Development Report, UC-80 Reactors General TID-4500 Distribution. Los Angeles, California (USA): Holmes and Narver, Inc.; 1967.
Ghanem RG, Spanos PD. Stochastic finite elements: a spectral approach. Berlin, Germany: Springer; 1991.
Gheorghe AV, Schlapfer M. Ubiquity of digitalization and risks of interdependent critical infrastructures. Proceedings of the 2006 IEEE International Conference on Systems, Man, and Cybernetics; October 8-11, 2006; Taipei, Taiwan. IEEE Systems, Man, and Cybernetics Society; 2006. p. 580-584.
Gordon KA, Wyss GD. Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness. Technical Report SAND 2005-7177. Albuquerque, New Mexico: SANDIA National Laboratories; 2005.
Graves GH. Analytical foundations of physical security system assessment. PhD Thesis defended at Texas A&M University, College Station, TX (USA); August 2006.
Gregory JJ, Breeding RJ, Helton JC, Murfin WB, Higgins SJ, Shiver AW. The NUREG-1150 Probabilistic Risk Assessment for the Sequoyah Nuclear Plant. Nuclear Engineering and Design 1992; 135(1): 95-115.
Guimerà R, Arenas A, Dìaz-Guilera A, Giralt F., 2002. Dynamical Properties of Model Communication Networks. Phys. Rev. E; 66: 026704.
Guyonnet D, Bourgine B, Dubois D, Fargier H, Côme B, Chilès JP. Hybrid approach for addressing uncertainty in risk assessments. Journal of the Environmental Engineering Division ASCE 2003; 129: 68–78.
Hacking I. The Emergence of Probability: A Philosophical Study of Early Ideas About Probability, Induction and Statistical Inference. London; New York: Cambridge University Press; 1975.
Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis 2006; 26(2): 293-296.
Haimes YY. Modeling complex systems of systems with Phantom System Models. Systems Engineering 2012; 15(3): 333-346.
Hansson SO, Helgesson G. What is stability? Synthese 2003; 136(2): 219-235.
Helbing D. Globally networked risks and how to respond. Nature 2013; 497(7447): 51-59.
Helton JC. Probability, Conditional Probability and Complementary Cumulative Distribution Functions in Performance Assessment for Radioactive Waste Disposal. Reliability Engineering and System Safety 1996; 54(2-3): 145-163.
Helton JC. Quantification of Margins and Uncertainties: Conceptual and Computational Basis. Reliability Engineering and System Safety 2011; 96(9): 976-1013.
Helton JC. Treatment of Uncertainty in Performance Assessments for Complex Systems. Risk Analysis 1994; 14(4): 483-511.
Helton JC. Uncertainty and Sensitivity Analysis in the Presence of Stochastic and Subjective Uncertainty. Journal of Statistical Computation and Simulation 1997; 57(1-4): 3-76.
Helton JC, Anderson DR, Jow H-N, Marietta MG, Basabilvazo G. Conceptual Structure of the 1996 Performance Assessment for the Waste Isolation Pilot Plant. Reliability Engineering and System Safety 2000a; 69(1-3): 151-165.
Helton JC, Anderson DR, Jow H-N, Marietta MG, Basabilvazo G. Performance Assessment in Support of the 1996 Compliance Certification Application for the Waste Isolation Pilot Plant. Risk Analysis 1999; 19(5): 959 - 986.

Helton JC, Breeding RJ. Calculation of Reactor Accident Safety Goals. Reliability Engineering and System Safety 1993; 39(2): 129-158.
Helton JC, Burmaster DE. Guest Editorial: Treatment of Aleatory and Epistemic Uncertainty in Performance Assessments for Complex Systems. Reliability Engineering and System Safety 1996; 54(2-3): 91-94.
Helton JC, Davis FJ, Johnson JD. Characterization of Stochastic Uncertainty in the 1996 Performance Assessment for the Waste Isolation Pilot Plant. Reliability Engineering and System Safety 2000b; 69(1-3): 167-189.
Helton JC, Davis FJ. Latin Hypercube Sampling and the Propagation of Uncertainty in Analyses of Complex Systems. Reliability Engineering and System Safety 2003; 81(1): 23-69.
Helton JC, Gross MB, Hansen CW, Sallaberry CJ, Sevougian SD. Expected Dose for the Seismic Scenario Classes in the 2008 Performance Assessment for the Proposed High-Level Radioactive Waste Repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 2014a; 122: 380-398.
Helton JC, Hansen CW, Sallaberry CJ. Conceptual Structure and Computational Organization of the 2008 Performance Assessment for the Proposed High-Level Radioactive Waste Repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 2014b; 122: 223-248.
Helton JC, Hansen CW, Sallaberry CJ. Expected Dose for the Early Failure Scenario Classes in the 2008 Performance Assessment for the Proposed High-Level Radioactive Waste Repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 2014c; 122: 297-309.
Helton JC, Hansen CW, Swift PN, eds. Special Issue: Performance Assessment for the Proposed High-Level Radioactive Waste Repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 2014d; 122: 1-456.
Helton JC, Johnson JD. Quantification of Margins and Uncertainties: Alternative Representations of Epistemic Uncertainty. Reliability Engineering and System Safety 2011; 96(9): 1034-1052.
Helton JC, Johnson JD, Oberkampf WL, Sallaberry CJ. Representation of Analysis Results Involving Aleatory and Epistemic Uncertainty. International Journal of General Systems 2010; 39(6): 605-646.
Helton JC, Johnson JD, Oberkampf WL, Storlie CB. A Sampling-Based Computational Strategy for the Representation of Epistemic Uncertainty in Model Predictions with Evidence Theory. Computational Methods in Applied Mechanics and Engineering 2007a; 196(37-40): 3980-3998.
Helton JC, Johnson JD, Oberkampf WL. An Exploration of Alternative Approaches to the Representation of Uncertainty in Model Predictions. Reliability Engineering and System Safety 2004; 85(1-3): 39-71.
Helton JC, Johnson JD, Oberkampf WL, Storlie CB. A sampling-based computational strategy for the representation of epistemic uncertainty in model predictions with evidence theory. Computer Methods in Applied Mechanics and Engineering 2007b; 196: 3980–98.
Helton JC, Johnson JD, Sallaberry CJ. Quantification of Margins and Uncertainties: Example Analyses from Reactor Safety and Radioactive Waste Disposal Involving the Separation of Aleatory and Epistemic Uncertainty. Reliability Engineering and System Safety 2011; 96(9): 1014-1033.
Helton JC, Johnson JD, Sallaberry CJ, Storlie CB. Survey of sampling-based methods for uncertainty and sensitivity analysis. Reliability Engineering & System Safety 2006; 91: 1175-1209.
Helton JC, Marietta MG, eds. Special Issue: The 1996 Performance Assessment for the Waste Isolation Pilot Plant. Reliability Engineering and System Safety 2000; 69(1-3): 1-451.
Helton JC, Martell M-A, Tierney MS. Characterization of Subjective Uncertainty in the 1996 Performance Assessment for the Waste Isolation Pilot Plant. Reliability Engineering and System Safety 2000c; 69(1-3): 191-204.
Helton JC, Oberkampf WL. Alternative representations of epistemic uncertainties. Reliability Engineering and System Safety 2004; 85(1-3): 1-10.
Helton JC, Oberkampf WL, Johnson JD. Competing Failure Risk Analysis Using Evidence Theory. Risk Analysis 2005; 25(4): 973-995.
Helton JC, Pilch M, eds. Special Issue: Quantification of Margins and Uncertainty. Reliability Engineering and System Safety 2011; 96(9): 959-1256.
Helton JC, Pilch M, Sallaberry CJ. Probability of Loss of Assured Safety in Systems with Multiple Time-Dependent Failure Modes: Representations with Aleatory and Epistemic Uncertainty. Reliability Engineering and System Safety 2014e; 124: 171-200.
Helton JC, Sallaberry C. Computational implementation of sampling-based approaches to the calculation of expected dose in performance assessments for the proposed high-level radioactive waste repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 2009; 94: 699-721.
Helton JC, Sallaberry CJ. Uncertainty and Sensitivity Analysis: From Regulatory Requirements to Conceptual Structure and Computational Implementation. IFIP Advances in Information and Communication Technology 2012; 377 AICT: 60-76.
Helton JC, Sallaberry CJ. Yucca Mountain 2008 Performance Assessment: Incorporation of Seismic Hazard Curve Uncertainty. In. Proceedings of the 13th International High-Level Radioactive Waste Management Conference (IHLRWMC), Albuquerque, NM April 10-14, 2011. La Grange Park, IL: American Nuclear Society, 2011: 1041-1048.
Henry D, Ramirez-Marquez EJ. Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering & System Safety 2012; 99: 114-122.

Hines P, Apt J, Talukdar S. Large blackouts in North America: Historical trends and policy implications. Energy Policy 2009; 37(12): 5249-5259.
Hines P, Blumsack S. A centrality measure for electrical networks. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences; 7–10 January 2008; Waikoloa, Big Island, Hawaii. Los Alamitos, CA: IEEE Computer Society; 2008. p. 185-185.
Hofer E, Kloos M, Krzykacz-Hausmann B, Peschke J, Woltereck M. An approximate epistemic uncertainty analysis approach in the presence of epistemic and aleatory uncertainties. Reliability Engineering and System safety 2002; 77: 229-238.
Hoffman FO, Hammonds JS. Propagation of Uncertainty in Risk Assessments: The Need to Distinguish Between Uncertainty Due to Lack of Knowledge and Uncertainty Due to Variability. Risk Analysis 1994; 14(5): 707-712.
Hollnagel E, Woods D, Levenson N. Resilience engineering: concepts and precepts. Abingdon, Oxon, UK: Ashgate Publishing Limited; 2006.
Holme P, Kim BJ, Yoon CN, Han SK. Attack vulnerability of complex networks. Physical Review E 2002; 65(5): 056109.
Holmgren ÅJ. Using graph models to analyze the vulnerability of electric power networks. Risk analysis 2006; 26(4): 955-969.
Hong L, Ouyang M, Peeta S, He XZ, Yan Y. Vulnerability assessment and mitigation for the Chinese railway system under floods. Reliability Engineering and System Safety 2015; 137: 58-68.
Hou Y, Yang B. Probability-Possibility Transformation for Small Sample Size Data. In: Proceedings of the 2010 Seventh International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2010); 10-12 Aug. 2010; Yantai, Shandong, China; Institute of Electrical and Electronics Engineers (IEEE), Inc.; 2010. p. 1720-1724.
Hromada M, Lukas L. Critical Infrastructure Protection and the Evaluation Process. International Journal of Disaster Recovery and Business Continuity 2012; 3: 37-46.
Hu Y. A guided simulation methodology for dynamic probabilistic risk assessment of complex systems. PhD Thesis; University of Maryland, College Park, MD; 2005.
Hu Y. et al. An entropy-based exploration strategy in dynamic PSA. In: Proceedings of 7th Probabilistic Safety Assessment and Management (PSAM 7) Conference; June 14–18, 2004; Berlin, Germany. London, UK: Springer-Verlag; 2004. p. 2391-2397.
Hu YS, Modarres M. Logic-based hierarchies for modeling behavior of complex dynamic systems with applications. In: Ruan D, ed. Fuzzy systems and soft computing in nuclear engineering. Berlin Heidelberg: Springer-Verlag; 2000.
Huang B, Du X. A robust design method using variable transformation and Gauss-Hermite integration. International Journal for Numerical Methods in Engineering 2006; 66: 1841-1858.
Huang D, Chen T, Wang MT. A fuzzy set approach for event tree analysis. Fuzzy Sets and Systems 2001; 118: 153–165.
Hurtado JE. Structural reliability - Statistical learning perspectives. Volume 17 of lecture notes in applied and computational mechanics. Berlin Heidelberg: Springer-Verlag; 2004.
Hurtado JE. Filtered importance sampling with support vector margin: a powerful method for structural reliability analysis. Structural Safety 2007; 29: 2-15.
IEEE (IEEE power and energy society). Distribution test feeders. http://ewh.ieee.org/soc/pes/dsacom/testfeeders/index.html; 2000.
IEEE. Power system test case archive, available at: http://www.ee.washington.edu/research/pstca/. September, 2014.
Iman RL, Conover WJ. A Distribution-Free Approach to Inducing Rank Correlation Among Input Variables. Communications in Statistics: Simulation and Computation 1982; B11(3): 311-334.
Iman RL, Davenport JM. Rank Correlation Plots for Use with Correlated Input Variables. Communications in Statistics: Simulation and Computation 1982; B11(3): 335-360.
Iyer SM, Nakayama MK, Gerbessiotis AV. A Markovian dependability model with cascading failures. IEEE Transactions on Computers 2009; 58(9): 1238-1249.
Jalal-Kamali A, Kreinovich V. Estimating correlation under interval uncertainty. Mechanical Systems and Signal Processing 2013; 37(1-2): 43-53.
Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety 2010; 95(12): 1335-1344.
Kafrawy KF, Rushdi AM. Uncertainty analysis of fault tree with statistically correlated failure data. Microelectronics and Reliability 1990; 30: 157–175.
Kalos MH, Whitlock PA. Monte Carlo methods. Volume I: Basics. New York, NY: Wiley; 1986.
Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk analysis 1981; 1(1): 11-27.
Karanki DR, Dang VN. Quantification of uncertainty in fault tree analysis with correlated basic events. In: Ale B, Papazoglu IA, Zio E, Eds. Reliability, Risk and Safety. Proceedings of the European Safety and Reliability (ESREL) 2010 Conference; 5-9 September 2010; Rhodes, Greece. London, UK: Taylor & Francis Group; 2010. p. 1619-1628.
Karanki DR, Jadhav PA, Chandrakar A, Srividya A, Verma AK. Uncertainty analysis in PSA with correlated input parameters. Int J Syst Assur Eng Manag 2010; 1: 66–71.

Karanki DR, Kushwaha HS, Verma AK, Ajit S. Uncertainty Analysis Based on Probability Bounds (P-Box) Approach in Probabilistic Safety Assessment. Risk Analysis 2009; 29(5): 662-675.
Keeney RL, Raiffa H. Decisions with Multiple Objectives: Preferences and Value Tradeoffs. New York, NY (USA): Wiley; 1976.
Keeney RL. Value-focused thinking: A path to creative decision making. Cambridge, MA: Harvard University Press; 1992.
Kelly DL, Smith CL. Bayesian Inference for Probabilistic Risk Assessment: A Practitioner's Guidebook. London (UK): Springer-Verlag; 2011.
Kelly DL, Smith CL. Bayesian inference in probabilistic risk assessment — The current state of the art. Reliability Engineering and System Safety 2009; 94: 628–643.
Kempe D, Kleinberg J, Tardos É. (). Maximizing the spread of influence through a social network. In: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining; August 24 - 27, 2003; Washington, DC, USA. New York, NY, USA: ACM; 2003. p. 137-146.
Kennedy M, O'Hagan A. Bayesian calibration of computer models. Journal of the Royal Statistical Society, Series B 2001; 63: 425-464.
Kentel E, Aral MM. 2D Monte Carlo versus 2D Fuzzy Monte Carlo Health Risk Assessment. Internat. J. Stochastic Environ. Res. Risk Assess. 2005; 19: 86–96.
Kentel E, Aral MM. Probabilistic-fuzzy health risk modeling. Stoch. Envir. Res. and Risk Ass. 2004; 18: pp. 324–338.
Kentel E, Aral MM. Risk tolerance measure for decision-making in fuzzy analysis: a health risk assessment perspective. Stoch. Environ Res. Ris. Assess. 2007; 21: 405–417.
Kersaudy P, Sudret B, Varsier N, Picon O, Wiart J. A new surrogate modeling technique combining Kriging and polynomial chaos expansions – Application to uncertainty analysis in computational dosimetry. Journal of Computational Physics 2015; 286: 103–117.
Kinney R, Crucitti P, Albert R, Latora V. Modeling cascading failures in the North American power grid. The European Physical Journal B-Condensed Matter and Complex Systems 2005; 46(1): 101-107.
Klein R. The EU FP6 Integrated Project IRRIIS on Dependent Critical Infrastructures - Summary and Conclusions. In: Xenakis C, Wolthusen SD, eds. 5th International Workshop, CRITIS; September 2010; Athens, Greece. Berlin Heidelberg: Springer-Verlag; 2011. p. 26-42.
Klir GJ, Yuan B. Fuzzy Sets and Fuzzy Logic: Theory and Applications. Upper Saddle River, NJ: Prentice-Hall; 1995.
Koonce AM, Apostolakis GE, Cook BK. Bulk power risk analysis: Ranking infrastructure elements according to their risk significance. International Journal of Electrical Power & Energy Systems 2008; 30(3): 169-183.
Koutsourelakis PS, Pradlwarter HJ, Schueller GI. Reliability of structures in high dimensions, Part I: algorithms and application. Probabilistic Engineering Mechanics 2004; 19: 409-417.
Kozine I, Filimonov Y. Imprecise reliabilities: experiences and advances. Reliab. Eng. Syst. Saf. 2000; 67: 75–83.
Kozine IO, Utkin LV. Processing unreliable judgements with an imprecise hierarchical model. Risk, Decision and Policy 2002; 7(03): 325-339.
Kröger W. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. Reliability Engineering & System Safety 2008; 93(12): 1781-1787.
Kröger W, Zio E. Vulnerable Systems. London, UK: Springer; 2011.
Krzykacz-Hausmann B. An approximate sensitivity analysis of results from complex computer models in the presence of epistemic and aleatory uncertainties. Reliability Engineering and System safety 2006; 91: 1210-1218.
Kuznetsov VP. Interval statistical models (in Russian). Radio i Svyaz 1991, Moscow.
Labeau PE. Probabilistic dynamics: estimation of generalized unreliability through efficient Monte Carlo simulation. Annals of Nuclear Energy 1996; 23(17): 1355-1369.
Labeau PE, Smidts C, Swaminathan S. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. Reliability Engineering & System Safety 2000; 68(3): 219-254.
Lamboni M, Monod H, Makowski D. Multivariate sensitivity analysis to measure global contribution of input factors in dynamic models. Reliability Engineering and System Safety 2011; 96: 450–459.
Lapointe S, Bobeè B. Revision of possibility distributions: A Bayesian inference pattern. Fuzzy Sets and Systems 2000; 116: 119-140.
Latora V, Marchiori M. Vulnerability and protection of infrastructure networks. Physical Review E 2005; 71(1): 015103.
Le Duy TD, Dieulle L, Vasseur D, Berenguer C, Couplet M. An alternative comprehensive framework using belief functions for parameter and model uncertainty analysis in nuclear probabilistic risk assessment applications. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 2013; 227(5): 471-490.
Le Duy TD, Vasseur D, Couplet M, Dieulle L, Bérenguer C. A study on updating belief functions for pa-rameter uncertainty representation in Nuclear Probabilistic Risk Assessment. In: Coolin F, De Cooman G, Fetz T, Oberguggenberger M, Eds. Proceedings of the 7th International Symposium on Imprecise Probability: Theories and Applications; 25-28 July 2011; Innsbruck, Austria; Innsbruck, Austria: SIPTA; 2011. p. 247-256.

Lee EE, Mitchell JE, Wallace WA. Restoration of services in interdependent infrastructure systems: A network flows approach. IEEE Transactions on Systems Man and Cybernetics Part C-Applications and Reviews 2007; 37(6): 1303-1317.

Leroy A, Mousseau V, Pirlot M. Learning the parameters of a multiple criteria sorting method based on a majority rule. In: Brafman R, ed. Proceedings of The Second International Conference on Algorithmic Decision Theory; October 26 - 28, 2011; Piscataway, NJ, USA. Berlin Heidelberg: Springer-Verlag; 2011. p. 219–233.

Lewis TG. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Hoboken, New Jersey (USA): John Wiley & Sons; 2006.

Li H. Hierarchical Risk Assessment of Water Supply Systems. Ph.D. thesis. Loughborough University, Leicestershire, UK; 2007.

Li J, Mosleh A, Kang R. Likelihood ratio gradient estimation for dynamic reliability applications. Reliability Engineering & System Safety 2011; 96(12): 1667-1679.

Li J, Mosleh A, Kang R. From Blind to Guided Simulation: Biased Monte Carlo Based on Entropy and Zero Variance for Dynamic PSA Applications. In: Proceedings of the 10th International Conference on Probabilistic Safety Assessment and Management (PSAM-10) 2010; 7-11 June 2010; Seattle, Washington, USA. Red Hook, NY: Curran Associates, Inc. p. 616-628.

Li YF, Sansavini G, Zio E. Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. Reliability Engineering & System Safety 2013; 111: 195-205.

Li AG, Zhou X, Zhang JL. Performance analysis of quantitative attributes inverse classification problem. JOURNAL OF COMPUTERS 2012; 7(5): 1067-1072.

Liel, A. B., Haselton, C. B., Deierlein, G. G., Baker, J. W., 2009. Incorporating modeling uncertainties in the assessment of seismic collapse risk of buildings. Structural Safety, 31(2), pp. 197-211.

Limbourg P, de Rocquigny E. Uncertainty analysis using evidence theory – confronting level-1 and level-2 approaches with data availability and computational constraints. Reliability Engineering and System Safety 2010; 95(5): 550-564.

Lin YH, Li YF, Zio E. Dynamic Reliability Models for Multiple Dependent Competing Degradation. In: Safety and Reliability: Methodology and Applications, Proceedings of the European Safety and Reliability Conference (ESREL) 2014; Wroclaw, Poland; September 2014. London, UK: Taylor and Francis Group; 2015. p. 775–782.

Lind M. An introduction to multilevel flow modeling. Nuclear safety and simulation 2011; 2(1): 22-32.

Lind M. Reasoning about causes and consequences in Multilevel Flow Models. In: Guedes Soares C, ed. Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, ESREL 2011. 18-22/09/2011; Troyes, France. London, UK: Taylor and Francis Group; 2012. p. 2359-2367.

Lindley DV. The philosophy of statistics. The Statistician 2000; 49(3): 293-337.

Lindley DV. Understanding uncertainty. Hoboken, NJ: Wiley; 2006.

Lo CK, Pedroni N, Zio E. Bayesian probabilistic analysis of a nuclear power plant small loss of coolant event tree model with possibilistic parameters. In: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia and A. C.W.M. Ton. Vrouwenvelder (Eds.). Safety, Reliability and Risk Analysis, Beyond the Horizon, Proceedings of the European Safety and RELiability Conference (ESREL) 2013; 29 September-2 October 2013; Amsterdam, The Netherlands. London, UK: Taylor and Francis Group; 2014a. p. 3321-3328.

Lo CK, Pedroni N, Zio E. Treating uncertainties in a nuclear seismic probabilistic risk assessment by means of the Dempster-Shafer theory of evidence. Nuclear Engineering and Technology 2014b; 46(1): 11-26.

Mackay FJ, Apostolakis GE, Hejzlar P. Incorporating reliability analysis into the design of passive cooling systems with an application to a gas-cooled reactor. Nuclear Engineering and Design 2008; 238(1): 217-228.

Marrel A, Iooss B, Laurent B, Roustant O. Calculations of Sobol indices for the Gaussian process metamodel. Reliability Engineering and System Safety 2009; 94: 742-751.

Marrel A, Marie N, De Lozzo M. Advanced surrogate model and sensitivity analysis methods for sodium fast reactor accident assessment, Reliability Engineering & System Safety 2015; 138: 232–241.

Marrel A, Perot N, Mottet C. Development of a surrogate model and sensitivity analysis for spatio-temporal numerical simulators. Stoch Environ Res Risk Assess 2015; 29: 959–974.

Marseguerra M, Zio E. Monte Carlo approach to PSA for dynamic process systems. Reliability Engineering & System Safety 1996; 52(3): 227-241.

Masson MH, Denoeux T. Inferring a possibility distribution from empirical data. Fuzzy Sets and Systems 2006; 157: 319–340.

Mathews TS, Arul AJ, Parthasarathy U, Kumar CS, Ramakrishnan M, Subbaiah KV. Integration of functional reliability analysis with hardware reliability: An application to safety grade decay heat removal system of Indian 500 MWe PFBR. Annals of Nuclear Energy 2009; 36: 481-492.

Mauris G. Inferring a Possibility Distribution from Very Few Measurements. In: Dubois D et al., Eds. Soft Methods for Handling Variability and Imprecision, ASC 48. Berlin, Heidelberg: Springer-Verlag; 2008. p. 92–99.

McCalley JD, Asgarpoor S, Bertling L, Billinion R, Chao H, Chen J, Endrenyi J, Fletcher R, Ford A, Grigg C. Probabilistic security assessment for power system operations. In: IEEE Power Engineering Society General

Meeting; 6-10 June 2004; Denver, Colorado (USA). Piscataway, NJ: IEEE Power Engineering Society; 2004. p. 212-220.
McCalley JD, Xiao F, Jiang Y, Chen Q. Computation of contingency probabilities for electric transmission decision problems. In: Proceedings of the 13th International Conference on Intelligent Systems Application to Power Systems; 6-10 Nov. 2005; Arlington, VA (USA). IEEE; 2005. p. 540-545.
McDaniels T, Chang S, Peterson K, Mikawoz J, Reed D. Empirical framework for characterizing infrastructure failure interdependencies. Journal of Infrastructure Systems 2007; 13(3): 175-184.
Mehl CH. P-boxes for cost uncertainty analysis. Mechanical Systems and Signal Processing 2013; 37(1-2): 253-263.
Metropolis N, Rosenbluth AW, Rosenbluth MN, Taller AH. Equations of state calculations by fast computing machines. Journal of Chemical Physics 1953; 21(6): 1087-1092.
Meyer MA, Booker JM. Eliciting and Analyzing Expert Judgment: A Practical Guide. Philadelphia, PA: SIAM; 2001.
Molchanov I. Theory of Random Sets. New York (NY): Springer; 2005.
Moller B. Fuzzy randomness – a contribution to imprecise probability. ZAMM - Z. Angew. Math. Mech. 2004; 84(10–11): 754 – 764.
Möller B, Beer M. Engineering computation under uncertainty – Capabilities of non-traditional models. Computers and Structures 2008; 86: 1024–1041.
Möller B, Beer M. Fuzzy Randomness: Uncertainty in Civil Engineering and Computational Mechanics. Berlin, Germany: Springer; 2004.
Moller B, Beer M, Graf W, Sickert JU. Time-dependent reliability of textile-strengthened RC structures under consideration of fuzzy randomness. Computers and Structures 2006; 84: 585–603.
Moller B, Graf W, Beer M. Safety assessment of structures in view of fuzzy randomness. Computers and Structures 2003; 81: 1567–1582.
Moore RE. Methods and Applications of Interval Analysis. Philadelphia, PA: SIAM; 1979.
Moore DA. Application of the API/NPRA SVA methodology to transportation security issues. Journal of Hazardous Materials 2006; 130(1-2): 107-121.
Moral S, Wilson N. Importance sampling Monte-Carlo algorithms for the calculation of Dempster-Shafer belief. In: Proc. 6th Int. Conf. Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU) 1996; 1-5 July 1996; Granada, Spain; 1996. p. 1337-1344.
Morgan M, Florig HK, Dekay ML, Fischbeck P. Categorizing risks for risk ranking. Risk Analysis 2000; 20: 49–58.
Morio J. Extreme quantile estimation with nonparametric adaptive importance sampling. Simul Model Pract Theory 2012; 27: 76–89.
Morris MD. Three technometrics experimental design classics. Technometrics 2000; 42(1): 26-27.
Moteff JD. Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service; 2012.
Motter AE. Cascade control and defense in complex networks. Physical Review Letters 2004; 93(9): 098701.
Motter AE, Lai YC. Cascade-based attacks on complex networks. Physical Review E 2002; 66(6): 065102.
Mousseau V, Slowinski R. Inferring an electre tri model from assignment examples. Journal of Global Optimization 1998; 12: 157–174.
Munoz Zuniga M, et al. Adaptive directional stratification for controlled estimation of the probability of a rare event. Reliability Engineering & System Safety 2011; 96(12): 1691-1712.
Murray L, Cancela H, Rubino G. A splitting algorithm for network reliability estimation." IIE Transactions 2013; 45(2): 177-189.
Muscolino G, Sofi A. Bounds for the stationary stochastic response of truss structures with uncertain-but-bounded parameters. Mechanical Systems and Signal Processing 2013; 37(1-2): 163-181.
NAS/NRC (National Academy of Science/National Research Council). Evaluation of Quantification of Margins and Uncertainties for Assessing and Certifying the Reliability of the Nuclear Stockpile. Washington, DC: National Academy Press; 2008.
NASA (National Aeronautics and Space Administration). Risk-Informed Decision Making Handbook. NASA/SP-2010-576 – Version 1.0. Washington, DC (USA): Office of Safety and Mission Assurance, NASA Headquarters; April 2010.
NECSI. Visualizing Complex Systems Science (CSS). New England Complex Systems Institute, www.necsi.org/projects/mclemens/viscss.html, Accessed: 30-Nov-2010; 2005.
Nedic DP, Dobson I, Kirschen DS, Carreras BA, Lynch VE. Criticality in a cascading failure blackout model. International Journal of Electrical Power & Energy Systems 2006; 28(9): 627-633.
Netkachov O, Popov P, Salako K. Quantification of the Impact of Cyber Attack in Critical Infrastructures. In: Bondavalli A, Ceccarelli A, Ortmeier F, eds. Computer Safety, Reliability, and Security. Springer International Publishing; 2014. p. 316-327.
Newman ME, Forrest S, Balthrop J. Email networks and the spread of computer viruses. Physical Review E 2002; 66(3): 035101.
Ng LW, Heldred MS. Multifidelity Uncertainty Quantification Using Non-Intrusive Polynomial Chaos and Stochastic Collocation. 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference;

23-26 April 2012; Honolulu, Hawaii. Reston, VA: American Institute of Aeronautics and Astronautics (AIAA); 2012.
North W. Probability Theory and Consistent Reasoning: Commentary. Risk Analysis 2010; 30(3): 377-380.
Nozick LK, Turnquist MA, Jones DA, Davis JR, Lawton CR. Assessing the performance of interdependent infrastructures and optimizing investments. International Journal of Critical Infrastructures 2005; 1(2-3): 144-154.
Obama B. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. Washington, DC (USA); 2013.
Oberkampf WL, Helton JC. Investigation of evidence theory for engineering applications. In: Proceedings of Non-Deterministic Approaches Forum, 43rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 2002; April 2002; Denver, Colorado; Reston, VA: American Institute of Aeronautics and Astronautics (AIAA); 2002. Paper 2002-1569.
Oberkampf WL, Helton JC, Sentz K. 2001. Mathematical Representation of Uncertainty. In: Proceedings of the AIAA Non-Deterministic Approaches Forum 2001; April 2001; Seattle, Washington; Reston, VA: American Institute of Aeronautics and Astronautics (AIAA); 2001. Paper 2001-1645.
Oberkampf WL, Trucano TG. Verification and validation benchmarks. Nuclear Engineering and Design 2008; 238(3): 716-743.
Ouyang M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos 2013; 23: 023114.
Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety 2014; 121: 43-60.
Ouyang M, Hong L, Mao ZJ, Yu MH, Qi F. A methodological approach to analyze vulnerability of interdependent infrastructures. Simulation Modelling Practice and Theory 2009; 17(5): 817-828.
Ouyang M, Zhao L, Hong L, Pan Z. Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliability Engineering and System Safety 2014; 123: 38-46.
Pannier S, Waurick M, Graf W, Kaliske M. Solutions to problems with imprecise data - An engineering perspective to generalized uncertainty models. Mechanical Systems and Signal Processing 2013; 37(1-2): 105-120.
Parry GW. The Characterization of Uncertainty in Probabilistic Risk Assessments of Complex Systems. Reliability Engineering and System Safety 1996; 54(2-3): 119-126.
Parry GW, Drouin MT. Risk-Informed Regulatory Decision-Making at the U.S. NRC: Dealing with model uncertainty. Washington, DC: US Nuclear Regulatory Commission, 2009.
Parry GW, Winter PW. Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis. Nuclear Safety 1981; 22(1): 28-42.
Pasanisi A, de Rocquigny E, Bousquet N, Parent E, 2009. Some useful features of the Bayesian setting while dealing with uncertainties in industrial practice. In: Guedes Soares C, Bris R, Martorell S, Eds. Reliability, Risk and Safety, Three volume set: Theory and Applications. Proceedings of the ESREL 2009 Conference; 7-10 September 2009; Prague, Czech Republic; London (UK): Taylor & Francis Group; 2010. p. 1795-1802.
Pasanisi A, Dutfoy A. An Industrial Viewpoint on Uncertainty Quantification in Simulation: Stakes, Methods, Tools, Examples (with discussion). In: Dienstfrey AM, Boisvert RF, Editors. Uncertainty Quantification in Scientific Computing. Berlin-Heidelberg (Germany): Springer; 2012. p. 27-45.
Pasanisi A, Keller M, Parent M. Estimation of a quantity of interest inuncertainty analysis: Some help from Bayesian decision theory. Reliability Engineering and System Safety 2012; 100: 93–101.
Patalano G, Apostolakis GE, Hejzlar P. Risk-informed design changes in a passive decay heat removal system. Nuclear Technology 2008; 163: 191-208.
Paté-Cornell ME. Uncertainties in Risk Analysis: Six Levels of Treatment. Reliability Engineering and System Safety 1996; 54(2-3): 95-111.
Patterson SA, Apostolakis GE. Identification of critical locations across multiple infrastructures for terrorist actions. Reliability Engineering & System Safety 2007; 92: 1183–1203.
Payne AC, Jr., Breeding RJ, Helton JC, Smith LN, Johnson JD, Jow H-N, Shiver AW. The NUREG-1150 Probabilistic Risk Assessment for the Peach Bottom Atomic Power Station. Nuclear Engineering and Design 1992; 135(1): 61-94.
Pebesma EJ, Heuvelink GBM. Latin hypercube sampling of Gaussian random fields. Technometrics 1999; 41(4): 203-212.
Pedroni N, Zio E. An Adaptive Metamodel-Based Subset Importance Sampling method for the efficient estimation of the small functional failure probability of a thermal-hydraulic passive system", submitted for publication on Applied Mathematical Modelling 2015a.
Pedroni N, Zio E. Empirical comparison of methods for the hierarchical propagation of hybrid uncertainty in risk assessment, in presence of dependences. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 2012; 20(4): 509-557.
Pedroni N, Zio E. Uncertainty analysis in fault tree models with dependent basic events. Risk Analysis, an International Journal 2013; 33(6): 1146-73.

Pedroni N, Zio E. Hybrid Uncertainty and Sensitivity Analysis of the Model of a Twin-Jet Aircraft. Journal of Aerospace Information Systems (Special Issue on NASA Langley Multidisciplinary Uncertainty Quantification Challenge) 2015b; 12: 73-96.

Pedroni N, Zio E, Apostolakis GE. Comparison of bootstrapped Artificial Neural Networks and quadratic Response Surfaces for the estimation of the functional failure probability of a thermal-hydraulic passive system. Reliability Engineering and System Safety 2010; 95(4): 386-395.

Pedroni N, Zio E, Ferrario E, Pasanisi A, Couplet M. Hierarchical propagation of probabilistic and non-probabilistic uncertainty in the parameters of a risk model. Computers and Structures 2013; 126: 199–213.

Pedroni N, Zio E, Ferrario E, Pasanisi A, Couplet M. Propagation of aleatory and epistemic uncertainties in the model for the design of a flood protection dike. Proceedings of the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012); 25-29 June 2012; Helsinki, Finland; Red Hook, NY USA: IAPSAM & ESRA - Printed by Curran Associates; 2012. p. 1193-1203.

Pedroni N, Zio E, Pasanisi A, Couplet M. Bayesian update of the parameters of probability distributions for risk assessment in a two-level hybrid probabilistic-possibilistic uncertainty framework. In: Steenbergen RDJM, van Gelder PHAJM, Miraglia S, Vrouwenvelder ACWM, Eds. Safety, Reliability and Risk Analysis, Beyond the Horizon. Proceedings of the European Safety and RELiability Conference (ESREL) 2013; 29 September-2 October 2013; Amsterdam, The Netherlands; London, UK: Taylor and Francis Group; 2014. p. 3295–3302.

Pedroni N, Zio E, Pasanisi A, Couplet M. Bayesian update of the parameters of probability distributions for risk assessment in a two-level hybrid probabilistic-possibilistic uncertainty framework, accepted for publication on the ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering 2015.

Peng Y, Lu T, Liu J, Gao Y, Guo X, Xie F. Cyber-physical system risk assessment. In: Proceedings of Ninth International Conference on Intelligent Information Hiding and Mulitmedia Signal Processing; 16-18 Oct. 2013; Beijing, China. IEEE Computer Society; 2013. p. 442-447.

Pepyne DL, Panayiotou CG, Cassandras CG, Ho YC. Vulnerability assessment and allocation of protection resources in power systems. In: Proceedings of the 2001 American Control Conference; 25 Jun 2001-27 Jun 2001; Arlington, VA (USA). IEEE; 2001. p. 4705-4710.

Perez M, et al. Uncertainty and sensitivity analysis of a LBLOCA in a PWR Nuclear Power Plant: Results of the Phase V of the BEMUSE programme. Nuclear Engineering and Design 2011; 241(10): 4206-4222.

Picheny V, Ginsbourger D, Roustant O, Haftka RT. Adaptive designs of experiments for accurate approximation of a target region. Journal of Mechanical Design 2010; 132(7): paper 071008, 9 pages.

Pidd H. India blackouts leave 700 million without power. The Guardian 2012; 31 July 2012.

Piwowar J, Chatelet E, Laclemence P. An efficient process to reduce infrastructure vulnerabilities facing malevolence. Reliability Engineering & System Safety 2009; 94(11): 1869-1877.

Poljanšek K, Bono F, Gutiérrez E. Seismic risk assessment of interdependent critical infrastructure systems: The case of European gas and electricity networks. Earthquake Engineering & Structural Dynamics 2012; 41(1): 61-79.

Pollet J, Cummins J. All-hazard approach for assessing readiness of critical infrastructure. Proceedings of the IEEE Conference on Technologies for Homeland Security; 11-12 May 2009; Boston, MA. IEEE 2009. p. 366–372.

Pradlwarter HJ, Pellissetti MF, Schenk CA, Schueller GI, Kreis A, Fransen S, Calvi A, Klein M. Realistic and efficient reliability estimation for aerospace structures. Computer Methods in Applied Mechanics and Engineering 2005; 194: 1597-1617.

Pradlwarter HJ, Schueller GI, Koutsourelakis PS, Charmpis DC. Application of line sampling simulation method to reliability benchmark problems. Structural Safety 2007; 29: 208-221.

Rao KD, Kushwaha HS, Verma AK, Srividya A. Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliability Engineering & System Safety 2007; 92(7): 947-956.

Rao KD, et al. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliability Engineering & System Safety 2009; 94(4): 872-883.

Reed DA, Kapur KC, Christie RD. Methodology for assessing the resilience of networked infrastructure. IEEE Systems Journal 2009; 3(2): 174-180.

Regan HM, Ferson S, Berleant D. Equivalence of five methods for bounding uncertainty. International Journal of Approximate Reasoning 2004; 36: 1-30.

Reid SG. Probabilistic confidence for decisions based on uncertain reliability estimates. Mechanical Systems and Signal Processing 2013; 37(1-2), 229-239.

Romero VJ, Swiler LP, Giunta AA. Construction of response surfaces based on progressive-lattice-sampling experimental designs with application to uncertainty propagation. Struct. Saf. 2004; 26(2): 201–219.

Roy B. Multicriteria Methodology for Decision Aiding. Dordrecht, The Netherlands: Kluwer Academic Publishers; 1996.

Roy B, Bouyssou D. Aide multicritère d'Aide à la Décision: Méthodes et Cas. Economica, Paris, 1993.

Roy CJ, Oberkampf WL. A comprehensive framework for verification, validation, and uncertainty quantification in scientific computing. Computer Methods in Applied Mechanics and Engineering 2011; 200(25–28): 2131-2144.

RTE. Le Réseau de Transport d'Electricité 400 kV. http://www.rte-france.com; 2013.

Rubinstein R. Y., and D. P. Kroese. "The cross-entropy method: a unified approach to combinatorial optimization, Monte-Carlo simulation and machine learning." Springer, 2004.
Rumelhart DE, Hinton GE, Williams RJ. Learning internal representations by error back-propagation. In: Rumelhart DE, McClelland JL (Eds.). Parallel distributed processing: exploration in the microstructure of cognition (vol. 1). Cambridge (MA): MIT Press; 1986.
Rushdi AM, Kafrawy KF. Uncertainty propagation in fault tree analyses using an exact method of moments. Microelectronics and Reliability 1988; 28: 945–965.
Sadiq R, Saint-Martin E, Kleiner Y. Predicting risk of water quality failures in distribution networks under uncertainties using fault-tree analysis. Urban Water 2008; 5(4): 287-304.
Sallaberry CJ, Hansen CW, Helton JC. Expected Dose for the Igneous Scenario Classes in the 2008 Performance Assessment for the Proposed High-Level Radioactive Waste Repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 2014; 122: 339-353.
Sallaberry CJ, Helton JC, Hora SC. Extension of Latin Hypercube samples with correlated variables. Reliability Engineering and System Safety 2008; 93(7): 1047-1059.
Sallak M, Schön W, Aguirre F. Reliability assessment for multi-state systems under uncertainties based on the Dempster–Shafer theory. IIE Transactions 2013; 45(9): 995-1007.
Sankararaman S, Mahadevan S. Distribution type uncertainty due to sparse and imprecise data. Mechanical Systems and Signal Processing 2013; 37(1-2): 182-198.
Sansavini G, Hajj MR, Puri IK, Zio E. A deterministic representation of cascade spreading in complex networks. EPL 2009; 87(4): art. no. 48004.
Schobi R, Sudret B, Wiart J, 2015. Polynomial-Chaos-based Kriging, International Journal of Uncertainty Quantification 2015; 5(2): 171-193.
Schroer S, Modarres M. An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment. Reliability Engineering and System Safety 2013; 117: 40–51
Schueller GI. Efficient Monte Carlo simulation procedures in structural uncertainty and reliability analysis - recent advances. Journal of Structural Engineering and Mechanics 2009; 32(1): 1–20.
Schueller GI, Pradlwarter HJ. Benchmark study on reliability estimation in higher dimensions of structural systems – An overview. Structural Safety 2007; 29(3): 167-182.
Schueller GI, Pradlwarter HJ, Koutsourelakis PS. A critical appraisal of reliability estimation procedures for high dimensions. Probabilistic Engineering Mechanics 2004; 19: 463-474.
Sentz K, Ferson S. Combination of Evidence in Dempster-Shafer Theory. Technical Report SAND 2002-0835. Albuquerque, New Mexico: SANDIA National Laboratories; 2002.
Serrurier M, Prade H. Maximum-Likelihood Principle For Possibility Distributions Viewed As Families Of Probabilities. In: Proceedings of the 2011 IEEE International Conference on Fuzzy Systems; June 27-30, 2011; Taipei, Taiwan; Institute of Electrical and Electronics Engineers (IEEE), Inc.; 2011. p. 2987-2993.
Seth A. Measuring emergence via nonlinear Granger causality. Artificial Life XI: Proceedings of the Eleventh International Conference on the Simulation and Synthesis of Living Systems; 5-8 August, 2008; Southampton, UK; MIT Press, Cambridge, MA; 2008. p.545-552.
Shafer G. A Mathematical Theory of Evidence. Princeton, NJ: Princeton Univ. Press; 1976.
Shafer G. Belief Functions and Possibility Measures. In: J Bezdek, ed. Analysis of Fuzzy Information. Vol. 1. Boca Raton, FL: CRC Press, 1987: 51-84.
Shafer G. Perspectives on the theory and practice of belief functions. International Journal of Approximate Reasoning 1990; 4: 323–62.
Shao S, Huang X, Stanley HE, Havlin S. Percolation of localized attack on complex networks. New Journal of Physics 2015; 17: paper 023049.
Singpurwalla N. Reliability and Risk. A Bayesian Perspective. New York (NY): Wiley; 2006.
Siu N, Kelly D. Bayesian parameter estimation in probabilistic risk assessment. Reliability Engineering and System Safety 1998; 62: 89–116.
Slay J, Miller M. Lessons learned from the Maroochy water breach. Critical Infrastructure Protection 2007; 253: 73–82.
Smets P. Belief Functions: The Disjunctive Rule of Combination and the Generalized Bayesian Theorem. International Journal of Approximate Reasoning 1993; 9: 1-35.
SRA (Society of Risk Analysis). Glossary of the specialty group on Foundations of Risk Analysis. http://www.sra.org/news/sra-develops-glossary-risk-related-terms; 2015.
Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. Proceedings of the IEEE 2012; 99(1): 1–15.
Stein M, Beer M. Bayesian quantification of inconsistent information. In: Faber M, Köhler J, Nishijima K, Eds. Applications of Statistics and Probability in Civil Engineering. Proceedings of the 11th International Conference on Applications of Statistics and Probability in Civil Engineering; August 1-4, 2011; Zurich, Switzerland; London, UK: Taylor & Francis Group; ISBN 978-0-415-66986-3; 2011. p. 463–470.
Stein M, Beer M, Kreinovich V. Bayesian Approach for Inconsistent Information. Information Sciences 2013; 245: 96–111.

Storlie CB, Helton JC. Multiple predictor smooting methods for sensitivity analysis: Description of techniques. Reliability Engineering and System Safety 2008; 93: 28-54.
Storlie CB, Swiler LP, Helton JC, Sallaberry CJ 2009. Implementation and evaluation of nonparametric regression procedures for sensitivity analysis of computationally demanding models. Reliability Engineering and System Safety 2009; 94: 1735-1763.
Strogatz SH. Exploring complex networks. Nature 2001; 410(6825): 268-276.
Stutzke MA. Scoping Estimates of Multiunit Accident Risk. Proceedings of the 2014 International Conference on Probabilistic Safety Assessment and Management (PSAM 12); 22-27 June 2014; Honolulu, Hawaii (USA); Paper 96.
Sudret B. Global sensitivity analysis using polynomial chaos expansions. Reliability Engineering and System Safety 2008; 93: 964–979.
Sudret B, Mai CV. Computing derivative-based global sensitivity measures using polynomial chaos expansions. Reliability Engineering and System Safety 2015; 134: 241–250.
Sun K, Han ZX. Analysis and comparison on several kinds of models of cascading failure in power system. In: Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES. Dalian, China. IEEE; 2005. p. 1–7.
Tonon F, Bernardini A, Mammino A. Determination of parameters range in rock engineering by means of Random Set Theory. Reliability Engineering and System Safety 2000a; 70: 241-261.
Tonon F, Bernardini A, Mammino A. Reliability analysis of rock mass response by means of Random Set Theory. Reliability Engineering and System Safety 2000b; 70: 263-282.
Tonon F. Using random set theory to propagate epistemic uncertainty through a mechanical system. Reliability Engineering and System Safety 2004; 85: 169–181.
Trucco P, Cagno E, De Ambroggi M. Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. Reliability Engineering & System Safety 2012; 105: 51-63.
Turati P, Pedroni N, Zio E. Advanced RESTART method for the estimation of the probability of failure of highly reliable hybrid dynamic systems. Under second review on Reliability Engineering and System Safety 2015a.
Turati P, Pedroni N, Zio E. An adaptive simulation framework for the efficient, semi-automatic exploration of extreme and unexpected events in the risk assessment of dynamic engineered systems. Submitted for publication on Risk Analysis, an International Journal 2015b.
Turati P, Pedroni N, Zio E. An entropy-driven method for exploring extreme and unexpected accident scenarios in the risk assessment of dynamic engineered systems. Accepted for publication on the Proceedings of the European Safety and RELiability Conference (ESREL) 2015; 7-10 September 2015; Zurich, Switzerland; 2015c.
UCTE. Final Report System Disturbance on 4 Nov. 2006: The lessons to be learned from the large disturbance in the European power system on the 4th of November 2006. Tech. Rep. E06-BAG-01-06. Brussels, Belgium: Union for the Coordination of Transmission of Electricity.
US-CA. Final Report on the August 14th blackout in the United States and Canada. Tech. Rep., United States Department of Energy and National Resources Canada; 2004.
US EPA (Environmental Protection Agency). Guidance on the Development, Evaluation, and Application of Environmental Models. EPA/100/K-09/003. Washington, DC: U.S. Environmental Protection Agency, Council for Regulatory Environmental Modeling; 2009.
US NRC (U.S. Nuclear Regulatory Commission). Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants. NUREG-1150, Vols. 1-3. Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Division of Systems Research; 1990-1991.
US NRC (Nuclear Regulatory Commission). Common-cause failure database and analysis system: event data collection, Classification, and coding. Technical report NUREG/CR-6268. Washington, DC: US Nuclear Regulatory Commission; 2007.
US NRC (Nuclear Regulatory Commission). Procedure for analysis of common-cause failures in probabilistic safety analysis. Technical report NUREG/CR-5801 (SAND91-7087). Washington, DC: US Nuclear Regulatory Commission; 1993.
US NRC (US Nuclear Regulatory Commission). EPRI/NRC-RES Fire PRA methodology for nuclear power facilities, Volume 2: detailed methodology. Technical Report NUREG-CR-6850. Washington, DC: US Nuclear Regulatory Commission; 2005.
US NRC (US Nuclear Regulatory Commission). An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. NUREG-1.174 – Revision 1. Washington, DC: US Nuclear Regulatory Commission; 2002.
US NRC (US Nuclear Regulatory Commission). Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. NUREG-1855. Washington, DC: US Nuclear Regulatory Commission; 2009.
US NRC (US Nuclear Regulatory Commission). Reactor Safety Study, an Assessment of Accident Risks. WASH 1400, Report NUREG-75/014. Washington, DC (USA): U.S. Nuclear Regulatory Commission; 1975.
Valdebenito MA, Pradlwarter HJ, Schueller GI. The role of the design point for calculating failure probabilities in view of dimensionality and structural nonlinearities. Structural Safety 2010; 32(2): 101-111.

Vaurio JK. Consistent mapping of common cause failure rates and alpha factors. Reliability Engineering and System Safety 2007; 92(5): 628–645.
Vaurio JK. Treatment of General Dependencies in System Fault-Tree and Risk Analysis. IEEE Transactions on Reliability 2002; 51(3): 278-287.
Viertl R, Hareter D. Fuzzy information and imprecise probability. ZAMM, Z. Angew. Math. Mech. 2004; 84(10–11): 731 – 739.
Viertl R, Hareter D. Generalized Bayes-theorem for non-precise a-priori distribution. Metrika 2004; 59(3): 263–273.
Viertl R, Hule H. On Bayes' theorem for fuzzy data. Stat. Pap. 1991; 32: 115-122.
Viertl R. Foundations of Fuzzy Bayesian Inference. Journal of Uncertain Systems 2008a; 2(3): 187–191.
Viertl R. Fuzzy Bayesian Inference. In: Dubois D, Lubiano MA, Prade H, Gil MA, Grzegorzewski P, Hryniewicz O, Eds. Soft Methods for Handling Variability and Imprecision, Series Advances in Intelligent and Soft-Computing 48. Berlin Heidelberg: Springer-Verlag; 2008b. p. 10–15.
Viertl R. On statistical inference for non precise data. Environmetrics 1997; 8: 541-568.
Viertl R. Statistical Methods for Fuzzy Data. Chichester, UK: Wiley; 2011.
Viertl R. Statistical Methods for Non-Precise Data. Boca Raton, FL; New York, NY; London, UK; Tokyo, Japan: CRC Press; 1996.
Viertl R. Statistics and integration of fuzzy functions. Environmetrics 1999; 10: 487-491.
Villemonteix J, Vazquez E,Walter E. An informational approach to the global optimization of expensive-to-evaluate functions. Journal of Global Optimization 2009; 44(4): 509–534.
Villén-Altamirano J. Asymptotic optimality of RESTART estimators in highly dependable systems. Reliability Engineering & System Safety 2014; 130: 115-124.
Villén-Altamirano J. Importance functions for restart simulation of general Jackson networks. European Journal of Operational Research 2010; 203(1): 156-165.
Villén-Altamirano J. Importance functions for RESTART simulation of highly-dependable systems. Simulation 2007; 83(12): 821-828.
Villén-Altamirano M, Villén-Altamirano J. Analysis of RESTART simulation: Theoretical basis and sensitivity study. European Transactions on Telecommunications 2002; 13(4): 373-385.
Villén-Altamirano M, Villén-Altamirano J. On the efficiency of RESTART for multidimensional state systems. ACM Transactions on Modeling and Computer Simulation (TOMACS) 2006; 16(3): 251-279.
Villén-Altamirano M, Villén-Altamirano J. RESTART: a straightforward method for fast simulation of rare events. Simulation Conference Proceedings, 1994. Winter; 11-14 Dec. 1994; Orlando, FL. IEEE; 1994. p. 282 – 289.
Volkova E, Iooss B, Van Dorpe F. Global sensitivity analysis for a numerical model of radionuclide migration from the RRC "Kurchatov Institute" redwaste disposal site. Stoch Environ Res Assess 2008; 22: 17-31.
Walley P. Statistical reasoning with imprecise probabilities. New York, NY: Chapman and Hall; 1991.
Wang S, Hong L, Chen X, Zhang J, Yan Y. Review of interdependent infrastructure systems vulnerability analysis. Intelligent Control and Information Processing (ICICIP), 2nd International Conference on; 25-28 July 2011; Herbin, China. IEEE; 2011. p. 446-451.
Wang TR, Mousseau V, Pedroni N, Zio E. An empirical classification-based framework for the safety-related criticality assessment of complex energy production systems, in presence of inconsistent data. Under first review on Reliability Engineering and System Safety 2015a.
Wang TR, Mousseau V, Pedroni N, Zio E. Assessing the Performance of a Classification-Based Vulnerability Analysis Model. Accepted for publication on Risk Analysis, an International Journal 2015b.
Wang TR, Mousseau V, Pedroni N, Zio E. Identification of protective actions to reduce the vulnerability of safety-critical systems to malevolent intentional acts: an optimization-based decision-making approach. Submitted for publication on European Journal of Operational Research 2015c.
Wang TR, Pedroni N, Zio E. Identification of protective actions to reduce the vulnerability of safety-critical systems to malevolent intentional acts: a sensitivity-based decision-making approach. Accepted for publication on Reliability Engineering and System Safety 2015d.
Wang Z, Scaglione A, Thomas RJ. A Markov-transition model for cascading failures in power grids. In: Proceedings of the 45th Hawaii International Conference on System Science (HICSS); 4-7 Jan. 2012; Maui, HI 2012. IEEE; 2012. p. 2115-2124.
Wang H, Thorp JS. Optimal locations for protection system enhancement: a simulation of cascading outages. IEEE Transactions on Power Delivery 2001; 16(4): 528-533.
Watts DJ. A simple model of global cascades on random networks. Proceedings of the National Academy of Sciences 2002; 99(9): 5766-5771.
Waugh, WL. Terrorism and the all-hazard model. Journal of Emergency Management 2005; 4: 8–10.
Weichselberger K. The theory of interval-probability as a unifying concept for uncertainty. Int. J. Approx. Reasoning 2000; 24(2–3): 149–170.
Weichselgartner J. Disaster mitigation: the concept of vulnerability revisited. Disaster Prevention and Management 2001; 10(2): 85-95.
Weron R, Simonsen I. Blackouts, risk, and fat-tailed distributions. In: Practical Fruits of Econophysics 2006. Tokyo, Japan: Springer; p. 215-219.

Wilkinson S, Dunn S, Ma S. The vulnerability of the European air traffic network to spatial hazards. Natural Hazards 2012; 60(3): 1027-1036.
Williamson RC, Downs T. Probabilistic arithmetic I: Numerical methods for calculating convolutions and dependency bounds. International Journal of Approximate Reasoning 1990; 4: 89-158.
Winkler RL. Uncertainty in probabilistic risk assessment. Reliability Engineering and System Safety 1996; 85: 127-132.
Yang, JE. Development of an integrated risk assessment framework for internal/external events and all power models. Nuclear Engineering and Technology 2012; 44(5): 459-470.
Zadeh LA. Fuzzy sets as a basis for a theory of possibility. Fuzzy Sets and Systems 1978; 1: 3-28.
Zadeh LA. Fuzzy sets. Information and Control 1965; 8: 338–353.
Zhang H, Dai H, Beer M, Wang W. Structural reliability analysis on the basis of small samples: An interval quasi-Monte Carlo method. Mechanical Systems and Signal Processing 2013; 37(1-2): 137-151.
Zhang Q. A general method dealing with correlations in uncertainty propagation in fault trees. Reliability Engineering and System Safety 1989; 26(3): 231–247.
Zhang Q. A method dealing with correlations in uncertainty propagation by using traditional correlation coefficients. Reliability Engineering and System Safety 1993; 41(2): 107–114.
Zhao K, Kumar A, Harrison TP, Yen J. Analyzing the resilience of complex supply network topologies against random and targeted disruptions. IEEE Systems Journal 2011; 5(1): 28-39.
Zhu D, Mosleh A, Smidts C. A framework to integrate software behavior into dynamic probabilistic risk assessment. Reliability Engineering & System Safety 2007; 92(12): 1733-1755.
Zio E. A study of the bootstrap method for estimating the accuracy of artificial neural networks in predicting nuclear transient processes. IEEE Transactions on Nuclear Science 2006; 53(3): 1460-1470.
Zio E. From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. International Journal of Critical Infrastructures 2007; 3(3): 488-508.
Zio E. Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions. Nuclear Engineering and Design 2014a; 280: 413-419.
Zio E. Reliability engineering: Old problems and new challenges. Reliability Engineering and System Safety 2009; 94: 125–141.
Zio E. The Monte Carlo Simulation Method for System Reliability and Risk Analysis. Springer Series in Reliability Engineering. London, UK: Springer; 2013.
Zio E. Vulnerability and risk analysis of critical infrastructures. Proceedings of the Second International Conference on Vulnerability and Risk Analysis and Management (ICVRAM2014) and Sixth International Symposium on Uncertainty, Modeling and Analysis (ISUMA2014); 13–16 Jul 2014; University of Liverpool, Liverpool, UK. American Society of Civil Engineers 2014b. p. 23-30.
Zio E, Aven T. Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them? Energy Policy 2011; 39(10): 6308-6320.
Zio E, Apostolakis GE, Pedroni N. Quantitative functional failure analysis of a thermal–hydraulic passive system by means of bootstrapped Artificial Neural Networks. Annals of Nuclear Energy 2010; 37(5): 639-649.
Zio E, Pedroni N. Building Confidence in the Reliability Assessment of Thermal-Hydraulic Passive Systems. Reliability Engineering and System Safety 2009a; 94(2): 268-281.
Zio E, Pedroni N. Estimation of the functional failure probability of a thermal-hydraulic passive systems by means of Subset Simulation. Nuclear Engineering and Design 2009b; 239: 580-599.
Zio E, Pedroni N. Functional failure analysis of a thermal-hydraulic passive system by means of Line Sampling. Reliability Engineering and System Safety 2009c; 94(11): 1764-1781.
Zio E, Pedroni N. An optimized Line Sampling method for the estimation of the failure probability of nuclear passive systems. Reliability Engineering and System Safety 2010a; 95(12): 1300-1313.
Zio E, Pedroni N. Reliability Estimation by Advanced Monte Carlo Simulation. In: J. Faulin, A.A. Juan, S. Martorell, J.E. Ramirez-Marquez (Eds). Simulation Methods for Reliability and Availability of Complex Systems (Springer series in Reliability Engineering). Springer-Verlag, London, United Kingdom; 2010b. p. 3-39.
Zio E, Pedroni N. How to effectively compute the reliability of a thermal-hydraulic passive system. Nuclear Engineering and Design 2011; 241(1): 310-327.
Zio E, Pedroni N. Monte Carlo Simulation-based Sensitivity Analysis of the model of a Thermal-Hydraulic Passive System. Reliability Engineering and System Safety 2012; 107: 90-106.
Zio E, Piccinelli R, Sansavini G. An all-hazard approach for the vulnerability analysis of critical infrastructures. Proceedings of the European Safety and RELiability (ESREL) 2011 Conference; 18-23 September 2011; Troyes, France. London, United Kingdom: Taylor & Francis Group; 2012. p. 2451–2458.
Zio E, Sansavini G. Component Criticality in Failure Cascade Processes of Network Systems. Risk Analysis 2011a; 31(8): 1196–1210.
Zio E, Sansavini G. Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Transactions on Reliability 2011b; 60(1): 94-101.
Zio E, Sansavini G, Maja R, Marchionni G. An analytical approach to the safety of road networks. International Journal of Reliability, Quality and Safety Engineering 2008; 15(01): 67-76.

Appendix: Contents of six selected publications

Paper I

N. Pedroni, E. Zio, E. Ferrario, A. Pasanisi, M. Couplet, "Hierarchical propagation of probabilistic and non-probabilistic uncertainty in the parameters of a risk model", *Computers and Structures* (*Special Issue on Uncertainty Quantification in Structural Analysis and Design*), Vol. 126, Sept. 2013, pp. 199–213, ISSN 0045-7949, published by Elsevier Ltd.

Paper II

N. Pedroni, E. Zio, "Uncertainty analysis in fault tree models with dependent basic events", *Risk Analysis, an International Journal*, Vol. 33, Issue 6, 2013, pp. 1146–1173, ISSN 0272-4332, published by Wiley-Blackwell.

Paper III

E. Ferrario, N. Pedroni, E. Zio, "Analysis of the robustness and recovery of critical infrastructures by Goal Tree Success Tree – Dynamic Master Logic Diagram, within a multi-state system-of-systems framework, in the presence of epistemic uncertainty", *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering* (*Special Issue on Non-probabilistic Approaches for Handling Uncertainty in Engineering*), Vol. 1(3), paper 031001; doi: 10.1115/1.4030439, ISSN 2332-9025, published by the American Society of Mechanical Engineers.

Paper IV

Y.-P. Fang, N. Pedroni, E. Zio, "Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network", accepted for publication on *IEEE Systems Journal*, 2015, doi: 10.1109/JSYST.2014.2352152, ISSN 1932-8184, published by IEEE Systems Council, Institute of Electrical and Electronics Engineers.

Paper V

E. Zio, N. Pedroni, "How to effectively compute the reliability of a thermal-hydraulic passive system", *Nuclear Engineering and Design*, Volume 241, Issue 1, Jan. 2011, pp. 310-327, ISSN 0029-5493, published by Elsevier Ltd.

Paper VI

T.-R. Wang, V. Mousseau, N. Pedroni, E. Zio, "Assessing the Performance of a Classification-Based Vulnerability Analysis Model", accepted for publication on *Risk Analysis, an International Journal*, 2014, doi: 10.1111/risa.12305, ISSN 0272-4332, published by Wiley-Blackwell.

Computers and Structures 126 (2013) 199–213

Contents lists available at SciVerse ScienceDirect

Computers and Structures

journal homepage: www.elsevier.com/locate/compstruc

Hierarchical propagation of probabilistic and non-probabilistic uncertainty in the parameters of a risk model

N. Pedroni [a], E. Zio [a,b,*,1,2], E. Ferrario [b,1,2], A. Pasanisi [c], M. Couplet [c]

[a] Energy Department, Politecnico di Milano, Via Ponzio, 34/3 – 20133 Milano, Italy
[b] Ecole Centrale Paris, Grande Voie des Vignes, 92295, Chatenay Malabry-Cedex, France
[c] Electricité de France, Chatou, France

ARTICLE INFO

Article history:
Received 21 May 2012
Accepted 6 February 2013
Available online 13 March 2013

Keywords:
Hierarchical uncertainty
Possibility distributions
Fuzzy interval analysis
Two-level Monte Carlo method
Dependences
Flood protection dike

ABSTRACT

We consider a model for the risk-based design of a flood protection dike, and use probability distributions to represent aleatory uncertainty and possibility distributions to describe the epistemic uncertainty associated to the poorly known parameters of such probability distributions.

A hybrid method is introduced to hierarchically propagate the two types of uncertainty, and the results are compared with those of a Monte Carlo-based Dempster–Shafer approach employing independent random sets and a purely probabilistic, two-level Monte Carlo approach: the risk estimates produced are similar to those of the Dempster–Shafer method and more conservative than those of the two-level Monte Carlo approach.

© 2013 Elsevier Ltd. All rights reserved.

1. Introduction

In risk analysis, uncertainty is typically distinguished into two types: randomness due to inherent variability in the system behavior and imprecision due to lack of knowledge and information on the system. The former type of uncertainty is often referred to as objective, aleatory, stochastic whereas the latter is often referred to as subjective, epistemic, state of knowledge [1,2].

We are interested in the framework of two hierarchical levels of uncertainty, referred to as "two-level" setting [3]: the models of the aleatory events (e.g., the failure of a mechanical component or the variation of its geometrical dimensions and material properties) contain parameters (e.g., probabilities, failure rates,...) that are epistemically uncertain because known with poor precision by the analyst.

Both the aleatory and epistemic uncertainties in the two-level framework can be represented by probability distributions, and propagated by two-level (or double loop) Monte Carlo (MC) simulation [4]: in the outer simulation loop, the values of the parameters affected by epistemic uncertainty are sampled and fed onto the probability distributions of the inner loop where the aleatory variables are sampled [5,6].

In some cases, the imprecise knowledge, incomplete information and scarce data impair the probabilistic representation of epistemic uncertainty. A number of alternative representation frameworks have been proposed to handle such cases [7], e.g., fuzzy set theory [8], Dempster–Shafer theory of evidence [9–14], possibility theory [15–18] and interval analysis [19–21].

In this paper, we use probability distributions to describe the first level aleatory uncertainty and possibility distributions to describe the second level epistemic uncertainty in the parameters of such probability distributions [15–18].

For the propagation of the hybrid (probabilistic and possibilistic) uncertainty representation, the MC technique [22,23] is combined with the extension principle of fuzzy set theory [24–33], within a "two-level" hierarchical setting [16,34–39]. This is done by (i) fuzzy interval analysis to process the uncertainty described by possibility distributions, (ii) repeated MC sampling of the random variables to process aleatory uncertainty [16,24,29].

The joint hierarchical propagation of probabilistic and possibilistic representations of uncertainty is applied to a model for the risk-based design of a flood protection dike developed as a realistic benchmark for uncertainty modeling [3]; the effectiveness of the propagation method is compared to that of: (i) a Monte Carlo (MC)-based Dempster–Shafer (DS) approach employing independent random sets (IRSs) (i.e., where the epistemically uncertain parameters are represented by *discrete*focal sets that are *randomly*

* Corresponding author at: Energy Department, Politecnico di Milano, Via Ponzio, 34/3 – 20133 Milano, Italy. Tel.: +39 02 2399 6340; fax: +39 02 2399 6309.
E-mail addresses: nicola.pedroni@mail.polimi.it (N. Pedroni), enrico.zio@polimi.it, enrico.zio@ecp.fr (E. Zio), alberto.pasanisi@edf.fr (A. Pasanisi).
[1] Chair of system science and the energetic challenge, Electricité de France-Ecole Centrale Paris and Supelec.
[2] Tel.: +33 01 41 13 16 06; fax: +33 01 41 13 12 72.

0045-7949/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compstruc.2013.02.003

and *independently* sampled by MC)[3] [40–50], (ii) a traditional two-level MC approach [2,4,6]. To the best of the authors' knowledge, this is the first time that the above mentioned methods are systematically compared with reference to *risk* assessment problems where *hybrid* uncertainty is separated into two *hierarchical* levels.

The remainder of the paper is organized as follows. In Section 2, the hybrid method for uncertainty propagation is described; in Section 3, the flood model is presented; in Section 4, the results of the joint hierarchical propagation of aleatory and epistemic uncertainties through the model of Section 3, and the comparison with the MC-based DS-IRS and two-level MC approaches are reported and commented; in Section 5, conclusions are provided. The details about the hybrid, MC-based DS-IRS and two-level MC computational procedures are given in Appendices A, B and C, respectively.

2. Joint hierarchical propagation of aleatory and epistemic uncertainties in a "two-level" framework

In all generality, we consider a model whose output is a function $Z = f(Y_1, Y_2, \ldots, Y_n)$ of n uncertain variables Y_i, $i = 1, \ldots, n$, ordered in such a way that the first k, $Y_1, Y_2, \ldots, Y_j, \ldots, Y_k$, are "probabilistic", i.e., their uncertainty is described by probability distributions $p_{Y_1}(y_1|\boldsymbol{\theta}_1), p_{Y_2}(y_2|\boldsymbol{\theta}_2), \ldots, p_{Y_j}(y_j|\boldsymbol{\theta}_j), \ldots, p_{Y_k}(y_k|\boldsymbol{\theta}_k)$, where $\boldsymbol{\theta}_j = \{\theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j}\}, j = 1, 2, \ldots, k$, are the vectors of the corresponding internal parameters, and the last $n-k$, $Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n$, are "purely possibilistic", i.e., their uncertainty is epistemic and represented by the possibility distributions $\pi^{Y_{k+1}}(y_{k+1}), \pi^{Y_{k+2}}(y_{k+2}), \ldots, \pi^{Y_l}(y_l), \ldots, \pi^{Y_n}(y_n)$.

In a "two-level" framework, the parameters $\boldsymbol{\theta}_j$, $j = 1, 2, \ldots, k$, are themselves affected by epistemic uncertainty. We describe these uncertainties by possibility distributions $\boldsymbol{\pi}^{\theta_j}(\boldsymbol{\theta}_j) = \{\pi^{\theta_{j,1}}(\theta_{j,1}), \pi^{\theta_{j,2}}(\theta_{j,2}), \ldots, \pi^{\theta_{j,m_j}}(\theta_{j,m_j})\}$, $j = 1, 2, \ldots, k$. For clarification by way of example, we may consider $Y \sim N(\mu, \sigma) = N(\boldsymbol{\theta}) = N(\theta_1, \theta_2)$, where the parameter $\mu = \theta_1$ has a triangular possibility distribution with core $\{c\}$ and support $[a, b]$, and parameter $\sigma = \theta_2$ has a triangular possibility distribution with core $\{f\}$ and support $[e, d]$.

The propagation of the hybrid uncertainty can be performed by combining the Monte Carlo (MC) technique [22,23] with the extension principle of fuzzy set theory [24–33] by means of the following two main steps [16,34–39]:

i. fuzzy interval analysis to process epistemic uncertainty;
ii. repeated MC sampling of the random variables to process aleatory uncertainty.

Technical details about the operative steps of the procedure are given in Appendix A.

The method produces m possibility distributions $\pi_i^f(z)$, $i = 1, 2, \ldots, m$, for the output variable $Z = f(Y_1, Y_2, \ldots, Y_n)$ (where m is the number of random samples of the aleatory variables drawn by MC). Then, for each set Acontained in the universe of discourse U_Z of Z, it is possible to obtain the possibility measure $\Pi_i^f(A)$ and the necessity measure $N_i^f(A)$ from $\pi_i^f(z)$, $i = 1, 2, \ldots, m$, by:

$$\Pi_i^f(A) = \max_{z \in A}\{\pi_i^f(z)\}, \tag{1}$$

$$N_i^f(A) = \inf_{z \notin A}\{1 - \pi_i^f(z)\} = 1 - \Pi_i^f(\overline{A}) \quad \forall A \subseteq U_Z. \tag{2}$$

The m different realizations of possibility and necessity can then be combined to obtain the belief $Bel(A)$ and the plausibility $Pl(A)$ for any set A, respectively [15]:

$$Bel(A) = \sum_{i=1}^{m} p_i N_i^f(A), \tag{3}$$

$$Pl(A) = \sum_{i=1}^{m} p_i \Pi_i^f(A), \tag{4}$$

where p_i is the probability of sampling the i-th realization of the random variable vector $(Y_1, Y_2, \ldots, Y_k)$: if m realizations are generated by plain random sampling, then p_i is simply $1/m$. For each set A, this technique thus computes the probability-weighted average of the possibility measures associated with each output fuzzy interval.

The likelihood of the value $f(Y)$ passing a given threshold z can then be computed by considering the belief and the plausibility of the set $A = (-\infty, z]$; in this respect, $Bel\ (f(Y) \in (-\infty, z])$ and $Pl(f(Y) \in (-\infty, z])$ can be interpreted as bounding, average cumulative distributions $\underline{F}(z) = Bel(f(Y) \in (-\infty, z])$, $\overline{F}(z) = Pl(f(Y) \in (-\infty, z])$ [15].

Let the *core* and the *support* of a possibilistic distribution $\pi^f(z)$ be the crisp sets of all points of U_Z such that $\pi^f(z)$ is equal to 1 and nonzero, respectively. Considering a generic value z of $f(Y)$, it is $Pl(f(Y) \in (-\infty, z]) = 1$ if and only if $\Pi_i^f(f(Y) \in (-\infty, z]) = 1$, $\forall i = 1, \ldots, m$, that is, for $z > z^* = \max_i\{\inf(core(\pi_i^f))\}$. Similarly, $Pl(f(Y) \in (-\infty, z]) = 0$ if and only if $\Pi_i^f(f(Y) \in (-\infty, z]) = 0$ $\forall i = 1, \ldots, m$, that is, for $z \leqslant z^* = \min_i\{\inf(\text{support}(\pi_i^f))\}$.

Finally, one way to estimate the total uncertainty on $f(Y)$ is to provide a confidence interval at a given level of confidence, taking the lower and upper bounds from $Pl(f(Y) \in (-\infty, z])$ and $Bel(f(Y) \in (-\infty, z])$, respectively [15]. On the other hand, $Bel(f(Y) \in (-\infty, z])$ and $Pl(f(Y) \in (-\infty, z])$ cannot convey any information on the prediction that $f(Y)$ lies within a given interval $[z_1, z_2]$, since neither $Bel(f(Y) \in [z_1, z_2])$ nor $Pl(f(Y) \in [z_1, z_2])$ can be expressed in terms of $Bel(f(Y) \in (-\infty, z])$ and $Pl(f(Y) \in (-\infty, z])$, respectively.

3. Case study: flood protection risk-based design

The case study deals with the design of a protection dike in a residential area closely located to a river with potential risk of floods. Two issues of concern are: (i) high construction and annual maintenance costs of the dike; (ii) uncertainty in the natural phenomenon of flooding. Then, the different design options must be evaluated within a flooding risk analysis framework accounting for uncertainty.

In Section 3.1, a short description of the model for flood protection dike design is given; in Section 3.2, the uncertain variables of the model are described.

3.1. The model

The maximal water level of the river (i.e., the output variable of the model, Z_c) is given as a function of several (and some uncertain) parameters (i.e., the input variables of the model) [3]:

$$Z_c = Z_v + \left(\frac{Q}{K_s * B * \sqrt{(Z_m - Z_v)/L}}\right)^{3/5}, \tag{5}$$

where:

- Q is the yearly maximal water discharge (m^3/s);
- Z_m and Z_v are the riverbed levels (m asl) at the upstream and downstream part of the river under investigation, respectively;
- K_s is the Strickler friction coefficient;
- B and L are the width and length of the river part (m), respectively.

The input variables are classified as follows:

[3] In the following, this method will be referred to as "MC-based DS-IRS approach" for brevity.

– *Constants:* B = 300 m, L = 5000 m.
– *Uncertain variables:* Q, Z_m, Z_v, K_s.

3.2. The input variables: physical description and representation of the associated uncertainty

The input variables are affected by aleatory and epistemic uncertainties. The aleatory part of the uncertainty is described by probability distributions of defined shape (e.g., normal, exponential,...). The parameters of the probability distributions describing the aleatory uncertainty are themselves affected by epistemic uncertainty represented in terms of possibility distributions.

In this section, a detailed description of the uncertain input variables is given together with the explanation of the reasons underlying the choices of their description by probability and possibility distributions. In particular, in Section 3.2.1, the yearly maximal water flow Q is discussed; in Section 3.2.2, the upstream and downstream riverbed levels Z_m and Z_v are presented; finally, in Section 3.2.3, the Strickler friction coefficient K_s is described.

3.2.1. The yearly maximal water flow, Q

The Gumbel distribution $Gum(q \mid \alpha, \beta)$ is a well-established probabilistic (aleatory) model for maximal flows [3]:

$$Gum(q|\alpha,\beta) = \frac{1}{\beta}\exp\left[-\exp\left(\frac{q-\alpha}{\beta}\right)\right]\exp\left[\frac{\alpha-q}{\beta}\right]. \tag{6}$$

The extreme physical bounds on variable Q are [3]:

– $Q_{\min}$ = 10 m^3/s;
– $Q_{\max}$ = 10,000 m^3/s.

The parameters α and β in (6) are affected by epistemic uncertainty; however, a large amount of data (i.e., 149 annual maximal flow values) is available for performing statistical inference on them. In particular, the point estimates $\hat{\mu}_\alpha$ and $\hat{\mu}_\beta$ and the corresponding standard deviations $\hat{\sigma}_\alpha$ and $\hat{\sigma}_\beta$ have been obtained for the parameters α and β of the Gumbel distribution (6) by performing maximum likelihood estimations with the 149 data available: the method has provided $\hat{\mu}_\alpha = 1013\ m^3/s$, $\hat{\mu}_\beta = 558\ m^3/s$, $\hat{\sigma}_\alpha = 48\ m^3/s$ and $\hat{\sigma}_\beta = 36\ m^3/s$ [3]. Since a large amount of data (i.e., 149) has been used for performing statistical inference on α and β, then the epistemic uncertainty associated to them is mainly of "statistical nature". As a consequence, a probabilistic treatment of this epistemic uncertainty has been proposed in the original paper [3]: in particular, α and β have been chosen to be normally distributed, i.e., $\alpha \sim p^\alpha(\alpha) = N(\hat{\mu}_\alpha, \hat{\sigma}_\alpha) = N(1013, 48)$ and $\beta \sim p^\beta(\beta) = N(\hat{\mu}_\beta, \hat{\sigma}_\beta) = N(558, 36)$ [3].

In the present paper, the Gumbel shape of the aleatory probability distributions (6) is retained but the epistemic uncertainty on the parameters is represented in possibilistic terms: this allows defining a family of probability distributions (properly bounded by plausibility and belief functions) that quantifies the expert's lack of knowledge about the parameters themselves and, thus, his/her inability to select a single probability distribution for them. To do so, the normal probability distributions $p^\alpha(\alpha)$ and $p^\beta(\beta)$ used in [3] are transformed into the possibility distributions $\pi^\alpha(\alpha)$ and $\pi^\beta(\beta)$ by normalization, i.e., $\pi^\alpha(\alpha) = \frac{p^\alpha(\alpha)}{\sup p^\alpha(\alpha)}$, $\pi^\beta(\beta) = \frac{p^\beta(\beta)}{\sup p^\beta(\beta)}$ [16]. The supports of the possibility distributions $\pi^\alpha(\alpha)$ and $\pi^\beta(\beta)$ are set to $[\hat{\mu}_\alpha - \hat{\sigma}_\alpha, \hat{\mu}_\alpha + \hat{\sigma}_\alpha] = [965, 1061]$ and $[\hat{\mu}_\beta - \hat{\sigma}_\beta, \hat{\mu}_\beta + \hat{\sigma}_\beta] = [523, 594]$, respectively, according to the suggestions by Limbourg and de Rocquigny [3]. The possibility distributions $\pi^\alpha(\alpha)$ and $\pi^\beta(\beta)$ are shown in Fig. 1, left and right, respectively.

Notice that in the present paper, the choice of transforming probability density functions into possibility distribution by *normalization* has been made arbitrarily, for the sake of simplicity, accepting that the resulting possibility distributions do not in general adhere to the probability–possibility consistency principle [51]; other techniques of transformation of probability density functions into possibility distributions exist, e.g., the principle of maximum specificity [52] and the principle of minimal commitment [53].

3.2.2. The upstream and downstream riverbed levels, Z_m and Z_v

The minimum and maximum physical bounds on variables Z_m and Z_v are $Z_{m,\min}$ = 53.5 m, $Z_{v,\min}$ = 48 m, $Z_{m,\max}$ = 57 m and $Z_{v,\max}$ = 51 m, respectively [3].

Normal distributions truncated at the minimum and maximum physical bounds have been selected in [3] to represent the aleatory part of the uncertainty, i.e., $Z_m \sim N(\mu_{Zm}, \sigma_{Zm})$ and $Z_v \sim N(\mu_{Zv}, \sigma_{Zv})$. An amount of 29 data has been used in the reference paper [3] to provide the point estimates $\hat{\mu}_{Zm} = 55.03$ m, $\hat{\mu}_{Zv} = 50.19$ m, $\hat{\sigma}_{Zm} = 0.45$ m, $\hat{\sigma}_{Zv} = 0.38$ m for parameters μ_{Zm}, μ_{Zv}, σ_{Zm} and σ_{Zv}, respectively, by means of the maximum likelihood estimation method. However, according to [3] there is large uncertainty about the shape of the probability distributions of Z_m and Z_v: as a consequence the authors embrace a conservative "two-level" framework, using the maximum likelihood estimation method to provide also standard deviations as a measure of the uncertainty on the point estimates $\hat{\mu}_{Zm}$, $\hat{\mu}_{Zv}$, $\hat{\sigma}_{Zm}$ and $\hat{\sigma}_{Zv}$: in particular, $\hat{\sigma}_{\hat{\mu}_{Zm}} = 0.08$, $\hat{\sigma}_{\hat{\mu}_{Zv}} = 0.07$, $\hat{\sigma}_{\hat{\sigma}_{Zm}} = 0.06$ and $\hat{\sigma}_{\hat{\sigma}_{Zv}} = 0.05$. Using this information, the authors in [3] model the epistemic uncertainty associated to the parameters μ_{Zm}, μ_{Zv}, σ_{Zm} and σ_{Zv} by normal distributions, i.e., $\mu_{Zm} \sim N(\hat{\mu}_{Zm}, \hat{\sigma}_{\hat{\mu}_{Zm}})$, $\mu_{Zv} \sim N(\hat{\mu}_{Zv}, \hat{\sigma}_{\hat{\mu}_{Zv}})$, $\sigma_{Zm} \sim N(\hat{\sigma}_{Zm}, \hat{\sigma}_{\hat{\mu}_{Zm}})$ and $\sigma_{Zv} \sim N(\hat{\sigma}_{Zv}, \hat{\sigma}_{\hat{\sigma}_{Zv}})$.

In this paper, the shapes of the aleatory probability distributions for Z_m and Z_v, i.e., $N(\mu_{Zm}, \sigma_{Zm})$ and $N(\mu_{Zv}, \sigma_{Zv})$, are kept unaltered with respect to those of [3]; on the contrary, the information produced by the maximum likelihood estimation method on parameters μ_{Zm}, μ_{Zv}, σ_{Zm} and σ_{Zv}, i.e., the point estimates $\hat{\mu}_{Zm}$, $\hat{\mu}_{Zv}$, $\hat{\sigma}_{Zm}$, $\hat{\sigma}_{Zv}$ and the corresponding standard deviations $\hat{\sigma}_{\hat{\mu}_{Zm}}$, $\hat{\sigma}_{\hat{\mu}_{Zv}}$, $\hat{\sigma}_{\hat{\sigma}_{Zm}}$, $\hat{\sigma}_{\hat{\sigma}_{Zv}}$, is used to build possibility distributions for μ_{Zm}, μ_{Zv}, σ_{Zm} and σ_{Zv} by means of the Chebyshev inequality [54,55]. The classical Chebyshev inequality [54,55] defines a bracketing approximation on the confidence intervals around the known mean μ of a random variable Y, knowing its standard deviation σ. The Chebyshev inequality can be written as follows:

$$P(|Y-\mu| \leqslant k\sigma) \geqslant 1 - \frac{1}{k^2} \quad \text{for } k \geqslant 1. \tag{7}$$

Formula (7) can be thus used to define a possibility distribution π that dominates any probability density function with given mean μ and standard deviation σ by considering intervals $[\mu - k\sigma, \mu + k\sigma]$ as α-cuts of π and letting $\pi(\mu - k\sigma) = \pi(\mu + k\sigma) = \frac{1}{k^2} = \alpha$. This possibility distribution defines a probability family $\mathcal{P}^{\mu,\sigma}(\pi)$ which has been proven to contain all probability distributions with mean μ and standard deviation σ, whether the unknown probability distribution function is symmetric or not, unimodal or not [54].

In this case, the point estimates $\hat{\mu}_{Zm}$, $\hat{\mu}_{Zv}$, $\hat{\sigma}_{Zm}$ and $\hat{\sigma}_{Zv}$ produced by the maximum likelihood estimation method, are used in (7) as the means of the parameters μ_{Zm}, μ_{Zv}, σ_{Zm} and σ_{Zv}, whereas the errors $\hat{\sigma}_{\hat{\mu}_{Zm}}$, $\hat{\sigma}_{\hat{\mu}_{Zv}}$, $\hat{\sigma}_{\hat{\sigma}_{Zm}}$ and $\hat{\sigma}_{\hat{\sigma}_{Zv}}$ associated to the estimates $\hat{\mu}_{Zm}$, $\hat{\mu}_{Zv}$, $\hat{\sigma}_{Zm}$ and $\hat{\sigma}_{Zv}$ are used in (7) as the standard deviations of the parameters μ_{Zm}, μ_{Zv}, σ_{Zm} and σ_{Zv} in order to build the corresponding possibility distributions $\pi^{\mu_{Zm}}$, $\pi^{\mu_{Zv}}$, $\pi^{\sigma_{Zm}}$ and $\pi^{\sigma_{Zv}}$; the supports of the possibility distributions are obtained by extending two times the standard deviation $\hat{\sigma}_{\hat{\mu}_{Zm}}$, $\hat{\sigma}_{\hat{\mu}_{Zv}}$, $\hat{\sigma}_{\hat{\sigma}_{Zm}}$ and $\hat{\sigma}_{\hat{\sigma}_{Zv}}$ in both directions with respect to the estimates $\hat{\mu}_{Zm}$, $\hat{\mu}_{Zv}$, $\hat{\sigma}_{Zm}$ and $\hat{\sigma}_{Zv}$ (Figs. 2 and 3).

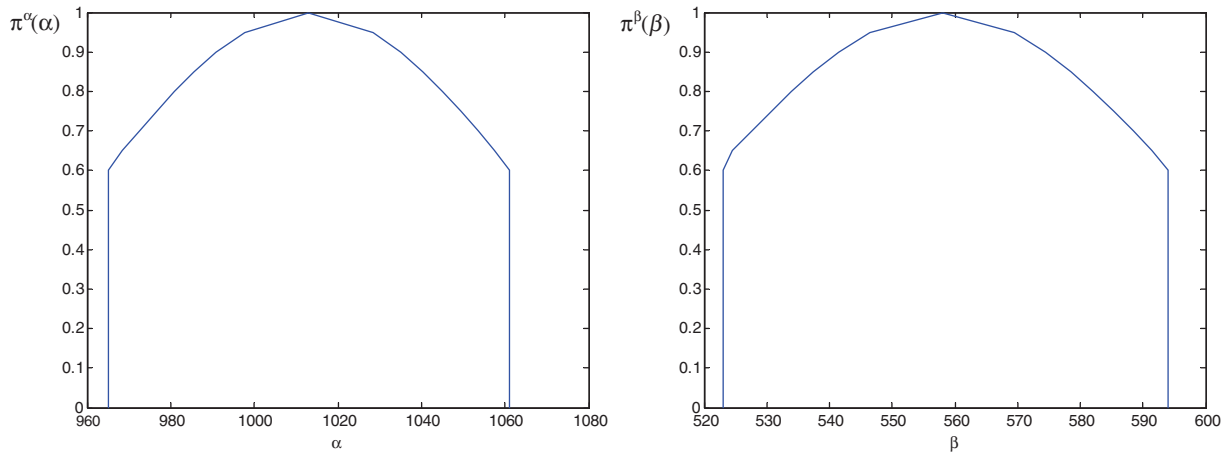


Fig. 1. Possibility distributions $\pi^{\alpha}(\alpha)$ (left) and $\pi^{\beta}(\beta)$ (right) of the parameters α and β of the Gumbel probability distribution (6) of the maximal water flow Q [m^3/s], obtained by normalization of the probability distributions $p^{\alpha}(\alpha)$ and $p^{\beta}(\beta)$ proposed in [3].

3.2.3. The Strickler friction coefficient, K_s

The Strickler friction coefficient K_s is the most critical source of uncertainty because it is usually a simplification of a complex hydraulic model. The absolute physical limits of K_s are $[a,b] = [5,60]$ [3].

The friction coefficient K_s is affected by random events modifying the river status (e.g., erosion): the corresponding variability is typically described by a normal distribution, i.e., $K_s \sim N(\mu_{Ks}, \sigma_{Ks})$ [3]. However, the mean value μ_{Ks} of this normal distribution is difficult to measure because data can only be obtained through "indirect calibration characterized by significant uncertainty": in [3] this is reflected in a "very small set of five data available with ±15% noise". The sample mean $\hat{\mu}_{Ks}$ and standard deviation $\hat{\sigma}_{Ks}$ of these five pieces of data equal 27.8 and 3, respectively. In order to reflect the imprecision generated by the indirect measurement process, the "minimal sample mean" $\hat{\mu}_{\min} = 23.63$ and the "maximal sample mean" $\hat{\mu}_{\max} = 31.97$ are also calculated under the conservative hypothesis that all measurements are biased in the same direction [3]. Moreover, since the small sample size adds a non-negligible "statistical epistemic uncertainty" to the values $\hat{\mu}_{\min}$ and $\hat{\mu}_{\max}$, as described in [3] the 70% confidence bounds on $\hat{\mu}_{\min}$ and $\hat{\mu}_{\max}$ are also computed as $\hat{\mu}_{\min} - \frac{\hat{\sigma}_{Ks}}{\sqrt{5}} = 22.3$ and $\hat{\mu}_{\min} - \frac{\hat{\sigma}_{Ks}}{\sqrt{5}} = 33.3$, respectively. In [3], these considerations result in the following uncertainty quantification for K_s:

$$K_s \sim N(\mu_{Ks}, \sigma_{Ks}),$$

$$\text{with } \sigma_{Ks} = \hat{\sigma}_{Ks} = 3 \text{ and } \mu_{Ks} \in \left[\hat{\mu}_{\min} - \frac{\hat{\sigma}_{Ks}}{\sqrt{5}}, \hat{\mu}_{\max} + \frac{\hat{\sigma}_{Ks}}{\sqrt{5}}\right] = [22.3, 33.3]. \tag{8}$$

In this paper, the shape of the aleatory probability distribution of K_s, i.e., $N(\mu_{Ks}, \sigma_{Ks})$ in (8) is retained; however, differently from the original paper, a possibility distribution is associated to μ_{Ks}. In particular, a trapezoidal possibility distribution is here proposed: the support is chosen to be $[a,b] = \left[\hat{\mu}_{\min} - \frac{\hat{\sigma}_{Ks}}{\sqrt{5}}, \hat{\mu}_{\max} + \frac{\hat{\sigma}_{Ks}}{\sqrt{5}}\right] = [22.3, 33.3]$ as in (8); however, in this paper additional information is provided concerning the most likely values of μ_{Ks} exploiting the available data set: in particular, since the core of the trapezoidal distribution contains the most likely values of the parameter μ_{Ks}, in this case it is set to $[c,d] = \left[\hat{\mu}_{\min} - \frac{\hat{\sigma}_{Ks}}{\sqrt{5}}, \hat{\mu}_{\max} + \frac{\hat{\sigma}_{Ks}}{\sqrt{5}}\right] = [26.5, 29.1]$, i.e., the interval obtained by adding/subtracting to the sample mean $\hat{\mu}_{Ks} = 27.8$ (which is *assumed* to be the *most likely* value for μ_{Ks}) the "statistical" epistemic uncertainty due to the low sample size (i.e., the quantity $\frac{\hat{\sigma}_{Ks}}{\sqrt{5}}$) (Fig. 4).

A final remark is in order with respect to the approaches considered in this work for constructing possibility distributions. The construction of the possibility distribution obviously depends on the information available on the uncertain parameter: when a probability distribution is originally available a corresponding possibility distribution can be generated by resorting to the probability–possibility transformations available in the open literature, e.g., the normalization method (like in the present case), the principle of maximum specificity or that of minimal commitment [29,52,53]; when the mean and the standard deviation of the parameter distribution can be estimated, e.g., by means of empirical data, the Chebyshev inequality can be used; finally, when the absolute physical limits and the most likely value(s) of the parameter are available, a triangular or trapezoidal possibility distribution can be constructed.

4. Application

In this Section, the hybrid method described in Section 2 is applied with the procedure in Appendix A to hierarchically propagate probabilistic and possibilistic uncertainties through the model of Section 3.1, in a "two-level" framework. The results obtained by the hybrid approach are compared to those produced by (i) a traditional one-level pure probabilistic approach, where the parameters of the aleatory probability distributions are fixed, known values (only for illustration purposes, Section 4.1), (ii) a MC-based DS-IRS approach, where the possibility distributions are encoded into discrete sets that are randomly and independently sampled by MC and (iii) a two-level (or double loop) Monte Carlo (MC) approach, where the parameters of the aleatory probability distributions are uncertain and themselves described by probability distributions (Section 4.2).

4.1. Comparison of the "two-level" hybrid Monte Carlo and possibilistic approach with a one-level pure probabilistic approach

Only for illustration purposes, the following one-level pure probabilistic model has been considered for comparison:

$$Q \sim Gum(\hat{\mu}_{\alpha}, \hat{\mu}_{\beta}) = Gum(1013, 558), \tag{9}$$

$$Z_m \sim N(\hat{\mu}_{Zm}, \hat{\sigma}_{Zm}) = N(55.03, 0.45), \tag{10}$$

$$Z_v \sim N(\hat{\mu}_{Zv}, \hat{\sigma}_{Zv}) = N(50.19, 0.38), \tag{11}$$

$$K_s \sim N(\hat{\mu}_{Ks}, \hat{\sigma}_{Ks}) = N(27.8, 3), \tag{12}$$

where the parameters of the probability distributions are defined in Sections 3.2.1,3.2.2,3.2.3: in particular, the parameters for Q, Z_m and

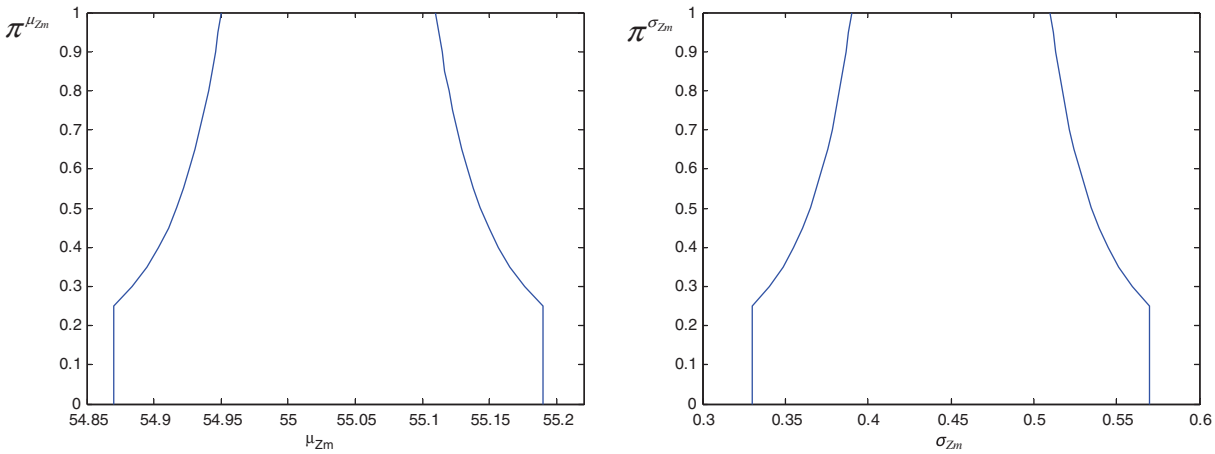


Fig. 2. Left: possibility distribution $\pi^{\mu_{Zm}}$ of μ_{Zm} constructed using Chebyshev inequality (7) with $\hat{\mu}_{Zm} = 55.03$ and $\hat{\sigma}_{\hat{\mu}_{Zm}} = 0.08$. Right: possibility distribution $\pi^{\sigma_{Zm}}$ of σ_{Zm} constructed using Chebyshev inequality (7) with $\hat{\sigma}_{Zm} = 0.45$ and $\hat{\sigma}_{\hat{\sigma}_{Zm}} = 0.06$.

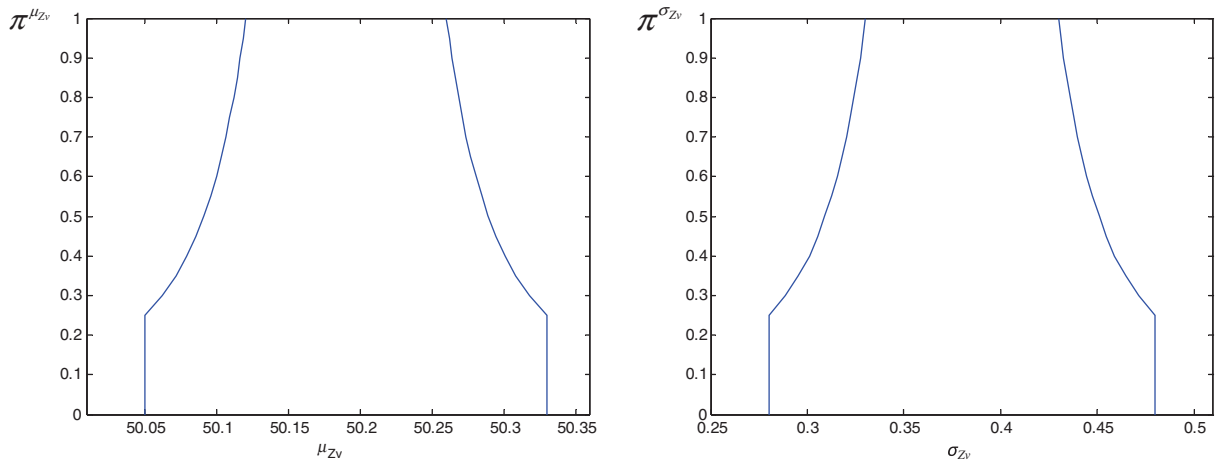


Fig. 3. Left: possibility distribution $\pi^{\mu_{Zv}}$ of μ_{Zv} constructed using Chebyshev inequality (7) with $\hat{\mu}_{Zv} = 50.19$ and $\hat{\sigma}_{\hat{\mu}_{Zv}} = 0.07$. Right: possibility distribution $\pi^{\sigma_{Zv}}$ of σ_{Zv} constructed using Chebyshev inequality (7) with $\hat{\sigma}_{Zv} = 0.38$ and $\hat{\sigma}_{\hat{\sigma}_{Zv}} = 0.05$.

Z_v correspond to their maximum likelihood estimates and the parameter $\hat{\mu}_{Ks}$ of K_s is the sample mean of the five available pieces of data obtained by neglecting measurement uncertainty.

Fig. 5 shows the comparison of the cumulative distribution functions of the maximal water level of the river (i.e., the output variable of the model, Z_c) obtained by the one-level pure probabilistic approach (solid line) with the belief (lower dashed curve) and plausibility (upper dashed curve) functions obtained by the hybrid Monte Carlo and possibilistic approach in a "two-level" setting (Section 2 and Appendix A).

It can be seen that:

- the hybrid approach propagates the uncertainty by separating the aleatory and epistemic components; this separation is visible in the output distributions of the maximal water level of the river where the *separation* between the belief and plausibility functions reflects the imprecision in the knowledge of the possibilistic parameters of the probability distributions;
- the uncertainty in the output distribution of the pure probabilistic approach is given *only* by the *slope* of the cumulative distribution;

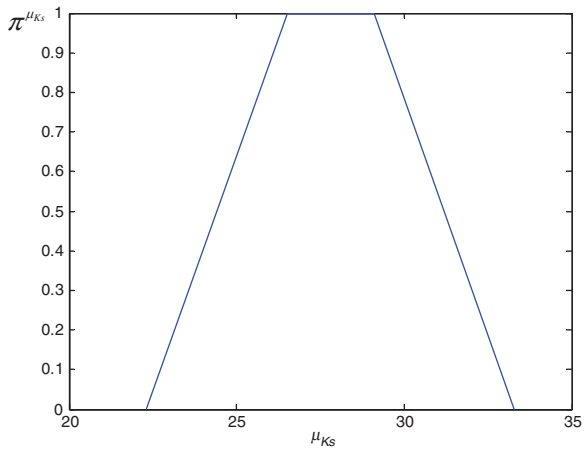


Fig. 4. Trapezoidal possibility distribution function for the parameter μ_{Ks} with support $[a,b] = [22.3, 33.3]$ and core $[c,d] = [26.5, 29.1]$.

- as expected, the cumulative distribution of the maximal water level of the river obtained by the pure probabilistic method is within the belief and plausibility functions obtained by the hybrid approach.

4.2. Comparison of the "two-level" hybrid Monte Carlo and possibilistic approach with the MC-based DS-IRS and two-level (double loop) MC approaches

In this Section, the following approaches are considered and compared in the task of hierarchically propagating aleatory and epistemic uncertainties in a "two-level" framework:

i. the hybrid Monte Carlo (MC) and possibilistic approach of Section 2 and Appendix A;
ii. the Monte Carlo (MC)-based Dempster–Shafer approach employing independent random sets (IRSs) (Appendix B);
iii. a two-level (double loop) MC approach (Appendix C):
   a. assuming independence between the epistemically uncertain parameters of the aleatory probability distributions. This choice has been made to perform a fair comparison with the MC-based DS-IRS approach, which assumes independence between the epistemically uncertain parameters (see Appendix B);
   b. assuming total dependence between the epistemically uncertain parameters of the aleatory probability distributions. This choice has been made to perform a fair comparison with the hybrid MC and possibilistic approach, which implicitly assumes by construction total dependence between the epistemically uncertain parameters (see Section 2 and Appendix A).[4]

It is worth noting that the representation of epistemic uncertainty here used in the MC-based DS-IRS approach entirely relies on the *possibilistic* representation described in Section 3.2 and employed by the hybrid MC and possibilistic approach: however, in order to tailor this possibilistic representation to the DS framework, the possibility distributions of Section 3.2 are *discretized* into *focal* sets (or intervals), each of which is assigned a probability mass: the reader is referred to Appendix B for some details.

In addition, notice that the probability distributions here used in the two-level MC approach for Q, Z_m and Z_v and for the corresponding epistemically uncertain parameters are the same as those proposed in the original paper by Limbourg and de Rocquigny [3] (and recalled in Sections 3.2.1 and 3.2.2); the only exception is represented by the probability distribution for μ_{Ks}, which for consistency and coherence of the comparison is here obtained by normalization of the trapezoidal possibility distribution described in Section 3.2.3 and shown in Fig. 4, i.e.,

$$p^{\mu_{Ks}}(\mu_{Ks}) = \frac{\pi^{\mu_{Ks}}(\mu_{Ks})}{\int_a^b \pi^{\mu_{Ks}}(\mu_{Ks})d\mu_{Ks}}.$$

Table 1 summarizes the characteristics of the approaches i–iii used in the following to propagate aleatory and epistemic uncertainties in a "two-level" framework.

The following comparisons are considered: approaches that represent in the *same* way the epistemic uncertainty (i.e., in terms of probability or possibility distributions) but assume *different* relationships (i.e., dependence or independence) between the epistemically uncertain parameters are compared in Section 4.2.1 (in particular, comparisons are performed between approaches iiia and iiib above and between approaches i and ii above): such comparisons are made to study the effect of the *state of dependence* between the epistemically uncertain parameters of the aleatory probability distributions when a probabilistic/non-probabilistic *representation* of epistemic uncertainty is *given*; approaches assuming the *same* dependence relationship between the epistemically uncertain parameters but employing *different* representations of the epistemic uncertainty are compared in Section 4.2.2 (in particular, comparisons are performed between approaches ii and iiia above and between approaches i and iiib above): such comparison are made to study the effect of the probabilistic/non-probabilistic *representations* of the epistemically uncertain parameters of the aleatory probability distributions when the *state of dependence* between the epistemically uncertain parameters is *given*. Table 2 summarizes the comparisons carried out in the present paper together with the corresponding objectives.

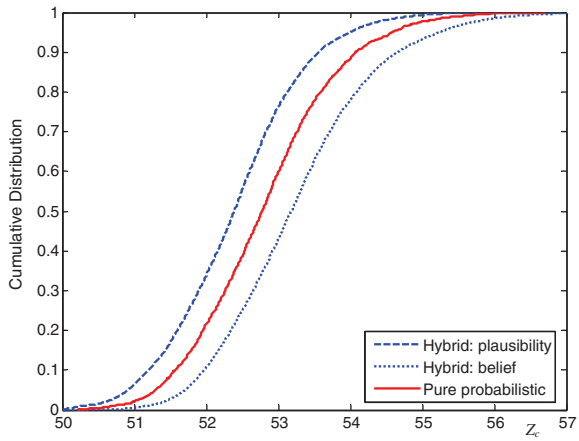


Fig. 5. Comparison of the cumulative distribution function of the maximal water level of the river Z_c obtained by a one-level pure probabilistic approach (solid line) with the belief (lower dashed curve) and plausibility (upper dashed curve) functions obtained by the "two-level" hybrid Monte Carlo and possibilistic approach of Section 2.

A final consideration is in order with respect to the analyses performed in the present paper. Only two *extreme* states of dependence between the epistemically uncertain parameters of the aleatory probability distribution functions (PDFs) are here considered: in particular, independence (methods ii and iiia) and total dependence (methods i and iiib) are assumed between *all* the uncertain parameters of the PDFs of *all* the aleatory variables. On one side, the choice of these extreme conditions serves the purpose of *strongly highlighting* the effects of epistemic dependence between the uncertain parameters, which allows deriving clear indications and guidelines for the application of the different approaches in risk assessment problems. On the other side, such (strong) assumptions of independence or total dependence between *all* the epistemically uncertain parameters may not be realistic in cases of practical interest, like the one analyzed in the present paper. Referring to the previous Section 3.2, it can be seen that the possibility distributions describing the uncertainty in the parameters of the PDFs of the four aleatory variables Q, Z_m, Z_v and K_s are estimated based on four *distinct* data sets (i.e., *one* data set for *each* aleatory variable). This has two implications: (1) when the PDF of a *given* aleatory variable contains *more than one* uncertain parameter (which is the case of Q, Z_m and Z_v), such parameters are *totally dependent* between each other (for example, the location parameter α and the scale parameter β of the PDF of variable Q are totally dependent between each other because their uncertainty is estimated based on the *same* data set); (2) the uncertain parameters of the PDF of a *given* aleatory variable are epistemically *independent* with respect to the parameters of the PDFs of the *other* aleatory variables (for example, the location parameter α and the scale parameter β of the PDF of variable Q are independent from

[4] It is important to note that the condition of total epistemic (or state-of-knowledge) dependence between parameters of risk models is far from unlikely. For example, consider the case of a system containing a number of *physically distinct*, but *similar/nominally identical* components whose failure rates are estimated by means of the *same data set*: in such situation, the distributions describing the uncertainty associated to the failure rates have to be considered *totally dependent* [56,57].

Table 1
Characteristics of the approaches considered to propagate aleatory and epistemic uncertainties in a "two-level" framework.

Method	Epistemic uncertainty representation	Epistemic uncertainty propagation	State of dependence between the epistemically uncertain parameters
Hybrid MC and possibilistic (i)	Possibility distributions	Fuzzy interval analysis	Total dependence
MC-based DS-IRS (ii)	Focal sets with associated probability masses (discretization of possibility distributions)	Random sampling (of discrete focal sets) by MC	Independence
Two-level MC (iii)	Probability distributions	Random sampling (of probability distributions) by MC	Independence (iiia)/total dependence (iiib)

the mean μ_{Zm} and the standard deviation σ_{Zm} of the PDF of variable Z_m because their uncertainty is estimated based on *two different* data sets).

4.2.1. Studying the effect of the state of dependence between the epistemically uncertain parameters of the aleatory probability distributions

We start by comparing approaches iiia and iiib. above, i.e., two-level MC assuming independence and total dependence between the uncertain parameters, respectively: the upper and lower cumulative distribution functions of the model output Z_c obtained by approaches iiia and iiib are shown in Fig. 6.

In this case, assuming total dependence between the uncertain parameters is shown to lead to a smaller gap between the upper and lower cumulative distribution functions of the model output Z_c than assuming independence. This can be easily explained by analyzing the input–output functional relationship of the model (5): it can be seen that one of the input variables (i.e., Q) appears at the numerator, whereas others (i.e., K_s and Z_m) appear at the denominator, and another one appears both at the numerator and at the denominator (i.e., Z_v). In such a case, the highest possible values for the model output Z_c are obtained with a *combination* of high values of *both* Q *and* Z_v (i.e., high values of the corresponding uncertain parameters α, β, μ_{Zv} and σ_{Zv}) *and* low values of *both* K_s *and* Z_m (i.e., low values of the corresponding uncertain parameters μ_{Ks}, σ_{Ks}, μ_{Zm} and σ_{Zm}); conversely, the lowest possible values for the model output Z_c are obtained with a combination of low values of both Q and Z_v and high values of both K_s and Z_m. These extreme situations (which give rise to the largest separation between the upper and lower cumulative distribution functions, i.e., to the most "epistemically" uncertain and, thus, conservative case), can be obtained only in case iiia above, i.e., assuming independence between the epistemically uncertain parameters. Actually, if a pure random sampling is performed among independent uncertain parameters, *all* possible *combinations* of values can be in principle generated, since the entire ranges of variability of the uncertain parameters can be explored independently: thus, in some random samples, high values of Q and Z_v may be combined by chance with low values of both K_s and Z_m, whereas in other random samples low values of both Q and Z_v may be combined by chance with high values of both K_s and Z_m. Conversely, such "extreme" situations cannot occur if there is total dependence between the uncertain parameters (i.e., case iiib above). Actually, in such a case high (low) values of both Q and Z_v can *only* be combined with high (low) values of both K_s and Z_m, giving rise to values of output Z_c which are lower (higher) than the highest (lowest) possible: in other words, the separation between the upper and lower cumulative distribution functions produced in case iiib is *always smaller* than that produced by the "extreme" situations described above (which are possible *only* in case iiia).

A final, straightforward remark is in order. The considerations made above about what combinations of parameter values would lead to the most conservative results (i.e., to the largest gap between the upper and lower cumulative distribution functions) are strictly dependent on the input–output relationship considered: obviously, a *different model* (with different functional relationships between inputs and outputs) would require *different combinations* of input values in order to obtain the most conservative results. For example, for the hypothetical model $w = (x * y)/z$ the most conservative results (i.e., the largest separation between the upper and lower cumulative distribution functions) would be obtained by imposing *total* dependence between x and y and *opposite* dependence between z and both x and y.

We now move onto compare i and ii. Fig. 7 shows the plausibility and belief functions of the model output Z_c produced by the MC-based DS-IRS method (case ii) and by the hybrid MC and possibilistic approach (case i).

The results are very similar because, in the present case, the effect of the different dependence relationships between the

Table 2
Comparisons performed between the different approaches, and their relative objectives.

		State of dependence between the epistemically uncertain parameters: Independence		Total dependence		Objective
Representation of epistemic uncertainty	Probabilistic	Two-level MC (iiia)	vs.	Two-level MC (iiib)	⇨	Study the effect of the state of dependence between the epistemically uncertain parameters of the aleatory probability distributions when a probabilistic/non-probabilistic representation of epistemic uncertainty is given
		vs.		vs.		
	Non-probabilistic	MC-based DS-IRS (ii)	vs.	Hybrid MC and possibilistic (i)	⇨	
		⇩		⇩		
	Objective	Study the effect of the probabilistic/non-probabilistic representation of the epistemically uncertain parameters of the aleatory probability distributions when the state of dependence between the epistemically uncertain parameters is given				

epistemically uncertain parameters is not evident. This may be explained as follows. In general, the closer the shape of the possibility distribution of a parameter is to that of a rectangle, defined over a given support, the higher the epistemic uncertainty associated to that parameter (actually, if a parameter is represented by a rectangular possibility distribution, the only information available about the parameter is the *interval* where it is defined, i.e., we are *totally ignorant* about its distribution). It can be easily seen that if the state of knowledge of many of the epistemically uncertain parameters is close to that of total ignorance, the state of dependence between them becomes negligible. By way of example, refer to the possibility distributions of the parameters μ_{Zm} (Fig. 8, left) and β (Fig. 8, right) described in Section 3.2. Selecting the same confidence level $\alpha = \alpha_1^{\mu_{Zm}} = \alpha_1^{\beta} = 0.5$ for the two variables (i.e., imposing total dependence between them) produces the same couple of α-cuts than selecting different levels $\alpha_1^{\mu_{Zm}} = 0.5 \neq \alpha_2^{\beta} = 0.1$. Notice that this holds for many other combinations of α values: for example, in this case all combinations with α^{β} ranging between 0 and 0.6 and $\alpha^{\mu_{Zm}}$ ranging between 0 and around 0.25 produce the same couple of α-cuts.

Since, in the present case study the shape of many of the possibility distributions are quite close to that of a rectangle (see Figs. 1–4), the state of dependence between the uncertain parameters scarcely affects the results.

A final consideration is in order with respect to the results obtained. The first comparison (Fig. 6) shows that in the present case study the two-level MC approach assuming dependence among parameters gives rise to a smaller separation between the cumulative distribution functions than the two-level MC approach assuming independence among parameters: in other words, it can be considered less conservative. The second comparison (Fig. 7) shows that the results obtained by the hybrid MC and possibilistic approach and the MC-based DS-IRS approach are very similar. Therefore, the state of dependence between the epistemically uncertain parameters of the aleatory probability distributions is more likely to become a critical factor (e.g., in risk-informed decisions) when the representation of the uncertain parameters is probabilistic.

4.2.2. Studying the effect of the probabilistic/non-probabilistic representation of the epistemically uncertain parameters of the aleatory probability distributions

In this Section, we perform comparisons between approaches ii and iiia and between approaches i and iiib above, i.e., approaches that represent epistemic uncertainty in radically different ways:

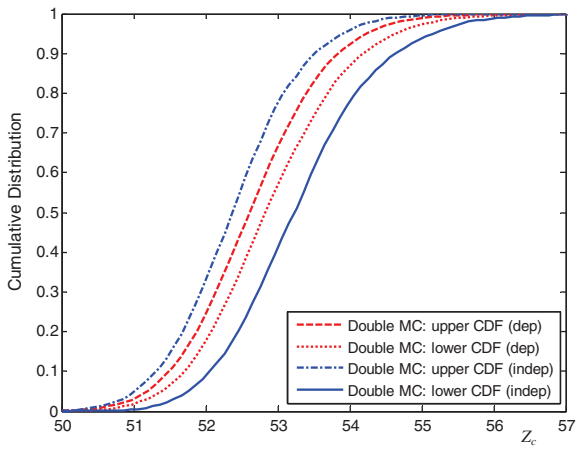


Fig. 6. Comparison of the upper and lower cumulative distribution functions of the maximal water level of the river Z_c obtained by the two-level Monte Carlo approach, considering both independence and total dependence between the epistemically uncertain parameters.

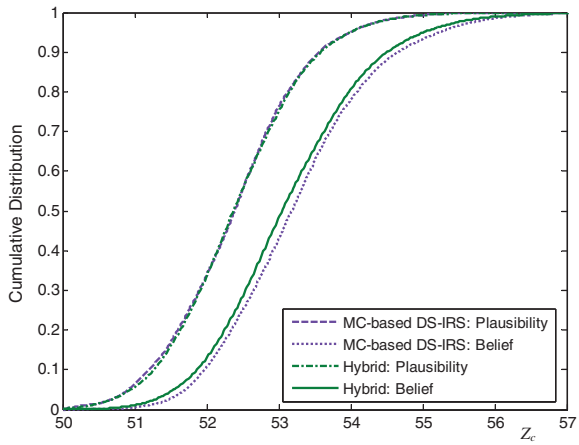


Fig. 7. Comparison of the cumulative distribution functions of the maximal water level of the river Z_c obtained by the Dempster–Shafer method and the hybrid method.

in particular, both in hybrid and in MC-based DS-IRS methods, possibility distributions are employed which identify a *family* of probability distributions for the epistemically uncertain parameters[5]; on the contrary, in the two-level MC approach, only a *single* probability distribution is assigned to represent the epistemic uncertainty associated to the parameters.

Fig. 9 shows the upper and lower cumulative distribution functions of the model output Z_c obtained by the two-level MC approach assuming independence between the uncertain parameters (case iiia) and the plausibility and belief functions produced by the MC-based DS-IRS approach (case ii).

The results are very similar, which is explained as follows. First of all, there is obviously a strong similarity between the shapes of the probability distributions of the epistemically uncertain parameters used in the two-level MC approach (case iiia) and the corresponding possibility distributions used in the MC-based DS-IRS approach (case ii).[6] For example, the ranges of variability of the uncertain parameters are the same for both the probability and the possibility distributions considered (see Sections 3.2.1,3.2.2,3.2.3); in addition, some of the possibility distributions employed in the MC-based DS-IRS approach (e.g., those of parameters α and β of the Gumbel distribution for Q) are obtained by simple normalization of the probability distributions employed in the two-level MC approach (Section 3.2.1); finally, the trapezoidal probability distribution used in the two-level MC approach for the Strickler friction coefficient K_s is also obtained by simple normalization of the trapezoidal possibility distribution proposed in the present paper and shown in Fig. 4 of Section 3.2.3.

In addition to the similarity between the probability and possibility distributions considered, the second motivation for the similarity between the results lies in the assumption of independence between the epistemically uncertain parameters and in the characteristics of the two algorithms used to propagate the uncertainties. In the two-level MC approach, a plain random sampling is performed from the probability distribution of the epistemically uncertain parameters, which are considered independent: as a consequence of this independence, in principle *all* possible *combinations* of values of the parameters can be sampled, since the entire ranges of variability of the parameters are explored *randomly* and *independently*. In the MC-based DS-IRS approach, the focal sets generated by the discretization of the possibility distributions are

[5] Remember that in the MC-based DS-IRS approach the possibility distributions are discretized into focal sets (Appendix B).

[6] As before, notice that this comparison is fair because both methods assume independence between the epistemically uncertain parameters.

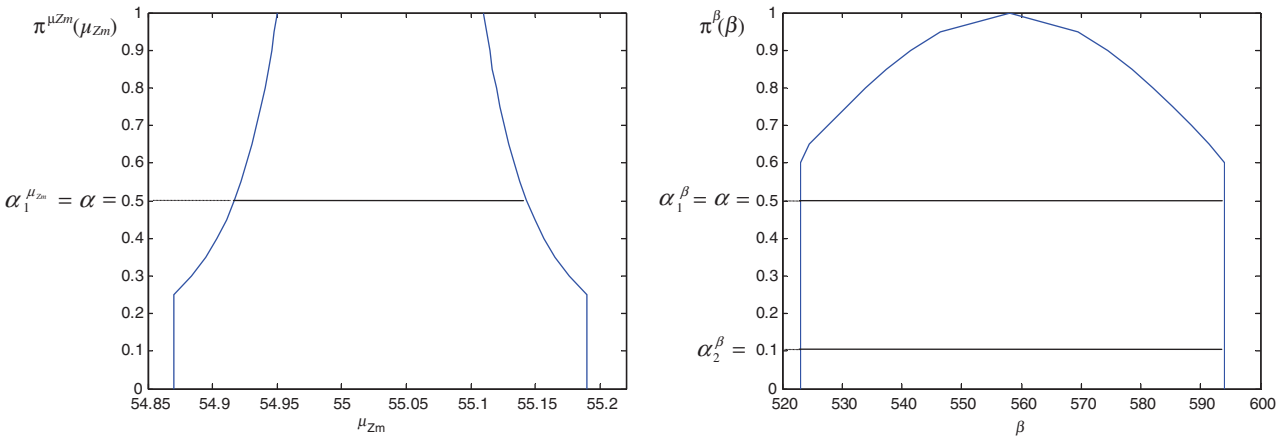


Fig. 8. Left: possibility distribution, $\pi^{\mu_{Zm}}(\mu_{Zm})$, of the parameter μ_{Zm} of the probability distribution of the variable Z_m (Section 3.2.2); right: possibility distribution, $\pi^{\beta}(\beta)$, of the parameter β of the probability distribution of the variable Q (Section 3.2.1).

selected *randomly* and *independently* by MC (step 2. of the procedure in Appendix B); in addition, all the focal sets selected are exhaustively searched to maximize/minimize the model output.

As a final comparison, Fig. 10 shows the upper and lower cumulative distribution functions of the model output Z_c obtained by the two-level MC approach assuming total dependence between parameters (case iiib) and the hybrid MC approach (case i) (which assumes total dependence between parameters).

From the consideration made above it is clear why the gap is smaller between the cumulative distributions in the two-level MC approach assuming total dependence between the uncertain parameters (case iiib) than between the plausibility and belief functions produced by the hybrid approach (case i).[7] Actually, in case iiib only a limited set of combinations of uncertain parameter values can be randomly explored, whereas in case i, the same confidence level α is chosen to build the α-cuts for all the possibility distributions of the uncertain parameters (step 3. of the procedure in Appendix A). Then, the minimum and maximum values of the model output Z_c are identified letting the uncertain parameters range *independently* within the corresponding α-cuts (step 3. of the procedure in Appendix A): thus, contrary to the case iiib, once a possibility level α is selected, *all* possible *combinations* of parameter values can be explored, since the α-cuts of all the parameters are *exhaustively* searched to maximize/minimize the model output Z_c (giving rise to a larger separation between the plausibility and belief functions).

A final remark is in order with respect to the results obtained. Since in this case the hybrid MC and possibilistic approach gives rise to a larger separation between the plausibility and belief functions than the two-level MC approach (assuming total dependence between the epistemically uncertain parameters), it can be considered *more conservative*. As a consequence, embracing one method instead of the other may significantly change the outcome of a decision making process in a risk assessment problem involving uncertainties: this is of paramount importance in systems that are critical from the safety view point, e.g., in the nuclear, aerospace, chemical and environmental fields. On the contrary, since the results obtained by the two-level MC approach (assuming independence among the epistemically uncertain parameters) and the MC-based DS-IRS are very similar, embracing one method instead of the other would not change significantly the final decision.

In conclusion, it is worth highlighting that when there is total dependence between the epistemically uncertain parameters, a probabilistic representation of epistemic uncertainty may fail to produce reliable and conservative results, which raises concerns from the point of view of safety. A quantitative demonstration of this statement is given in what follows.

The final goal of the uncertainty propagation is to determine (i) the dike level necessary to guarantee a given flood return period or (ii) the flood risk for a given dike level.

With respect to issue (i) above, the quantity of interest that is most relevant to the decision maker is the 99% quantile of Z_c, i.e., $Z_c^{0.99}$, taken as the annual maximal flood level. This corresponds to the level of a "centennial" flood, the yearly maximal water level with a 100 year-return period. With respect to issue (ii) above, the quantity of interest that is most relevant to the decision maker is the probability that the maximal water level of the river Z_c exceeds a given threshold z^*, i.e., $P(Z_c \geqslant z^*)$; in the present report, $z^* = 55.5$ m as in [3]. Table 3 reports the lower ($Z_{c,lower}^{0.99}$) and upper ($Z_{c,upper}^{0.99}$) 99th percentiles obtained from the two limiting cumulative distributions and the corresponding $LowerBound(Z_c \geqslant z^*)$ and $UpperBound(Z_c \geqslant z^*)$. In addition, as synthetic mathematical indicators of the imprecision in the knowledge of Z_c (i.e., of the separation between the lower and upper cumulative distribution functions), the following percentage widths have been reported:

- $W_{Zc} = \frac{Z_{c,upper}^{0.99} - Z_{c,lower}^{0.99}}{Z_{c,prob}^{0.99}}$ of the interval $[Z_{c,lower}^{0.99}, Z_{c,upper}^{0.99}]$ with respect to the percentile $Z_{c,prob}^{0.99}$ obtained by the pure probabilistic approach of Section 4.1;
- $W^* = \frac{UpperBound(Z_c \geqslant z^*) - LowerBound(Z_c \geqslant z^*)}{P(Z_c \geqslant z^*)_{prob}}$ of the interval $[LowerBound(Z_c \geqslant z^*), UpperBound(Z_c \geqslant z^*)]$ with respect to the percentile $Z_{c,prob}^{0.99}$ obtained by the pure probabilistic approach of Section 4.1.

The considerations previously reported are confirmed: there is a similarity between the values of the indicators relative to the hybrid MC and possibilistic approach (case i), to the MC-based DS-IRS approach (case ii) and to the two-level MC approach assuming independence among the uncertain parameters (case iiia); on the contrary, there is a significant difference between these indicators and those produced by the two-level MC approach assuming total dependence between the uncertain parameters (case iiib). In particular, as anticipated before, one consideration concerning the comparison between the hybrid approach and the two-level MC considering total dependence is worth to be done. Analyzing, for instance, the probability that the maximal water level of the river Z_c exceeds the threshold $z^* = 55.5$ m, $P[Z_c \geqslant z^* = 55.5]$, it can be seen that the hybrid approach is much more conservative than the two-level MC approach assuming total dependence between parameters: in fact, for instance, the upper bounds of $P[Z_c \geqslant z^*]$

[7] As before, notice that this comparison is fair because both methods assume total dependence between the epistemically uncertain parameters.

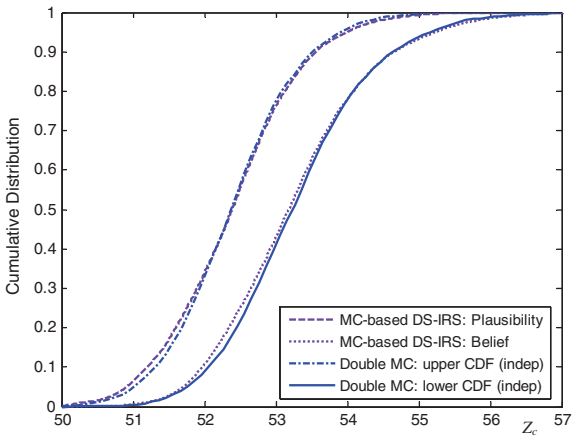


Fig. 9. Comparison of the cumulative distribution functions of the maximal water level of the river Z_c obtained by the Dempster–Shafer method and the two-level Monte Carlo method assuming independence between the epistemically uncertain parameters.

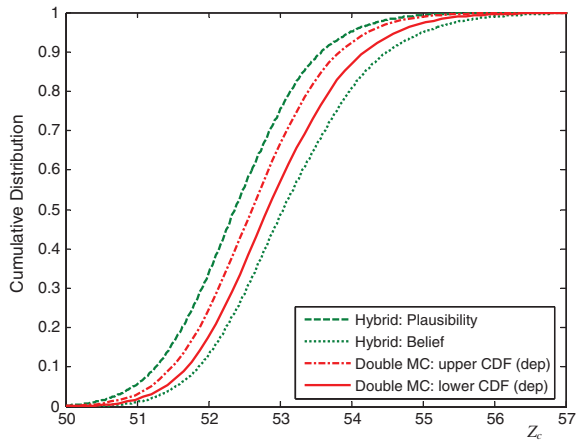


Fig. 10. Comparison of the cumulative distribution functions of the maximal water level of the river Z_c obtained by the hybrid method and the two-level Monte Carlo method assuming total dependence between the epistemically uncertain parameters.

are 0.0241 and 0.0111 for cases i and iib, respectively. Thus, in this case the use of the two-level MC approach would lead to underestimating by about 54% the probability that the maximal water level of the river Z_c exceeds the threshold $z^* = 55.5$ m: in other words, it would lead to underestimating by about 54% the "failure probability" of the dike and, at the same time, the flood risk. The same consideration holds for the dike level necessary to guarantee a 100 year-return period represented by the 99% quantile $Z_c^{0.99}$ of the water level of the river; for example, the upper bounds of $Z_c^{0.99}$ are 56.03 m and 55.50 m for cases i and iib, respectively. Thus, also in this case the use of the two-level MC approach would lead to a slight underestimation of the dike level necessary to guarantee a 100 year flood return period. Therefore, even if the two-level MC approach purposely tries to separate variability from imprecision, differently from the hybrid approach, it treats lack-of-knowledge in the same way as it treats variability (i.e., using probability distributions): as a consequence, in some cases, it may fail to produce reliable and conservative results, which can raise great concerns from the safety point of view: in particular, in the present case study, the two-level MC approach leads to less conservative results when total dependence between the epistemically uncertain parameters is assumed. This leads to conclude also that when the state of dependence between the parameters is *not known* to the analyst (which is far from unlikely in practice), a non-probabilistic representation of epistemic uncertainty may represent the "safest" choice.

5. Discussion of the results

The analyses performed in the previous Section 4 can be summarized as follows:

1. a comparison between the hybrid method and the one-level pure probabilistic approach, highlighting that:
   - the hybrid method explicitly propagates the uncertainty by separating the contributions coming from the aleatory and epistemic variables;
   - the uncertainty in the output distribution of the pure probabilistic approach is given *only* by the *slope* of the cumulative distribution;
   - as expected, the cumulative distribution of the model output obtained by the pure probabilistic method is within the belief and plausibility functions obtained by the hybrid approach;
2. comparisons between the hybrid, MC-based DS-IRS and two-level MC approaches with the following objectives:
   a. the study of the *effect of dependence* between the epistemically uncertain parameters of the aleatory probability distributions when a probabilistic/non-probabilistic *representation* of epistemic uncertainty is *adopted*:
      - the comparison between two-level MC approaches assuming total dependence and independence between the parameters, respectively, has shown that in the case study considered assuming dependence between the parameters leads to a smaller gap between the upper and lower cumulative distributions of the model output, i.e., to less conservative results;
      - the comparison between the MC-based DS-IRS and hybrid approaches has shown that the plausibility and belief functions produced by the two approaches are similar: in other words, the hybrid method is not significantly influenced by the total dependence between the epistemically uncertain parameters, due to the large uncertainty that is associated to the parameters in the case study considered.

   Based on the considerations above, it can be argued that the state of dependence between the epistemically uncertain parameters of the aleatory probability distributions is more likely to become a *critical factor* (e.g., in risk-informed decisions) when the representation of the uncertain parameters is *probabilistic*.

   b. the study of the *effect* of the probabilistic/non-probabilistic *representation* of epistemic uncertainty when the *state of dependence* between parameters is *defined*:
      - the comparison between the MC-based DS-IRS approach and the two-level MC approach assuming independence between the epistemically uncertain parameters has shown that in the case study considered the upper and lower cumulative distribution functions of the model output produced by the two approaches are similar. This is due to i) the strong similarity between the shapes of the possibility and probability distributions of the epistemically uncertain parameters used in the MC-based DS-IRS and two-level MC approaches, respectively, ii) the independence between the parameters and iii) the similar characteristics of the two algorithms used to propagate the uncertainties;
      - the comparison between the hybrid and the two-level MC approach assuming total dependence between the parameters has shown that the gap between the plausibility and belief functions of the model output produced by the hybrid approach is larger than the gap between

Table 3
Comparison of the lower and upper values of Z_c percentiles and threshold exceedance probability obtained by the three methods analyzed; the respective percentage widths W of the intervals are also reported. All values are in meters.

Method	$Z_c^{0.99}$ (pure probabilistic value = 55.34)		$P[Z_c \geqslant 55.5]$ (pure probabilistic value = 0.0076)	
	$[Z_{c,lower}^{0.99}, Z_{c,upper}^{0.99}]$	W_{Zc} [%]	[LowerBound, UpperBound]	W^* [%]
Hybrid MC and possibilistic (total dependence) (case i)	[54.79, 56.03]	2.2	[0.0024, 0.0241]	286
MC-based DS-IRS (independence) (case ii)	[54.82, 56.23]	2.6	[0.0014, 0.0335]	423
Two-level MC (independence) (case iiia)	[54.56, 56.06]	2.7	[0.0013, 0.0293]	368
Two-level MC (total dependence) (case iiib)	[54.05, 55.50]	0.8	[0.0042, 0.0111]	91

the upper and lower cumulative distribution functions produced by the two-level MC method. This is due to both the different representations of epistemic uncertainties and to the characteristics of the two algorithms used to propagate the uncertainties. Actually, in the hybrid method the epistemic uncertainty on the parameters is represented by possibility distributions defining a *family* of probability distributions; on the contrary, in the two-level MC approach only a *single* probability distribution is selected to represent the epistemic uncertainty on a parameter. As a result, the two algorithms propagate the uncertainty differently: in the hybrid method, an *exhaustive* interval analysis is performed for different α-cuts of the possibility distributions, whereas in the two-level MC method a plain *random* sampling is performed from the probability distribution of the uncertain parameters: the result is that the hybrid approach is able to explore a larger set of combinations of uncertain parameter values than the two-level MC approach (assuming dependence among parameters), thus producing more conservative results. This has been quantitatively confirmed by way of the risk model for the design of a flood protection dike through the computation of i) the dike level necessary to guarantee a 100 year flood return period and ii) the flood risk for a given dike level. In fact, both quantities have been underestimated by the two-level MC approach with respect to the hybrid approach.

Based on the considerations above, it can be argued that a probabilistic representation of the epistemically uncertain parameters of the aleatory probability distributions may *fail* to

Table 4
Comparisons performed between the different approaches, and their relative findings.

	Independence	State of dependence between the epistemically uncertain parameters			Findings	
			Total dependence			
Representation of epistemic uncertainty	Probabilistic	Two-level MC (iiia) vs.	vs.	Two-level MC (iiib) vs.	➔	*Method (iiia) vs. (iiib):* –In the case study considered, assuming dependence between the parameters leads to a *smaller* gap between the upper and lower CDFs of the model output, i.e., to *less conservative* results
	Non-probabilistic	MC-based DS-IRS (ii)	vs.	Hybrid MC and possibilistic (i)	➔	*Method (i) vs. (ii):* –The plausibility and belief functions produced by the two approaches are *similar*: in other words, the hybrid method is *not significantly influenced* by the total dependence between the epistemically uncertain parameters
						General: –The state of dependence between the epistemically uncertain parameters of the aleatory probability distributions is more likely to become a *critical factor* (e.g., in risk-informed decisions) when the representation of the uncertain parameters is *probabilistic*
	Findings	➓ *Method (ii) vs. (iiia):* –In the cases study considered, the upper and lower CDFs of the model output produced by the two approaches are *similar*		➓ *Method (i) vs. (iiib):* The gap between the plausibility and belief functions of the model output produced by the hybrid approach is *larger* than the gap between the upper and lower CDFs produced by the two-level MC method		
		General: A probabilistic representation of the epistemically uncertain parameters of the aleatory probability distributions may *fail* to produce reliable and *conservative* results when there is *total dependence* between the uncertain parameters, which raises concerns from the point of view of safety				

produce *reliable* and *conservative* results when there is *total dependence* between the uncertain parameters, which raises concerns from the point of view of safety.

The findings gained by the comparisons performed in Section 4 are summarized in Table 4 for the sake of clarity.

6. Conclusions

In the present paper, we performed the joint hierarchical propagation of hybrid probabilistic and possibilistic uncertainty representations onto a flood risk-based design model in a "two-level" framework. The results obtained have been compared with those produced by a one-level pure probabilistic approach, a MC-based DS-IRS approach and a two-level (double loop) MC approach with the objective of studying the effects of (i) (*in*)*dependence* between the epistemically uncertain parameters of the aleatory probability distributions and (ii) *probabilistic/non-probabilistic representations* of epistemic uncertainty. To the best of the authors' knowledge, this is the first time that the above mentioned methods are systematically compared with reference to risk assessment problems where hybrid uncertainty is separated into two hierarchical levels.

The findings of the work show that adopting different methods for jointly propagating hybrid uncertainties may generate different results and possibly different decisions in risk problems involving uncertainties: this is of paramount importance in systems that are critical from the safety viewpoint, e.g., in the nuclear, aerospace, chemical and environmental fields.

In particular, it seems advisable to suggest that, if nothing is known about the dependence relationship between the epistemically uncertain parameters, one should resort to the hybrid MC and possibilistic approach or to the MC-based DS-IRS approach because their risk estimates are more conservative than (or at least comparable to) those obtained by the two-level MC approach assuming dependence (or independence) between the epistemically uncertain parameters: thus, a non-probabilistic representation of epistemic uncertainty represents in general a "safer" choice than a probabilistic one.

Appendix A. Operative procedure for the propagation of aleatory and epistemic uncertainty in the hybrid MC and possibilistic approach

The operative steps for the propagation of hybrid probabilistic and possibilistic uncertainty in a "two-level" framework are the following:

1. sample a matrix $\{u_j^i\}$, $i = 1,2,\ldots,m$, $j = 1,2,\ldots,k$, of random numbers from a uniform distribution $U[0,1)$;
2. set $\alpha = 0$ (outer loop processing epistemic uncertainty);
3. select the α-cuts $A_\alpha^{\theta_{j,1}}, A_\alpha^{\theta_{j,2}}, \ldots, A_\alpha^{\theta_{j,m_j}}$ of the possibility distributions $\boldsymbol{\pi}^{\theta_j}(\boldsymbol{\theta}_j) = \{\pi^{\theta_{j,1}}(\theta_{j,1}), \pi^{\theta_{j,2}}(\theta_{j,2}), \ldots, \pi^{\theta_{j,m_j}}(\theta_{j,m_j})\}$ of the parameters $\boldsymbol{\theta}_j = \{\theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j}\}$, of the "probabilistic" variables $Y_1, Y_2, \ldots, Y_j, \ldots, Y_k$, and the α-cuts $A_\alpha^{k+1}, A_\alpha^{k+2}, \ldots, A_\alpha^{n}$ of the possibility distributions $\{\pi^{Y_{k+1}}(y_{k+1}), \pi^{Y_{k+2}}(y_{k+2}), \ldots, \pi^{Y_l}(y_l), \ldots, \pi^{Y_n}(y_n)\}$ of the "purely possibilistic" variables, $Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n$, as intervals of possible values $[\underline{\boldsymbol{\theta}}_{j,\alpha}, \bar{\boldsymbol{\theta}}_{j,\alpha}] = \{[\underline{\theta}_{j,1,\alpha}, \bar{\theta}_{j,1,\alpha}], [\underline{\theta}_{j,2,\alpha}, \bar{\theta}_{j,2,\alpha}], \ldots, [\underline{\theta}_{j,m_j,\alpha}, \bar{\theta}_{j,m_j,\alpha}]\}$, $j = 1,2,\ldots,k$, and $[\underline{y}_{l,\alpha}, \bar{y}_{l,\alpha}]$, $l = k+1, k+2, \ldots, n$, respectively;
4. set $i = 1$ (inner loop processing aleatory uncertainty);
5. sample the i-th random intervals $[\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]$, $j = 1,2,\ldots,k$, of the "probabilistic" variables Y_j, $j = 1,2,\ldots,k$, corresponding to the α-cuts $[\underline{\boldsymbol{\theta}}_{j,\alpha}, \bar{\boldsymbol{\theta}}_{j,\alpha}] = \{[\underline{\theta}_{j,1,\alpha}, \bar{\theta}_{j,1,\alpha}], [\underline{\theta}_{j,2,\alpha}, \bar{\theta}_{j,2,\alpha}], \ldots, [\underline{\theta}_{j,m_j,\alpha}, \bar{\theta}_{j,m_j,\alpha}]\}$ (found at step 3. above) and to the i-th random vector $\{u_1^i, u_2^i, \ldots, u_j^i, \ldots, u_k^i\}$ (generated at step 1. above). In particular, the i-th random interval $[\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]$ for Y_j, $j = 1,2,\ldots,k$, is calculated by $\underline{y}_{j,\alpha}^i = \inf_{\boldsymbol{\theta}_j \in [\underline{\boldsymbol{\theta}}_{j,\alpha}, \bar{\boldsymbol{\theta}}_{j,\alpha}]} F_{Y_j}^{-1}(u_j^i|\boldsymbol{\theta}_j)$ and $\bar{y}_{j,\alpha}^i = \sup_{\boldsymbol{\theta}_j \in [\underline{\boldsymbol{\theta}}_{j,\alpha}, \bar{\boldsymbol{\theta}}_{j,\alpha}]} F_{Y_j}^{-1}(u_j^i|\boldsymbol{\theta}_j)$, where $F_{Y_j}^{-1}(\cdot|\boldsymbol{\theta}_j)$ is the inverse of the cumulative distribution function (*cdf*) $F_{Y_j}(\cdot|\boldsymbol{\theta}_j)$ of $p_{Y_j}(\cdot|\boldsymbol{\theta}_j)$; by way of example, Fig. A.1 shows the procedure for sampling the i-th random interval $[\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]$ for the generic uncertain variable Y_j.
6. calculate the smallest and largest values of $f(Y_1, Y_2, \ldots, Y_j, \ldots, Y_k, Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n)$, denoted by $\underline{f}_\alpha^i$ and $\bar{f}_\alpha^i$ respectively, letting variables Y_j range within the intervals $[\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]$, $j = 1,2,\ldots,k$, and letting variables Y_l, $l = k+1, k+2, \ldots, n$ range within $[\underline{y}_{l,\alpha}, \bar{y}_{l,\alpha}]$, $l = k+1, k+2, \ldots, n$; in particular, $\underline{f}_\alpha^i = \inf_{j, Y_j \in [\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]; l, Y_l \in [\underline{y}_{l,\alpha}, \bar{y}_{l,\alpha}]} f(Y_1, Y_2, \ldots, Y_j, \ldots, Y_k, Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n)$ and $\bar{f}_\alpha^i = \sup_{j, Y_j \in [\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]; l, Y_l \in [\underline{y}_{l,\alpha}, \bar{y}_{l,\alpha}]} f(Y_1, Y_2, \ldots, Y_j, \ldots, Y_k, Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n)$.
7. take the values $\underline{f}_\alpha^i$ and $\bar{f}_\alpha^i$ found in 6. above as the lower and upper limits of the α-cut of $f(Y_1, Y_2, \ldots, Y_j, \ldots, Y_k, Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n)$ in correspondence of the i-th random realization of the aleatory uncertainty;
8. if $i \neq m$, then set $i = i + 1$ and return to step 5. above; otherwise go to step 9. below;
9. if $\alpha \neq 1$, then set $\alpha = \alpha + \Delta\alpha$ (e.g., $\Delta\alpha = 0.05$) and return to step 3. above; otherwise, stop the algorithm: the fuzzy random realization (fuzzy interval) π_i^f, $i = 1,2,\ldots,m$ of $Z = f(Y_1, Y_2, \ldots, Y_n)$ is constructed as the collection of the values $\underline{f}_\alpha^i$ and $\bar{f}_\alpha^i$, $i = 1,2,\ldots,m$, found at step 6. above (in other words, π_i^f is defined by all its α-cut intervals $[\underline{f}_\alpha^i, \bar{f}_\alpha^i]$).

It is worth noting that performing an interval analysis on α-cuts assumes total dependence between the epistemically uncertain variables. Actually, this procedure implies strong dependence between the information sources (e.g., the experts or observers) that supply the input possibility distributions, because the same confidence level α is chosen to build the α-cuts for all the epistemically uncertain variables [15].

Finally, by way of example and only for illustration purposes, in Fig. A.1 the procedure for sampling the i-th random interval $[\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]$ for the generic uncertain variable Y_j is shown. Let us suppose that the probability distribution of Y_j is normal with parameters $\boldsymbol{\theta}_j = \{\theta_{j,1}, \theta_{j,2}\} = \{\mu, \sigma\}$; the mean $\mu = \theta_{j,1}$ is represented by a triangular possibility distribution with core $c = 5$ and support $[a,b] = [4,6]$ and the standard deviation $\sigma = \theta_{j,2}$ is a fixed point-wise value ($\sigma = \theta_{j,2} = 4$). With reference to the operative procedure outlined above, a possibility value α (e.g., $\alpha = 0.3$ in Fig. A.1, left) is selected and the corresponding α-cut for $\mu = \theta_{j,1}$ is found, i.e., $[\underline{\mu}_\alpha, \bar{\mu}_\alpha] = [\underline{\theta}_{j,1,\alpha}, \bar{\theta}_{j,1,\alpha}] = [4.3, 5.7]$ (see step 3. of the procedure above). The cumulative distribution functions $F_{\theta_j}^{Y_j}$ are constructed using the upper and lower values of μ, i.e., $\underline{\mu}_\alpha = \underline{\theta}_{j,1,\alpha} = 4.3$ and $\bar{\mu}_\alpha = \bar{\theta}_{j,1,\alpha} = 5.7$ (Fig. A.1, right); then, a random number u_j^i (e.g., $u_j^i = 0.7$ in Fig. A.1, right) is sampled from a uniform distribution in [0,1) and the interval $[\underline{y}_{j,\alpha}^i, \bar{y}_{j,\alpha}^i]$ is computed as $[\inf_{\boldsymbol{\theta}_j \in [\underline{\boldsymbol{\theta}}_{j,\alpha}, \bar{\boldsymbol{\theta}}_{j,\alpha}]} F_{Y_j}^{-1}(u_j^i|\boldsymbol{\theta}_j), \sup_{\boldsymbol{\theta}_j \in [\underline{\boldsymbol{\theta}}_{j,\alpha}, \bar{\boldsymbol{\theta}}_{j,\alpha}]} F_{Y_j}^{-1}(u_j^i|\boldsymbol{\theta}_j)] = [\inf_{\mu \in [\underline{\mu}_\alpha, \bar{\mu}_\alpha]} F_{Y_j}^{-1}(u_j^i|\mu), \sup_{\mu \in [\underline{\mu}_\alpha, \bar{\mu}_\alpha]} F_{Y_j}^{-1}(u_j^i|\mu)] = [\inf_{\mu \in [4.3, 5.7]} F_{Y_j} -1(0.7|\mu), \sup_{\mu \in [4.3, 5.7]} F_{Y_j}^{-1}(0.7|\mu)] = [6.4, 7.8]$ (see step 5. of the procedure above).

Appendix B. Operative procedure for the propagation of aleatory and epistemic uncertainty in the Monte Carlo-based Dempster–Shafer approach employing independent random sets

In the MC-based DS-IRS approach, the possibility distributions employed in the hybrid MC and possibilistic method (Appendix A) are encoded into discrete (focal) sets as follows:

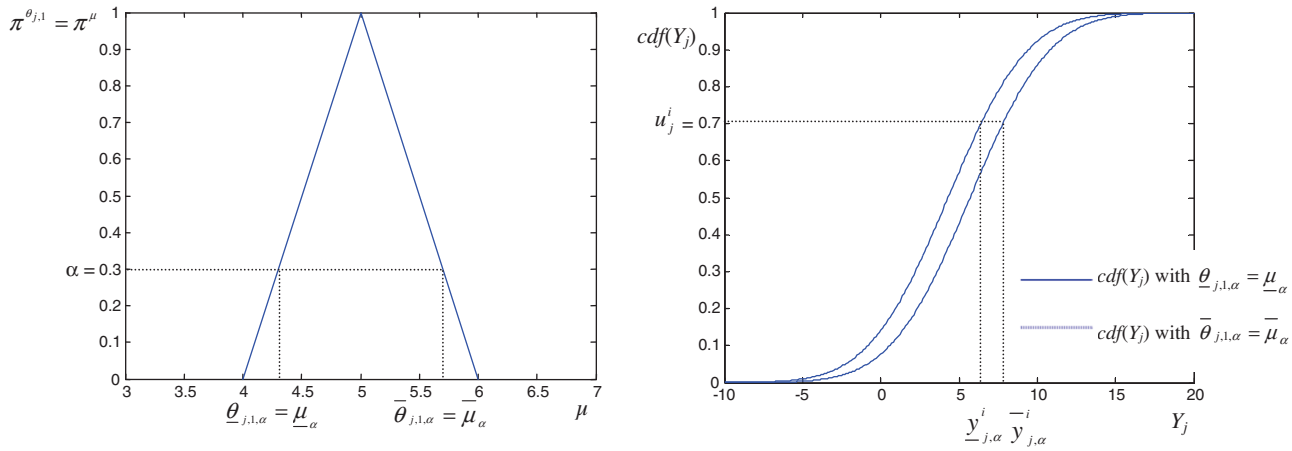


Fig. A.1. Left: triangular possibility distribution of the mean μ of the normal probability distribution of $Y_j \sim N(\mu, 4) = N(\theta)$; in evidence the α-cut of level $\alpha = 0.3[\underline{\theta}_{j,1,\alpha}, \overline{\theta}_{j,1,\alpha}] = [\underline{\mu}_{\alpha}, \overline{\mu}_{\alpha}] = [4.3, 5.7]$. Right: cumulative distribution functions of Y_j built in correspondence of the extreme values $\underline{\mu}_{\alpha} = 4.3$ and $\overline{\mu}_{\alpha} = 5.7$ of the α-cut $[\underline{\mu}_{\alpha}, \overline{\mu}_{\alpha}]$ of μ. The random interval $[\underline{y}_{j,\alpha}^i, \overline{y}_{j,\alpha}^i]$ (corresponding to the uniform random number $u_j^i = 0.7$) is found using the inverse transform method.

i. determine q (nested) focal sets for the generic possibilistic variable/parameter Y as the α-cuts $A_{\alpha_t} = [\underline{y}_{\alpha_t}, \overline{y}_{\alpha_t}]$, $t = 1, 2, \ldots, q$, with $\alpha_1 = 1 > \alpha_2 > \cdots > \alpha_q > \alpha_{q+1} = 0$;
ii. build the mass distribution of the focal sets by assigning $m_{\alpha_t} = \Delta\alpha_t = \alpha_t - \alpha_{t+1}$.

In particular, in the case study of the work presented in this paper, $q = 20$ and $m_{\alpha_t} = \Delta\alpha_t = \Delta\alpha = 0.05$, for the sake of comparison with the hybrid MC and possibilistic approach described in Section 2 and Appendix A and applied in Section 4.

The operative steps for the propagation of aleatory and epistemic uncertainty in a "two-level" framework according to the MC-based DS-IRS approach are the following[8]:

1. set $i_\alpha = 1$ (outer loop processing epistemic uncertainty);
2. sample the values $\{\alpha_{j,i_p}^{i_\alpha}\}$, $j = 1, 2, \ldots, k$, $i_p = 1, 2, \ldots, m_j$, from the discrete distribution $\{(\alpha_{j,i_p,t}, m_{\alpha_{j,i_p,t}}) : t = 1, 2, \ldots, q = 20\} = \{(\alpha_{j,i_p,1}, m_{\alpha_{j,i_p,1}}), (\alpha_{j,i_p,2}, m_{\alpha_{j,i_p,2}}), \ldots, (\alpha_{j,i_p,q=20}, m_{\alpha_{j,i_p,q=20}})\} = \{(1, 0.05), (0.95, 0.05), \ldots, (0, 0.05)\}$; these sampled values represent the α levels of the focal sets of the discretized possibility distributions $\boldsymbol{\pi}^{\boldsymbol{\theta}_j}(\boldsymbol{\theta}_j) = \{\pi^{\theta_{j,1}}(\theta_{j,1}), \pi^{\theta_{j,2}}(\theta_{j,2}), \ldots, \pi^{\theta_{j,m_j}}(\theta_{j,m_j})\}$ of the parameters $\boldsymbol{\theta}_j = \{\theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j}\}$ of the "probabilistic" variables $Y_1, Y_2, \ldots, Y_j, \ldots, Y_k$. Then sample the values $\{\alpha_l^{i_\alpha}\}$, $l = k+1, k+2, \ldots, n$, from the discrete distribution $\{(\alpha_{l,t}, m_{\alpha_{l,t}}) : t = 1, 2, \ldots, q = 20\} = \{(\alpha_{l,1}, m_{\alpha_{l,1}}), (\alpha_{l,2}, m_{\alpha_{l,2}}), \ldots, (\alpha_{l,q=20}, m_{\alpha_{l,q=20}})\} = \{(1, 0.05), (0.95, 0.05), \ldots, (0, 0.05)\}$; these sampled values represent the α levels of the focal sets of the discretized possibility distributions $\pi^{Y_{k+1}}(y_{k+1}), \pi^{Y_{k+2}}(y_{k+2}), \ldots, \pi^{Y_l}(y_l), \ldots, \pi^{Y_n}(y_n)$ of the "purely possibilistic" variables, $Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n$. Notice that, differently from the hybrid MC and possibilistic approach (Appendix A), a different value α is *randomly* and *independently* sampled for each epistemically uncertain parameter/variable, i.e., *independence* is assumed between the epistemically uncertain parameters/variables;
3. on the basis of the α levels sampled at step 2., select the random focal sets $A_{\alpha_{j,1}^{i_\alpha}}^{\theta_{j,1}}, A_{\alpha_{j,2}^{i_\alpha}}^{\theta_{j,2}}, \ldots, A_{\alpha_{j,m_j}^{i_\alpha}}^{\theta_{j,m_j}}$, $j = 1, 2, \ldots, k$, for the parameters $\boldsymbol{\theta}_j = \{\theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j}\}$ and the random focal sets $A_{\alpha_{k+1}^{i_\alpha}}^{k+1}, A_{\alpha_{k+2}^{i_\alpha}}^{k+2}, \ldots, A_{\alpha_n^{i_\alpha}}^{n}$ for the "purely possibilistic" variables $Y_{k+1}, Y_{k+2}, \ldots, Y_l, \ldots, Y_n$, as intervals of possible values $[\underline{\boldsymbol{\theta}}_{j,\alpha_{j,i_p}^{i_\alpha}}, \overline{\boldsymbol{\theta}}_{j,\alpha_{j,i_p}^{i_\alpha}}] = \{[\underline{\theta}_{j,1,\alpha_{j,1}^{i_\alpha}}, \overline{\theta}_{j,1,\alpha_{j,1}^{i_\alpha}}], [\underline{\theta}_{j,2,\alpha_{j,2}^{i_\alpha}}, \overline{\theta}_{j,2,\alpha_{j,2}^{i_\alpha}}], \ldots, [\underline{\theta}_{j,m_j,\alpha_{j,m_j}^{i_\alpha}}, \overline{\theta}_{j,m_j,\alpha_{j,m_j}^{i_\alpha}}]\}$, $j = 1, 2, \ldots, k$, and $[\underline{y}_{l,\alpha_l^{i_\alpha}}, \overline{y}_{l,\alpha_l^{i_\alpha}}]$, $l = k+1, k+2, \ldots, n$, respectively;
4. perform the same steps 4.–8. (inner loop processing aleatory uncertainty) as in the procedure of Appendix A to obtain $\underline{f}^{i,i_\alpha}$ and $\overline{f}^{i,i_\alpha}$, $i = 1, 2, \ldots, m$, $i_\alpha = 1, 2, \ldots, m_\alpha$, as the upper and lower limit of $f(Y_1, Y_2, \ldots, Y_n)$ in correspondence of the i-th random realization of the aleatory uncertainty and of the i_α-th random realization of epistemic uncertainty;
5. if $i_\alpha \neq m_\alpha$, then set $i_\alpha = i_\alpha + 1$ and return to step 2.; otherwise, stop the algorithm: the random sets $E^{i,i_\alpha} = [\underline{f}^{i,i_\alpha}, \overline{f}^{i,i_\alpha}]$, $i = 1, 2, \ldots, m$, $i_\alpha = 1, 2, \ldots, m_\alpha$, of $Z = f(Y_1, Y_2, \ldots, Y_n)$ are obtained with the collection of the values $\underline{f}^{i,i_\alpha}$ and $\overline{f}^{i,i_\alpha}$, $i = 1, 2, \ldots, m$, $i_\alpha = 1, 2, \ldots, m_\alpha$, found at step 5. above. A probability mass $m(E^{i,i_\alpha}) = \frac{1}{m_\alpha * m}$, is associated at each random set E^{i,i_α}.

For each set A contained in the universe of discourse U_Z of the output variable Z, it is possible to obtain the belief $Bel(A)$ and the plausibility $Pl(A)$ for any set A, respectively [14,15]:

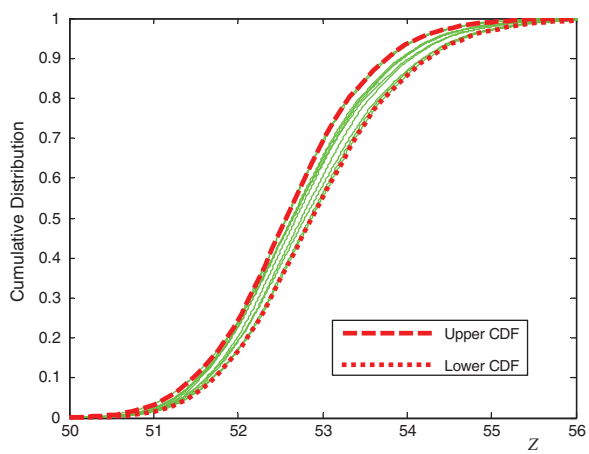


Fig. C.1. $m_p = 10$ cumulative distribution functions $\widehat{F}_{i_p}^{Z}$, $i_p = 1, 2, \ldots, m_p$, (solid lines) produced by a two-level MC approach together with the corresponding upper and lower empirical cumulative distribution functions (dashed lines).

[8] The reader is referred to Section 2 and Appendix A for the notation used.

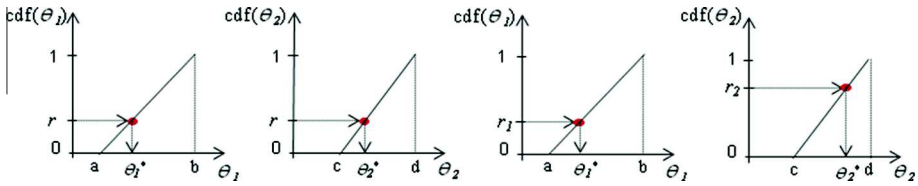


Fig. C.2. Left: random sampling of realizations of the uncertain parameters θ_1 and θ_2 assuming total dependence; right: random sampling of realizations of the uncertain parameters θ_1 and θ_2 assuming independence.

$$Bel(A) = \sum_{E^{i,i_\alpha} \subseteq A} m(E^{i,i_\alpha}), \tag{B.1}$$

$$Pl(A) = \sum_{E^{i,i_\alpha} \cap A \neq 0} m(E^{i,i_\alpha}). \tag{B.2}$$

Appendix C. Two-level Monte Carlo method

Let us consider a model whose output is a function $Z = f(Y_1, Y_2, \ldots, Y_j, \ldots, Y_n)$ of n uncertain variables Y_j, $j = 1,2,\ldots,n$, that are "probabilistic", i.e., their uncertainty is described by probability distributions $p_{Y_1}(y_1|\boldsymbol{\theta}_1), p_{Y_2}(y_2|\boldsymbol{\theta}_2), \ldots, p_{Y_j}(y_j|\boldsymbol{\theta}_j), \ldots, p_{Y_k}(y_k|\boldsymbol{\theta}_k)$ with parameters $\boldsymbol{\theta}_j = \{\theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j}\}$, $j = 1,2,\ldots,n$; the parameters $\{\boldsymbol{\theta}_j{:}j = 1,2,\ldots,n\}$ are themselves described by probability distributions $\boldsymbol{p}^{\boldsymbol{\theta}_j}(\boldsymbol{\theta}_j) = \{p^{\theta_{j,1}}(\theta_{j,1}), p^{\theta_{j,2}}(\theta_{j,2}), \ldots, p^{\theta_{j,m_j}}(\theta_{j,m_j})\}$. By way of example, let $Y \sim N(\mu,\sigma) = N(\boldsymbol{\theta}) = N\ (\theta_1,\theta_2)$ and the parameters $\boldsymbol{\theta} = \{\theta_1, \theta_2\} = \{\mu,\sigma\}$ have a normal distribution with known mean and variance, i.e., $\theta_1 = \mu \sim N(\mu_\mu, \sigma_\mu)$ and $\theta_2 = \sigma \sim N(\mu_\sigma, \sigma_\sigma)$.[9]

In such a case, the propagation of uncertainty can be performed by a two-level Monte Carlo (MC) technique, which is constituted by the following two main steps [2,4]:

i. MC sampling of the parameters affected by epistemic uncertainty (outer loop processing epistemic uncertainty);
ii. repeated MC sampling of possible values of the "probabilistic" variables from the corresponding probability distributions conditioned at the values of the epistemically uncertain parameters sampled at step i above (inner loop processing aleatory uncertainty).

In more detail, the operative steps of the procedure are:

1. set $i_p = 1$ (outer loop processing epistemic uncertainty);
2. sample a vector $\{r_k^{i_p}\}$, $k = 1,2,\ldots,n_p$ of uniform random numbers in $[0,1)$ (n_p is the total number of epistemically uncertain parameters, i.e., $n_p = \sum_{j=1}^{n} m_j$);
3. identify the i_p-th set of random realizations $\theta_k^{i_p}$, $k = 1,2,\ldots,n_p$, of the epistemically uncertain parameters θ_k, $k = 1,2,\ldots,n_p$, using the random vector $\{r_1^{i_p}, r_2^{i_p}, \ldots, r_k^{i_p}, \ldots, r_{n_p}^{i_p}\}$ sampled at step 2. above. In particular, the value $\theta_k^{i_p}$ is calculated by $\theta_k^{i_p} = [F^{\theta_k}]^{-1}(r_k^{i_p})$, $k = 1,2,\ldots,n_p$, where $[F^{\theta_k}]^{-1}$ is the inverse of the cumulative distribution F^{θ_k} of p^{θ_k};
4. set $i = 1$ (inner loop processing aleatory uncertainty);
5. sample a vector $\{u_j^i\}$, $j = 1,2,\ldots,n$, of uniform random numbers in $[0,1)$;
6. identify the i-th set of random realizations y_j^{i,i_p}, $j = 1,2,\ldots,n$, of the "probabilistic" variables Y_j, $j = 1,2,\ldots,n$, using the random vector $\{u_1^i, u_2^i, \ldots, u_j^i, \ldots, u_n^i\}$ sampled at step 5. above and the random realizations $\theta_k^{i_p}$, $k = 1,2,\ldots,n_p$, of the epistemically uncertain parameters sampled at step 3. above. In particular, the value y_j^{i,i_p} is calculated by $y_j^{i,i_p} = F_{Y_j}^{-1}(u_j^i|\theta_k^{i_p})$, $j = 1,2,\ldots,n$ where $F_{Y_j}^{-1}(\cdot|\theta_k^{i_p})$ is the inverse of the cumulative distribution $F_{Y_j}(\cdot|\theta_k^{i_p})$ of $p_{Y_j}(\cdot|\theta_k^{i_p})$ (notice that $p_{Y_j}(\cdot|\theta_k^{i_p})$ is the probability distribution of Y_j conditioned at the values $\theta_k^{i_p}$, $k = 1,2,\ldots,n_p$, of the epistemically uncertain parameters θ_k, $k = 1,2,\ldots,n_p$, sampled at step 3. above;
7. calculate the value z^{i,i_p} of the model output Z as $z^{i,i_p} = f(y_1^{i,i_p}, y_2^{i,i_p}, \ldots, y_j^{i,i_p}, \ldots, y_n^{i,i_p})$;
8. if $i \neq m$, then set $i = i + 1$ and return to step 5.; otherwise, build the empirical cumulative distribution function $\widehat{F}_{i_p}^Z$ for Z using the m values of $z^{i,i_p} = f(y_1^{i,i_p}, y_2^{i,i_p}, \ldots, y_j^{i,i_p}, \ldots, y_n^{i,i_p})$, $i = 1,2,\ldots,m$, obtained performing steps 5.–7.: in other words, $\widehat{F}_{i_p}^Z$ is the empirical cumulative distribution function of the model output Z when the epistemically uncertain parameters θ_k, $k = 1,2,\ldots,n_p$, are set to the values $\theta_k^{i_p}$, $k = 1,2,\ldots,n_p$.
9. if $i_p \neq m_p$, then set $i_p = i_p + 1$ and return to step 2.; otherwise, stop the algorithm: the output of the algorithm is a set of m_p empirical cumulative distribution functions $\{\widehat{F}_{i_p}^Z : i_p = 1,2,\ldots,m_p\}$ for the model output Z. This set $\{\widehat{F}_{i_p}^Z : i_p = 1,2,\ldots,m_p\}$ have to be post-processed in order to obtain the upper and lower cumulative distribution functions for Z: Fig. C.1 shows an example of $m_p = 10$ cumulative distribution functions (solid lines) produced by the two-level MC approach together with the corresponding upper and lower cumulative distribution functions (dashed lines).

The operative steps of the two-level MC method described above assume independence between the epistemically uncertain parameters: actually, the random vector $\{r_1^{i_p}, r_2^{i_p}, \ldots, r_k^{i_p}, \ldots, r_{n_p}^{i_p}\}$ sampled at step 2. above is such that $r_1^{i_p} \neq r_2^{i_p} \neq \cdots \neq r_k^{i_p} \neq \cdots \neq r_{n_p}^{i_p}$; on the contrary, in case of total dependence, the condition $r_1^{i_p} = r_2^{i_p} = \cdots = r_k^{i_p} = \cdots = r_{n_p}^{i_p}$ have to be imposed (Fig. C.2).

[9] It is worth noting that in the following, for ease of notation, the entire set of epistemically uncertain parameters $\{\theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j}\}$, $j = 1,2,\ldots,n$, is "condensed" into a single vector $\boldsymbol{\theta} = \{\theta_1, \theta_2, \ldots, \theta_k, \ldots, \theta_{n_p}\}$, with $n_p = \sum_{j=1}^{n} m_j$, and the corresponding probability distributions are referred to as $\{p^{\theta_1}(\theta_1), p^{\theta_2}(\theta_2), \ldots, p^{\theta_k}(\theta_k), \ldots, p^{\theta_{n_p}}(\theta_{n_p})\}$.

References

[1] Apostolakis GE. The concept of probability in safety assessments of technological systems. Science 1990;250(4986):1359–64.
[2] Helton JC, Oberkampf. Alternative representations of epistemic uncertainty. Spec Issue Reliab Eng Syst Saf 2004;85(1–3):1–10.
[3] Limbourg P, de Rocquigny E. Uncertainty analysis using evidence theory – confronting level-1 and level-2 approaches with data availability and computational constraints. Reliab Eng Syst Saf 2010;95(5):550–64.
[4] Cullen AC, Frey HC. Probabilistic techniques in exposure assessment: a handbook for dealing with variability and uncertainty in models and inputs. New York, NY: Plenum Press; 1999.
[5] Rao KD, Kushwaha HS, Verma AK, Srividya A. Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliab Eng Syst Saf 2007;92(7):947–56.
[6] Karanki DR, Kushwaha HS, Verma AK, Ajit S. Uncertainty analysis based on probability bounds (p-box) approach in probabilistic safety assessment. Risk Anal 2009;29(5):662–75.
[7] Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliab Eng Syst Saf 2011;96(1):64–74.
[8] Klir GJ, Yuan B. Fuzzy sets and fuzzy logic: theory and applications. Upper Saddle River, NJ: Prentice-Hall; 1995.
[9] Ferson S, Kreinovich V, Ginzburg L, Sentz K, Myers DS. Constructing probability boxes and Dempster–Shafer structures. Sandia National Laboratories, Technical Report SAND2002-4015, Albuquerque, New Mexico, 2003.

[10] Ferson S, Nelsen RB, Hajagos J, Berleant DJ, Zhang J, Tucker WT, Ginzburg LR, Oberkampf WL. Dependence in probabilistic modeling, Dempster–Shafer theory, and probability bounds analysis. SAND2004, 2004.
[11] Helton JC, Johnson JD, Oberkampf WL, Storlie CB. A sampling-based computational strategy for the representation of epistemic uncertainty in model predictions with evidence theory. Comput Methods Appl Mech Eng 2007;196:3980–98.
[12] Helton JC, Johnson JD, Oberkampf WL, Sallaberry CJ. Representation of analysis results involving aleatory and epistemic uncertainty. SAND2008-4379, 2008.
[13] Sentz K, Ferson S. Combination of evidence in Dempster–Shafer theory. Sandia National Laboratories, Technical Report SAND2002-0835, Albuquerque, New Mexico, 2002.
[14] Shafer G. A mathematical theory of evidence. Princeton, NJ: Princeton University Press; 1976.
[15] Baudrit C, Dubois D, Guyonnet D. Joint propagation and exploitation of probabilistic and possibilistic information in risk assessment. IEEE Trans Fuzzy Syst 2006;14(5):593–608.
[16] Baudrit C, Dubois D, Perrot N. Representing parametric probabilistic models tainted with imprecision. Fuzzy Sets Syst 2008;159(15):1913–28.
[17] Dubois D, Prade H. Possibility theory: an approach to computerized processing of uncertainty. New York, NY: Plenum Press; 1988.
[18] Dubois D. Possibility theory and statistical reasoning. Comput Stat Data Anal 2006;51:47–69.
[19] Ferson S, Tucker WT. Sensitivity in risk analyses with uncertain numbers. Setauket, New York 11733, SAND2006-2801, 2006
[20] Ferson S, Kreinovich V, Hajagos J, Oberkampf W, Ginzburg L. Experimental uncertainty estimation and statistics for data having interval uncertainty. Setauket, New York 11733, SAND2007-0939, 2007.
[21] Moore RE. Methods and applications of interval analysis. Philapdelphia, PA: SIAM; 1979.
[22] Kalos MH, Whitlock PA. Monte Carlo methods. Basics, vol. I. New York, NY: Wiley; 1986.
[23] Marseguerra M, Zio E. Basics of the Monte Carlo Method with application to system reliability. Hagen, Germany: LiLoLe-Verlag GmbH; 2002.
[24] Baraldi P, Zio E. A combined Monte Carlo and possibilistic approach to uncertainty propagation in event tree analysis. Risk Anal 2008;28(5):1309–26.
[25] Baudrit C, Guyonnet D, Dubois D. Post-processing the hybrid method for addressing uncertainty in risk assessments. J Environ Eng Div ASCE 2005;131(12):1750–4.
[26] Baudrit C, Guyonnet D, Dubois D. Joint propagation of variability and imprecision in assessing the risk of groundwater contamination. J Contam Hydrol 2007;93:72–84.
[27] Baudrit C, Couso I, Dubois D. Joint propagation of probability and possibility in risk analysis: toward a formal framework. Int J Approx Reason 2007;45(1):82–105.
[28] Cooper JA, Ferson S, Ginzburg L. Hybrid processing of stochastic and subjective uncertainty data. Risk Anal 1996;16(6):785–91.
[29] Flage R, Baraldi P, Zio E, Aven T. Possibility–probability transformation in comparing different approaches to the treatment of epistemic uncertainties in a fault tree analysis. In: Ale B, Papazoglu IA, Zio E, editors. Reliability, risk and safety – proceedings of the European safety and reliability (ESREL) 2010 conference, Rhodes, Greece. London, United Kingdom: Taylor & Francis Group; 2010. p. 714–21. ISBN 978-0-415-60427-7.
[30] Guyonnet D, Bourgine B, Dubois D, Fargier H, Côme B, Chilès JP. Hybrid approach for addressing uncertainty in risk assessments. J Environ Eng Div ASCE 2003;129:68–78.
[31] Kentel E, Aral MM. Probabilistic-fuzzy health risk modeling. Stoch Environ Res Risk Assess 2004;18:324–38.
[32] Kentel E, Aral MM. Risk tolerance measure for decision-making in fuzzy analysis: a health risk assessment perspective. Stoch Environ Res Risk Assess 2007;21:405–17.
[33] Zadeh LA. Fuzzy sets. Inf Control 1965;8(3):338–53.
[34] Kentel E, Aral MM. 2D Monte Carlo versus 2D fuzzy Monte Carlo health risk assessment. Int J Stoch Environ Res Risk Assess 2005;19:86–96.
[35] Moller B. Fuzzy randomness – a contribution to imprecise probability. ZAMM – Z Angew Math Mech 2004;84(10–11):754–64.
[36] Möller B, Beer M. Fuzzy randomness: uncertainty in civil engineering and computational mechanics. Berlin: Springer; 2004.
[37] Möller B, Beer M. Engineering computation under uncertainty – capabilities of non-traditional models. Comput Struct 2008;86:1024–41.
[38] Moller B, Graf W, Beer M. Safety assessment of structures in view of fuzzy randomness. Comput Struct 2003;81:1567–82.
[39] Moller B, Beer M, Graf W, Sickert JU. Time-dependent reliability of textile-strengthened RC structures under consideration of fuzzy randomness. Comput Struct 2006;84:585–603.
[40] Baudrit C, Dubois D. Comparing methods for joint objective and subjective uncertainty propagation with an example in a risk assessment. In: Cozman FG, Nau R, Seidenfeld T, editors. Fourth international symposium on imprecise probabilities and their applications (ISIPTA '05), Pittsburgh, PA, USA, 20/07/2005–23/07/2005.
[41] Baudrit C, Dubois D, Fargier H. Propagation of uncertainty involving imprecision and randomness. In: Proceedings of the international conference in fuzzy logic and technology (EUSFLAT03), Zittau, Germany, 10/09/2003–12/09/2003.
[42] Fetz T. Sets of joint probability measures generated by weighted marginal focal sets. In: de Cooman G, Fine TL, Seidenfeld T, editors. Proceedings of the second international symposium on imprecise probability and their applications. Maastricht: Shaker Publishing; 2001. p. 171–8.
[43] Fetz T, Oberguggenberger M. Propagation of uncertainty through multivariate functions in the framework of sets of probability measures. Reliab Eng Syst Saf 2004;85:73–87.
[44] Helton JC, Johnson JD, Oberkampf WL. An exploration of alternative approaches to the representation of uncertainty in model predictions. Reliab Eng Syst Saf 2004;85:39–72.
[45] Moral S, Wilson N. Importance sampling Monte-Carlo algorithms for the calculation of Dempster–Shafer belief. Technical Report, UTAI University of Granada, 1996.
[46] Oberkampf WL, Helton JC. Investigation of evidence theory for engineering applications. AIAA Non-Deterministic Approaches Forum, April 2002, Denver, Colorado, paper 2002-1569.
[47] Oberkampf WL, Helton JC, Sentz K. Mathematical representation of uncertainty. AIAA Non-Deterministic Approaches Forum, April 2001, Seattle, Washington, paper 2001-1645.
[48] Tonon F. Using random set theory to propagate epistemic uncertainty through a mechanical system. Reliab Eng Syst Saf 2004;85:169–81.
[49] Tonon F, Bernardini A, Mammino A. Determination of parameters range in rock engineering by means of random set theory. Reliab Eng Syst Saf 2000;70:241–61.
[50] Tonon F, Bernardini A, Mammino A. Reliability analysis of rock mass response by means of random set theory. Reliab Eng Syst Saf 2000;70:263–82.
[51] Dubois D, Prade H. Fuzzy sets and systems: theory and applications. New York: Academic Press; 1980.
[52] Dubois D, Prade H, Sandri S. On possibility/probability transformations. In: Lowen R, Roubens M, editors. Fuzzy logic: state of the art. Dordrecht: Kluwer Academic Publishers.; 1993. p. 103–12.
[53] Dubois D, Prade H, Smets P. A definition of subjective possibility. Int J Approx Reason 2008;48:352–64.
[54] Baudrit C, Dubois D. Practical representations of incomplete probabilistic knowledge. Comput Stat Data Anal 2006;51(1):86–108.
[55] Kendall M, Stuart A. The advanced theory of statistics. London, UK: Griffin and Co.; 1977.
[56] Apostolakis GE, Kaplan S. Pitfalls in risk calculations. Reliab Eng 1981;2(2):135–45.
[57] USNRC. Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making. NUREG-1855, US Nuclear Regulatory Commission, Washington, DC, 2009.

Risk Analysis, Vol. 33, No. 6, 2013 DOI: 10.1111/j.1539-6924.2012.01903.x

Uncertainty Analysis in Fault Tree Models with Dependent Basic Events

Nicola Pedroni[1] and Enrico Zio[1,2,*]

In general, two types of dependence need to be considered when estimating the probability of the top event (TE) of a fault tree (FT): "objective" dependence between the (random) occurrences of different basic events (BEs) in the FT and "state-of-knowledge" (epistemic) dependence between estimates of the epistemically uncertain probabilities of some BEs of the FT model. In this article, we study the effects on the TE probability of objective and epistemic dependences. The well-known Frèchet bounds and the distribution envelope determination (DEnv) method are used to model all kinds of (possibly unknown) objective and epistemic dependences, respectively. For exemplification, the analyses are carried out on a FT with six BEs. Results show that both types of dependence significantly affect the TE probability; however, the effects of epistemic dependence are likely to be overwhelmed by those of objective dependence (if present).

KEY WORDS: Epistemically uncertain probabilities; fault tree; objective and epistemic dependences

1. INTRODUCTION

In fault tree analysis (FTA),[1–5] limiting relative frequency probabilities are typically used to describe aleatory uncertainty and subjective probabilities to describe epistemic uncertainty.[3(2,6–14)] Recently, it has been argued that a probabilistic representation of epistemic uncertainty is difficult to justify in those cases in which the analysis is carried out based on insufficient knowledge, information, and data. To overcome this hurdle, a number of alternative nonprobabilistic representation frameworks have been proposed,[15–19] for example, fuzzy set theory,[20–28] possibility theory,[29–33] hybrid combinations of probability and possibility theories,[30,34–36] Dempster-Shafer (DS) theory of evidence,[37–44] and interval analysis.[45–49]

To describe the epistemic uncertainty in the probabilities (chances) of the basic events (BEs) of a fault tree (FT) model, here we use possibility distributions and DS structures, together with probability distributions. The epistemic uncertainties are then propagated onto the probability (chance) of the top event (TE) by resorting to the general and comprehensive framework of DS theory of evidence.[37–44]

Dependence may exist among some BEs of the FT model.[40] In particular, two types of dependence need to be considered. The first type relates to the (dependent) occurrence of different (random) BEs (in the following, this kind of dependence will be referred to as "objective" or "aleatory"). An example

[1]Energy Department, Politecnico di Milano, Via Ponzio, 34/3 – 20133 Milano, Italy.
[2]Chair of system science and the energetic challenge, Electricitè de France-Ecole Centrale de Paris and Supelec, Grande Voie des Vignes, 92295, Chatenay Malabry-Cedex, France.
[3]In the following, "probability" refers to the limiting relative frequency concept whenever followed by the word "chance" in parentheses, and to the epistemic concept whenever used alone.
*Address correspondence to Enrico Zio, Electricitè de France-Ecole Centrale de Paris and Supelec, Grande Voie des Vignes, 92295, Chatenay Malabry-Cedex, France; tel: +33-01-41-13-16-06; fax: +33-01-41-13-12-72; enrico.zio@ecp.fr; enrico.zio@supelec.fr.

 0272-4332/13/0100-1146$22.00/1 © 2012 Society for Risk Analysis

of this objective (aleatory) dependence may be represented by the occurrence of multiple failures that result directly from a common or shared root cause (e.g., extreme environmental conditions, failure of a piece of hardware external to the system, or a human error): they are termed common cause failures (CCFs) and frequently affect, for example, identical components in redundant trains of a safety system;[2,50–52] another example is that of cascading failures, that is, multiple failures initiated by the failure of one component in the system, as a sort of chain reaction or domino effect.[52–57] The second type refers to the dependence possibly existing between the estimates of the epistemically uncertain probabilities (chances) of some BEs of the FT model (in the following, this kind of dependence will be referred to as "state-of-knowledge" or "epistemic"). This state-of-knowledge (epistemic) dependence exists when the probabilities (chances) of some BEs are estimated by resorting to dependent information sources (e.g., to the same experts/observers or to correlated data sets).[2,11]

In this context, the aim of this article is to systematically analyze and quantify the effects of objective (aleatory) and state-of-knowledge (epistemic) dependences between the BEs on the TE probability (chance). In more details, the following analyses are performed:

1. The study of the effects of different states of objective dependence between the BEs when the state of epistemic dependence between the BE probabilities (chances) is defined. In this analysis the well-known Frèchet bounds[40,58–60] are used to model the full range of objective dependences here of interest;
2. The study of the *effects* of different states of epistemic dependence between the BE probabilities (chances) when the state of objective dependence between the BEs is given. In this analysis the distribution envelope determination (DEnv) method[61–65] is undertaken in order to account for all kinds of (possibly unknown) epistemic dependences between the BE probabilities (chances).

To keep the analysis simple and thus retain a clear view of each step, the investigations are carried out with respect to an example involving a FT with six BEs; different numerical indicators are considered to perform a fair and quantitative comparison between different states of objective and epistemic dependence and evaluate their effects on the TE probability (chance).

The work benefits from the efforts that have already been done to address objective and state-of-knowledge dependences in FTA. In Refs. 66–68, objective dependencies between BEs are treated by means of alpha factor models within the traditional framework of CCF analysis. In Refs. 40 and 60 the use of Frank copula and Pearson correlation coefficient is proposed to describe a wide range of objective dependences between the BEs. In Refs. 69 and 70 (fuzzy) dependency factors are employed to model dependent BEs. In Refs. 71–74 state-of-knowledge dependences between the BE probabilities (chances) are described by traditional correlation coefficients and propagated by the method of moments. In Refs. 68 and 75 statistical epistemic correlations are modeled by resorting to the Nataf transformation[76] within a traditional Monte Carlo simulation framework.[77,78] Finally, in Ref. 79 the dependency bound convolution approach is undertaken to account for all kinds of (possibly unknown) epistemic dependences between the probabilities (chances) of correlated BEs.

The remainder of the article is organized as follows. In Section 2, the methods employed in this study to model objective and state-of-knowledge dependences in FTA are described; in Section 3, the FT studied is presented; in Section 4, the results of the application of the methods of Section 2 to the FT of Section 3 are shown; finally, Section 5 offers some discussions and conclusions.

2. METHODS EMPLOYED IN THIS STUDY FOR MODELING DEPENDENCES IN FAULT TREE ANALYSIS

In this section, the computational strategies here employed for modeling dependences in FTA are described in detail: in particular, Section 2.1 deals with the representation of objective (aleatory) dependences between (the occurrence of) BEs; instead, Section 2.2 concerns the treatment of state-of-knowledge (epistemic) dependences between the probabilities (chances) of the BEs.

Other approaches for modeling objective dependences between (random) events can be found in Refs. 40, 60, and 66–70.

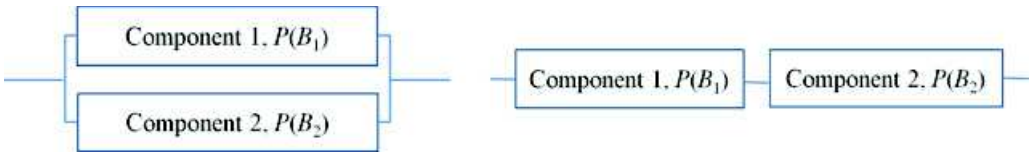


Fig. 1. Simple parallel (left-hand side) and series (right-hand side) systems of two components whose failure probabilities (chances) are $P(B_1)$ and $P(B_2)$, respectively.

2.1 Modeling Objective (Aleatory) Dependences Between the Basic Events

Let B_1 and B_2 be two BEs with probabilities (chances) $P(B_1)$ and $P(B_2)$, respectively; with reference to the simple parallel and series systems of Fig. 1 (left- and right-hand side, respectively), B_1 and B_2 may represent the events of failure of Components 1 and 2, respectively, and $P(B_1)$ and $P(B_2)$ the corresponding probabilities (chances). If B_1 and B_2 are independent, the occurrence of one event (e.g., failure of Component 1) does not affect the occurrence of the other (e.g., failure of Component 2), that is, $P(B_1|B_2) = P(B_1)$ and $P(B_2|B_1) = P(B_2)$. Then, the probabilities (chances) $P(B_1 \cap_{ind} B_2)$ and $P(B_1 \cup_{ind} B_2)$ of the conjunction $(B_1 \cap_{ind} B_2)$ and disjunction $(B_1 \cup_{ind} B_2)$ of events B_1 and B_2 (i.e., the probabilities-chances of failure of the parallel and series systems of Fig. 1, left- and right-hand side, respectively) are given by the well-known deterministic functions $g_{B_1 \cap_{ind} B_2}(P(B_1),\ P(B_2))$, that is, Equations (1) and $g_{B_1 \cup_{ind} B_2}(P(B_1),\ P(B_2))$ (2), respectively:[40,60]

$$\begin{aligned} P(B_1 \cap_{ind} B_2) &= g_{B_1 \cap_{ind} B_2}(P(B_1),\ P(B_2)) \\ &= P(B_1) \times P(B_2) \end{aligned} \tag{1}$$

$$\begin{aligned} P(B_1 \cup_{ind} B_2) &= g_{B_1 \cup_{ind} B_2}(P(B_1),\ P(B_2)) \\ &= 1 - (1 - P(B_1)) \times (1 - P(B_2)), \end{aligned} \tag{2}$$

where the symbols "$\cap_{ind}$" and "$\cup_{ind}$" denote the conjunction and disjunction of independent events, respectively.

If events B_1 and B_2 are perfectly dependent (i.e., $B_1 \subset B_2$ or $B_2 \subset B_1$), the occurrence of one event (e.g., failure of Component 1 in Fig. 1) implies the occurrence of the other (e.g., failure of Component 2 in Fig. 1) (i.e., $P(B_2|B_1) = 1$ or $P(B_1|B_2) = 1$, respectively). In this case, $P(B_1 \cap_{perf} B_2)$ and $P(B_1 \cup_{perf} B_2)$ are given by Equations (3) and (4), respectively:[40,60]

$$\begin{aligned} P(B_1 \cap_{perf} B_2) &= g_{B_1 \cap_{perf} B_2}(P(B_1),\ P(B_2)) \\ &= \min\,(P(B_1),\ P(B_2)) \end{aligned} \tag{3}$$

$$\begin{aligned} P(B_1 \cup_{perf} B_2) &= g_{B_1 \cup_{perf} B_2}(P(B_1),\ P(B_2)) \\ &= \max(P(B_1),\ P(B_2)), \end{aligned} \tag{4}$$

where the symbols "$\cap_{perf}$" and "$\cup_{perf}$" denote the conjunction and disjunction of perfectly dependent events, respectively. Examples of perfect dependence can be found in many engineered systems. For example, some components may be subject to the same maintenance strategy and suffer a common mistake in the procedure, or may experience the same history of environmental conditions leading to failure. Such shared life conditions may make failures of components close to perfectly dependent events.[2,40,50,51] The importance of this state of dependence can be understood with reference to the simple parallel system of Fig. 1, left-hand side: if Components 1 and 2 were perfectly dependent, the failure of only one component would lead to the failure of the entire parallel system.

Finally, if events B_1 and B_2 are oppositely dependent, the occurrence of one event minimizes the likelihood of occurrence of the other. In this case, $P(B_1 \cap_{opp} B_2)$ and $P(B_1 \cup_{opp} B_2)$ are given by Equations (5) and (6), respectively:[40,60]

$$\begin{aligned} P(B_1 \cap_{opp} B_2) &= g_{B_1 \cap_{opp} B_2}(P(B_1),\ P(B_2)) \\ &= \max(P(B_1) + P(B_2) - 1,\ 0) \end{aligned} \tag{5}$$

$$\begin{aligned} P(B_1 \cup_{opp} B_2) &= g_{B_1 \cup_{opp} B_2}(P(B_1),\ P(B_2)) \\ &= \min\,(P(B_1) + P(B_2), 1), \end{aligned} \tag{6}$$

where the symbols "$\cap_{opp}$" and "$\cup_{opp}$" denote the conjunction and disjunction of oppositely dependent events, respectively. An example of opposite dependence may be represented by the series of a fuse wire (e.g., Component 1 in Fig. 1, right-hand side) and an electronic device (e.g., Component 2 in Fig. 1, right-hand side). In case of overcurrent, failure of the fuse wire (event B_1) prevents failure of the electronic component (event B_2); thus, the joint failure of both components might be better modeled by events that are oppositely dependent than independent.

When no information at all about the state of objective dependence between events B_1 and B_2 is available, precise estimates for $P(B_1 \cap B_2)$ and $P(B_1 \cup B_2)$ cannot be computed. Instead, extreme bounds $P(B_1 \cap_{ukn} B_2)$ (Equation (7)) and $P(B_1 \cup_{ukn} B_2)$ (Equation (8)) on $P(B_1 \cap B_2)$ and $P(B_1 \cup B_2)$, respectively, can be obtained by means of the classical Frèchet inequalities:[40,58–60]

$$P(B_1 \cap_{ukn} B_2) = [g_{B_1 \cap_{opp} B_2}, g_{B_1 \cap_{perf} B_2}] = [\max(P(B_1) + P(B_2) - 1, 0), \min(P(B_1), P(B_2))] \quad (7)$$

$$P(B_1 \cup_{ukn} B_2) = [g_{B_1 \cup_{perf} B_2}, g_{B_1 \cup_{opp} B_2}] = [\max(P(B_1), P(B_2)), \min(P(B_1) + P(B_2), 1)], \quad (8)$$

where functions $g_{B_1 \cap_{perf} B_2}, g_{B_1 \cup_{perf} B_2}, g_{B_1 \cap_{opp} B_2}$, and $g_{B_1 \cup_{opp} B_2}$ are defined in Equations (3)–(6) and the symbols "$\cap_{ukn}$" and "$\cup_{ukn}$" denote the conjunction and disjunction of events whose state of objective dependence is completely unknown, respectively. As stated in Ref. 40, it is worth mentioning that (i) $P(B_1 \cap_{ukn} B_2)$ (Equation (7)) and $P(B_1 \cup_{ukn} B_2)$ (Equation (8)) are "bounds on all possible cases of objective dependence" (because they include by construction dependences ranging from opposite to perfect) and (ii) they represent the "best possible bounds in the absence of information about objective dependence, that is, they could not be any tighter without excluding some possible objective dependences."[40]

Finally, if the analyst is able to say something about the sign of objective dependence, then Frèchet bounds (Equations (7) and (8)) can be tightened. In particular, if B_1 and B_2 are positively dependent, that is, the occurrence of one event favors the occurrence of the other, then $P(B_1|B_2) > P(B_1)$ and $P(B_2|B_1) > P(B_2)$, from which it follows that $P(B_1 \cap_{pos} B_2) > P(B_1 \cap_{ind} B_2)$. In this case, bounds $P(B_1 \cap_{pos} B_2)$ and $P(B_1 \cup_{pos} B_2)$ on $P(B_1 \cap B_2)$ and $P(B_1 \cup B_2)$ are obtained by Equations (9) and (10), respectively:[40,60]

$$P(B_1 \cap_{pos} B_2) = [g_{B_1 \cap_{ind} B_2}, g_{B_1 \cap_{perf} B_2}] = [P(B_1) \times P(B_2), \min(P(B_1), P(B_2))] \quad (9)$$

$$P(B_1 \cup_{pos} B_2) = [g_{B_1 \cup_{perf} B_2}, g_{B_1 \cup_{ind} B_2}] = [\max(P(B_1), P(B_2)), 1 - (1 - P(B_1)) \times (1 - P(B_2))]. \quad (10)$$

On the contrary, if B_1 and B_2 are negatively dependent, then bounds $P(B_1 \cap_{neg} B_2)$ and $P(B_1 \cup_{neg} B_2)$ on $P(B_1 \cap B_2)$ and $P(B_1 \cup B_2)$ are obtained using Equations (11) and (12), respectively:[40,60]

$$P(B_1 \cap_{neg} B_2) = [g_{B_1 \cap_{opp} B_2}, g_{B_1 \cap_{ind} B_2}] = [\max(P(B_1) + P(B_2) - 1, 0), P(B_1) \times P(B_2)] \quad (11)$$

$$P(B_1 \cup_{neg} B_2) = [g_{B_1 \cup_{ind} B_2}, g_{B_1 \cup_{opp} B_2}] = [1 - (1 - P(B_1)) \times (1 - P(B_2)), \min(P(B_1) + P(B_2), 1)]. \quad (12)$$

2.2 Modeling State-of-Knowledge (Epistemic) Dependences Between the Probabilities (Chances) of the Basic Events

In all generality, let us assume that:

i. events B_1 and B_2 are linked to an event Z of interest by the generic logical connection "o" (e.g., "o" may stand for "$\cap$," "$\cup$," ...);
ii. the state of objective dependence between events B_1 and B_2 is defined and indicated as "o_{obj}": for example, if there is positive objective dependence between B_1 and B_2, then the subscript "*obj*" stands for "*pos*" (see Section 2.1);
iii. the probability (chance) $P(Z)$ of the event $Z = (B_1\ \mathrm{o}_{obj}\ B_2)$ of interest is obtained as $P(Z) = g_Z(P(B_1), P(B_2))$, where $g_Z(P(B_1), P(B_2))$ is a deterministic function that provides a formal, mathematical description of the state of objective dependence between events B_1 and B_2 (for example, $g_Z(\cdot, \cdot)$ may be one of those reported in Equations (1)–(12)).
iv. the probabilities (chances) $P(B_1)$ and $P(B_2)$ of events B_1 and B_2 are considered epistemically uncertain. For ease of explanation, let us suppose that the epistemic uncertainty on $P(B_1)$ and $P(B_2)$ is represented by the DS structures $\{(A^i_{P(B_1)}, m(A^i_{P(B_1)})) : i = 1, 2, \ldots, n_{B_1}\}$ and $\{(A^j_{P(B_2)}, m(A^j_{P(B_2)})) : j = 1, 2, \ldots, n_{B_2}\}$, respectively: in other words, $P(B_1)$ and $P(B_2)$ are described by two sets of n_{B_1} and n_{B_2} intervals (focal elements) $A^i_{P(B_1)} = [\underline{p}^i_{B_1}, \overline{p}^i_{B_1}], i = 1, 2, \ldots, n_{B_1}$, and $A^j_{P(B_2)} = [\underline{p}^j_{B_2}, \overline{p}^j_{B_2}], j = 1, 2, \ldots, n_{B_2}$, respectively, each of which is assigned a probability (or belief) mass $m(A^i_{P(B_1)}), i = 1, 2, \ldots, n_{B_1}$, and $m(A^j_{P(B_2)}), j = 1, 2, \ldots, n_{B_2}$, respectively (it is worth stressing that $m(A^i_{P(B_1)})$ and $m(A^j_{P(B_2)})$ represent the degrees of belief

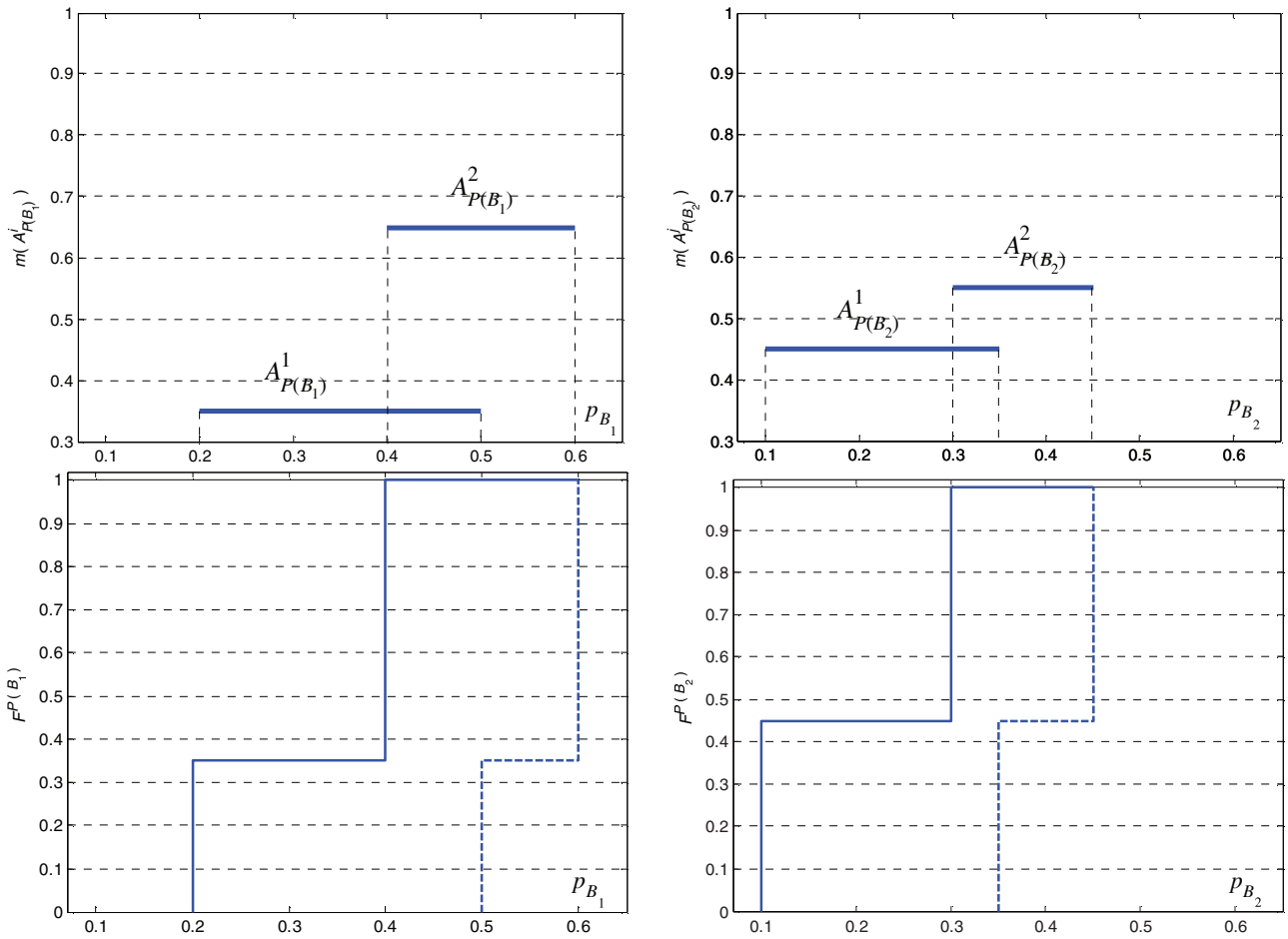


Fig. 2. Top panel: illustrative DS structures {([0.20, 0.50], 0.35), ([0.40, 0.60], 0.65)} and {([0.10, 0.35], 0.45), ([0.30, 0.45], 0.55)} for $P(B_1)$ (left-hand side) and $P(B_2)$ (right-hand side), respectively. Bottom panel: upper (solid line) and lower (dashed line) CDFs, $\overline{F}^{P(B_1)}$, $\overline{F}^{P(B_2)}$, $\underline{F}^{P(B_1)}$, and $\underline{F}^{P(B_2)}$, respectively, corresponding to the illustrative DS structures described above.

of membership of $P(B_1)$ and $P(B_2)$ in sets $A^i_{P(B_1)}$ and $A^j_{P(B_2)}$ only, but without any specification of how these degrees of belief might be apportioned over $A^i_{P(B_1)}$ and $A^j_{P(B_2)}$, respectively; in other words, $m(A^i_{P(B_1)})$ and $m(A^j_{P(B_2)})$ express the proportion to which all available and relevant evidence supports the claim that $P(B_1)$ and $P(B_2)$, whose characterization is incomplete, belong to sets $A^i_{P(B_1)}$ and $A^j_{P(B_2)}$, respectively). By way of example, let $\{(A^i_{P(B_1)}, m(A^i_{P(B_1)})) : i = 1, 2, \ldots, n_{B_1} = 2\} = \{([0.20, 0.50], 0.35), ([0.40, 0.60], 0.65)\}$ and $\{(A^j_{P(B_2)}, m(A^j_{P(B_2)})) : j = 1, 2, \ldots, n_{B_2} = 2\} = \{([0.10, 0.35], 0.45), ([0.30, 0.45], 0.55)\}$: for clarity, the corresponding DS structures are pictorially shown in Fig. 2, top left- and right-hand side, respectively. Referring to probability (chance) $P(B_1)$ of event B_1 (Fig. 2, top left-hand side), the corresponding DS structure can be interpreted as follows: probability (chance) $P(B_1)$ of event B_1 lies within interval $A^1_{P(B_1)} = [0.20, 0.50]$ at least with probability $m(A^1_{P(B_1)}) = 0.35$, whereas it lies within interval $A^2_{P(B_1)} = [0.40, 0.60]$ at least with probability $m(A^2_{P(B_1)}) = 0.65$. Notice that the DS structures described above can be transformed into upper and lower cumulative distribution functions (CDFs) $\overline{F}^{P(B_1)}$, $\overline{F}^{P(B_2)}$, $\underline{F}^{P(B_1)}$, and

$\underline{F}^{P(B_2)}$ for $P(B_1)$ and $P(B_2)$, respectively: in particular, $\overline{F}^{P(B_1)}(p_{B_1}) = \overline{P}[P(B_1) < p_{B_1}] = \sum_{A^i_{P(B_1)} \cap [0, p_{B_1}] \neq 0} m(A^i_{P(B_1)})$ and $\underline{F}^{P(B_1)}(p_{B_1}) = \underline{P}[P(B_1) < p_{B_1}] = \sum_{A^i_{P(B_1)} \subset [0, p_{B_1}]} m(A^i_{P(B_1)})$; in the same way, $\overline{F}^{P(B_2)}(p_{B_2}) = \overline{P}[P(B_2) < p_{B_2}] = \sum_{A^j_{P(B_2)} \cap [0, p_{B_2}] \neq 0} m(A^j_{P(B_2)})$ and $\underline{F}^{P(B_2)}(p_{B_2}) = \underline{P}[P(B_2) < p_{B_2}] = \sum_{A^j_{P(B_2)} \subset [0, p_{B_2}]} m(A^j_{P(B_2)})$.

The upper and lower CDFs, $\overline{F}^{P(B_1)}$, $\overline{F}^{P(B_2)}$, $\underline{F}^{P(B_1)}$, and $\underline{F}^{P(B_2)}$, respectively, corresponding to the illustrative DS structures {([0.20, 0.50], 0.35)., .([0.40, 0.60], 0.65)}, and {([0.10, 0.35], 0.45)., .([0.30, 0.45], 0.55)} of $P(B_1)$ and $P(B_2)$ are pictorially shown in Fig. 2, bottom left- and right-hand side, respectively. For example, referring again to event B_1, the upper and lower CDFs, $\overline{F}^{P(B_1)}$ and $\underline{F}^{P(B_1)}$, can be interpreted as follows: the probability $P[P(B_1) < p_{B_1}]$ that $P(B_1)$ is lower than or equal to, for example, $p_{B_1} = 0.30$ lies within interval $[\underline{F}^{P(B_1)}(0.30), \overline{F}^{P(B_1)}(0.30)] = [0, 0.35]$ (referring to the concept of Bayesian subjective probabilities, the bounds $[\underline{F}^{P(B_1)}(0.30), \overline{F}^{P(B_1)}(0.30)] = [0, 0.35]$ reflect that the analyst is not able or willing to precisely assign his/her probability $P[P(B_1) < p_{B_1}]$). Further details about DS structures (and DS theory of evidence) are not given here for brevity: the interested reader is referred to the copious literature in the field.[4(37–44)]

The focal elements $A^{ij}_{P(Z)} = [\underline{p}^{ij}_Z, \overline{p}^{ij}_Z]$, $i = 1, 2, \ldots, n_{B_1}$, $j = 1, 2, \ldots, n_{B_2}$, of the probability (chance) $P(Z)$ of the event $Z = (B_1 \circ_{obj} B_2)$ are obtained as images of the focal sets $A^i_{P(B_1)}$, $i = 1, 2, \ldots, n_{B_1}$, and $A^j_{P(B_2)}$, $j = 1, 2, \ldots, n_{B_2}$, through the function $g_Z(P(B_1), P(B_2))$ as $A^{ij}_{P(Z)} = [\underline{p}^{ij}_Z, \overline{p}^{ij}_Z] = [\min_{P(B_1) \in A^i_{P(B_1)}, P(B_2) \in A^j_{P(B_2)}} \{g_Z(P(B_1), P(B_2))\}, .. \max_{P(B_1) \in A^i_{P(B_1)}, P(B_2) \in A^j_{P(B_2)}} \{g_Z(P(B_1), P(B_2))\}]$, $i = 1, 2, \ldots, n_{B_1}$, $j = 1, 2, \ldots, n_{B_2}$. For illustration purposes, again let B_1 and B_2 be the events of failure of Components 1 and 2, respectively, of the simple parallel system of Fig. 1 left-hand side, and $P(B_1)$ and $P(B_2)$ the corresponding probabilities (chances): then, the probability (chance) $P(Z)$ of failure of the parallel system of Fig. 1 left is the probability (chance) of the conjunction $Z = (B_1 \cap_{obj} B_2)$ of B_1 and B_2. For the sake of simplicity, we also suppose that B_1 and B_2 are (objectively) independent events (i.e., "*obj*" = "*ind*"): in such a case, $P(Z)$ is given by the product of $P(B_1)$ and $P(B_2)$, that is, $P(Z) = g_Z(P(B_1), P(B_2)) = P(B_1) \cdot P(B_2)$ (see Equation (1)). Finally, we suppose that $P(B_1)$ and $P(B_2)$ are distributed as in Fig. 2. In this case, the lower (resp., upper) bound $\underline{p}^{ij}_Z$ (resp., $\overline{p}^{ij}_Z$) of the focal set $A^{ij}_{P(Z)}$ is computed as the product of the lower bounds $\underline{p}^i_{B_1}$ and $\underline{p}^j_{B_2}$ (resp., upper bounds $\overline{p}^i_{B_1}$ and $\overline{p}^j_{B_2}$) of the focal sets $A^i_{P(B_1)}$ and $A^j_{P(B_2)}$, respectively, that is, $\underline{p}^{ij}_Z = \underline{p}^i_{B_1} \cdot \underline{p}^j_{B_2}$ (resp., $\overline{p}^{ij}_Z = \overline{p}^i_{B_1} \cdot \overline{p}^j_{B_2}$), $i = 1, 2$, $j = 1, 2$. Thus, it is found that $A^{11}_{P(Z)} = [0.2 \cdot 0.1, 0.5 \cdot 0.35] = [0.02, 0.175]$, $A^{12}_{P(Z)} = [0.2 \cdot 0.3, 0.5 \cdot 0.45] = [0.06, 0.225]$, $A^{21}_{P(Z)} = [0.4 \cdot 0.1, 0.6 \cdot 0.35] = [0.04, 0.210]$, $A^{22}_{P(Z)} = [0.4 \cdot 0.3, 0.6 \cdot 0.45] = [0.120, 0.270]$.

The probability masses $m(A^{ij}_{P(Z)})$ of the focal elements $A^{ij}_{P(Z)}$, $i = 1, 2, \ldots, n_{B_1}$, $j = 1, 2, \ldots, n_{B_2}$, thereby obtained have to be determined based on the state of epistemic dependence between the estimates of $P(B_1)$ and $P(B_2)$. Three conditions of epistemic dependence are often encountered in risk assessment problems and, thus, considered in this article: (i) independence (Section 2.2.1), (ii) total (perfect) dependence (Section 2.2.2), and (iii) unknown dependence[5] (Section 2.2.3).

2.2.1 Independence

If the distributions describing the epistemic uncertainty associated to $P(B_1)$ and $P(B_2)$ are built using "different information sources" (e.g., different experts, observers, or data sets), then state-of-knowledge independence (item i. above, "*epi*" = "*ind*") exists between the estimates of $P(B_1)$ and

[4]Notice that representing the epistemic uncertainty in the probabilities (chances) $P(B_1)$ and $P(B_2)$ by DS structures does not impair the generality of the description. Actually, *any* other type of distribution that may be used to describe the epistemic uncertainty in $P(B_1)$ and $P(B_2)$ can be easily transformed into a DS structure: approaches for transforming *probability* distributions can be found in Refs. 80 and 81, whereas techniques for transforming *possibility* distributions can be found in Refs. 30.

[5]In the rest of the article, the state of epistemic dependence between the probabilities (chances) $P(B_1)$ and $P(B_2)$ of events B_1 and B_2 linked to an event Z of interest by the logical connection "$\circ_{obj}$" is indicated as $(B_1 \circ_{obj} B_2)^{epi}$, where the superscript "*epi*" stands for "*ind*," "*perf*," or "*ukn*" in the cases of independence, total (perfect), or unknown epistemic dependence, respectively.

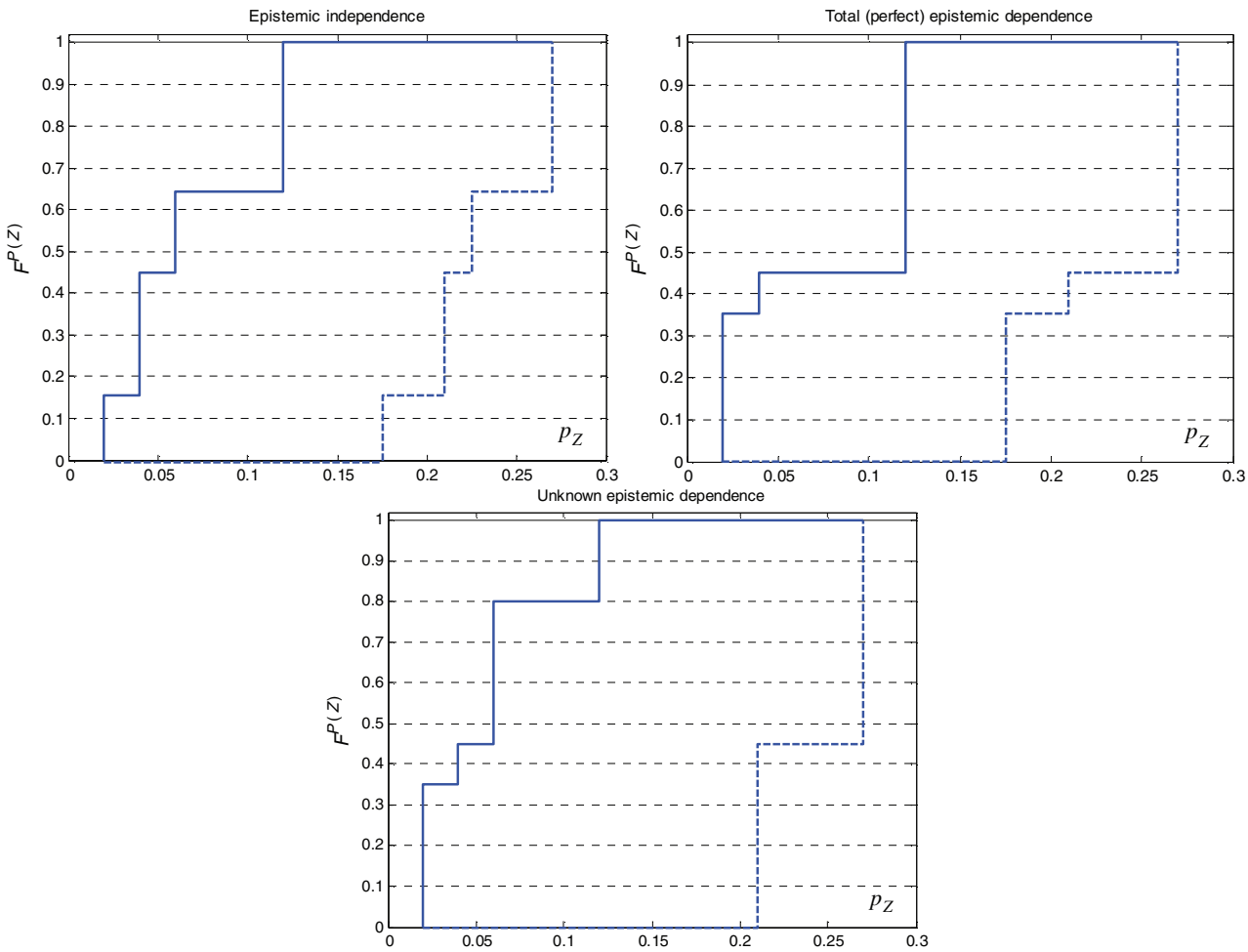


Fig. 3. Upper (solid lines) and lower (dashed lines) CDFs, $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$, of the probability (chance) $P(Z)$ of the conjunction of two (objectively) independent events B_1 and B_2 with probabilities (chances) $P(B_1)$ and $P(B_2)$ distributed as in Fig. 2, under the assumptions of independence (top left-hand side), total (top right-hand side), and unknown (bottom panel) epistemic dependence.

$P(B_2)$: in this article, such condition is modeled by assuming "random set independence" between the focal elements $A^i_{P(B_1)} = [\underline{p}^i_{B_1}, \overline{p}^i_{B_1}]$, $i = 1, 2, \ldots, n_{B_1}$, and $A^j_{P(B_2)} = [\underline{p}^j_{B_2}, \overline{p}^j_{B_2}]$, $j = 1, 2, \ldots, n_{B_2}$.[40,82–84] In practice, this amounts to computing the probability masses $m(A^{ij}_{P(Z)})$ of the focal elements $A^{ij}_{P(Z)}$ as the product of the probability masses $m(A^i_{P(B_1)})$ and $m(A^j_{P(B_2)})$, that is, $m(A^{ij}_{P(Z)}) = m(A^i_{P(B_1)}).m(A^j_{P(B_2)})$, $i = 1, 2, \ldots, n_{B_1}$, $j = 1, 2, \ldots, n_{B_2}$. Thus, referring again to the example above, it is found that under the assumption of random set independence ("*epi*" = "*ind*") the probability masses of the focal sets $A^{11}_{P(Z)} = [0.02, 0.175]$, $A^{12}_{P(Z)} = [0.06, 0.225]$, $A^{21}_{P(Z)} = [0.04, 0.210]$ and $A^{22}_{P(Z)} = [0.120, 0.270]$ are $m(A^{11}_{P(Z)}) = 0.35 \times 0.45 = 0.1575$, $m(A^{12}_{P(Z)}) = 0.35 \times 0.55 = 0.1925$, $m(A^{21}_{P(Z)}) = 0.65 \times 0.45 = 0.2925$ and $m(A^{22}_{P(Z)}) = 0.65 \times 0.55 = 0.3575$, respectively. The corresponding upper and lower CDFs, $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$, of the probability (chance) $P(Z)$ of $Z = (B_1 \cap_{ind} B_2)^{ind}$ are shown in Fig. 3, top left-hand side.

2.2.2 Total (Perfect) Dependence

When the same information source is employed to construct the uncertainty distributions for $P(B_1)$ and $P(B_2)$, then total (perfect) dependence (item ii. above, "*epi*" = "*perf*") exists between the estimates of $P(B_1)$ and $P(B_2)$.[2,11] By way of example, consider the case of a system containing a number of physically distinct, but similar/nominally

identical components whose failure probabilities (chances) are estimated by means of the same data set: in such situation, the state of knowledge about these failure probabilities (chances) is exactly the same and, thus, the distributions describing the epistemic uncertainty associated to such failure probabilities (chances) have to be considered totally (perfectly) dependent.[6(2,11)] In this article, such condition is straightforwardly modeled by imposing maximal correlation between the distributions of $P(B_1)$ and $P(B_2)$.[(2,11)] In practice, assuming that the distributions of $P(B_1)$ and $P(B_2)$ are totally (perfectly) correlated implies that when one uncertain parameter (e.g., $P(B_1)$) is large with reference to its statistical distribution, then also the other uncertain parameter (e.g., $P(B_2)$) is large "to the same degree with respect to its own statistical distribution."[(40)] This "empirical" definition suggests the computational strategy for simulating total (perfect) correlation between the distributions of the uncertain parameters $P(B_1)$ and $P(B_2)$: (i) choose a set of n_B (equally spaced) values β^i, $i = 1, 2, \ldots, n_B$, within [0, 1) (e.g., $\beta^1 = 0$, $\beta^2 = 0.01, \ldots, \beta^{nB-1} = 0.99$, $\beta^{nB} = 1$); (ii) identify the corresponding focal sets $A^i_{P(B_1)} = [\underline{p}^i_{B_1}, \overline{p}^i_{B_1}]$ and $A^i_{P(B_2)} = [\underline{p}^i_{B_2}, \overline{p}^i_{B_2}]$ of $P(B_1)$ and $P(B_2)$ using the inverse transform method, that is, $[(\overline{F}^{P(B_1)})^{-1}(\beta^i), (\underline{F}^{P(B_1)})^{-1}(\beta^i)]$ and $[(\overline{F}^{P(B_2)})^{-1}(\beta^i), (\underline{F}^{P(B_2)})^{-1}(\beta^i)]$, $i = 1, 2, \ldots, n_B$, respectively (notice that using the same values β^i for the identification of the focal sets of both $P(B_1)$ and $P(B_2)$ implies total (perfect) dependence between them);[(11)] (iii) calculate the focal elements $A^i_{P(Z)}$ as $[\min_{P(B_1)\in A^i_{P(B_1)}, P(B_2)\in A^i_{P(B_2)}}\{g_Z(P(B_1), P(B_2))\}, [\max_{P(B_1)\in A^i_{P(B_1)}, P(B_2)\in A^i_{P(B_2)}}\{g_Z(P(B_1), P(B_2))\}]$, $i = 1, 2, \ldots, n_B$; (iv) associate to $A^i_{P(Z)}$ the probability mass $m(A^i_{P(Z)}) = 1/n_B$, $i = 1, 2, \ldots, n_B$. Referring again to the example above, it is found that under the assumption of total (perfect) epistemic dependence the probability masses of the focal sets $A^{11}_{P(Z)} = [0.02, 0.175]$, $A^{12}_{P(Z)} = [0.06, 0.225]$, $A^{21}_{P(Z)} = [0.04, 0.210]$ and $A^{22}_{P(Z)} = [0.120, 0.270]$ obtained by performing steps (i)–(iv) above are $m(A^{11}_{P(Z)}) = 0.35$, $m(A^{12}_{P(Z)}) = 0$, $m(A^{21}_{P(Z)}) = 0.10$ and $m(A^{22}_{P(Z)}) = 0.55$, respectively. The resulting upper and lower CDFs, $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$, of the probability (chance) $P(Z)$ of $Z = (B_1 \cap_{ind} B_2)^{perf}$ are shown in Fig. 3, top right-hand side.

[6]As stated in Ref. 2, p. 54, "an analyst's state of knowledge about the possible values of a parameter θ can be expressed in terms of a probability distribution $f^{\theta}(\theta)$ when using Bayesian updating or expert judgment. It is common practice to assign the same value to the parameters of BEs of identical or similar components. Therefore, for example, the probability of failure of a class of identical motor-operated valves (MOVs) to open is considered the same. Suppose that θ_1 and θ_2 represent the parameters of two physically distinct but identical MOVs: because this discussion assumes that all such MOVs have the same parameter, it is necessary to set $\theta_1 = \theta_2$. Moreover, because the analyst's state of knowledge is the same for the two valves, it follows that $f^{\theta_1}(\theta_1) = f^{\theta_2}(\theta_2)$. Thus, $f^{\theta_1}(\theta_1)$ and $f^{\theta_2}(\theta_2)$ must be regarded as being equal distributions and treated as completely dependent distributions."

2.2.3 *Unknown Dependence*

When the state of dependence between the information sources used to build the distributions of $P(B_1)$ and $P(B_2)$ cannot be defined precisely by the analyst (item iii. above, "*epi*" = "*ukn*"), for the sake of conservatism all kinds of (possibly unknown) epistemic dependences between the estimates of $P(B_1)$ and $P(B_2)$ have to be accounted for. In this article, the distribution envelope determination (DEnv) method[(61–65)] is adopted to this aim. The DEnv method allows computing extreme upper and lower CDFs $\overline{F}^{P(Z)}_{DEnv}(p_Z)$ and $\underline{F}^{P(Z)}_{DEnv}(p_Z)$ on the probability (chance) $P(Z) = g_Z(P(B_1), P(B_2))$ of the event $Z = (B_1 \circ_{obj} B_2)^{ukn}$ of interest no matter what correlations or dependencies exist among $P(B_1)$ and $P(B_2)$; these bounds are also the "pointwise best possible, which means they could not be any tighter without excluding some possible dependences."[(40)] In practice, the aim of the DEnv approach is to identify the $n_{B_1} \times n_{B_2}$ probability masses $m(A^{ij}_{P(Z)})$ for the focal elements $A^{ij}_{P(Z)}$, $i = 1, 2, \ldots, n_{B_1}$, $j = 1, 2, \ldots, n_{B_2}$, such that the upper CDF on $P(Z)$ is the maximal possible (i.e., $\overline{F}^{P(Z)}_{DEnv}(p_Z) = \max\{\overline{F}^{P(Z)}(p_Z)\}$ and the lower CDF on $P(Z)$ is the minimal possible ($\underline{F}^{P(Z)}_{DEnv}(p_Z) = \min\{\underline{F}^{P(Z)}(p_Z)\}$ provided that a precise set of constraints is satisfied.[(61–65)] In more detail, $\overline{F}^{P(Z)}_{DEnv}(p_Z)$ and $\underline{F}^{P(Z)}_{DEnv}(p_Z)$ are found by solving the following linear maximization (Equation (13)) and minimization (Equation (14)) problems, respectively:

$$\begin{aligned}
&\text{Find } m\left(A^{ij}_{P(Z)}\right), i = 1, 2, \ldots, n_{B_1}, j = 1, 2, \ldots, n_{B_2}: \\
&\overline{F}^{P(Z)}_{DEnv}(p_Z) = \max\left\{\overline{F}^{P(Z)}(p_Z)\right\} \\
&= \max\left\{\sum_{A^{ij}_{P(Z)} = g_Z\left(A^i_{P(B_1)}, A^j_{P(B_2)}\right) \cap [0, p_Z] \neq 0} m\left(A^{ij}_{P(Z)}\right)\right\}, \forall p_Z
\end{aligned} \tag{13}$$

$$\text{Find } m\left(A^{ij}_{P(Z)}\right),\ i = 1, 2, \ldots, n_{B_1},\ j = 1, 2, \ldots, n_{B_2}:$$
$$\underline{F}^{P(Z)}_{DEnv}(p_Z) = \min\left\{\underline{F}^{P(Z)}(p_Z)\right\}$$
$$= \min\left\{\sum_{A^{ij}_{P(Z)} = g_Z\left(A^i_{P(B_1)},\, A^j_{P(B_2)}\right) \subset [0,\, p_Z]} m\left(A^{ij}_{P(Z)}\right)\right\},\ \forall p_Z \tag{14}$$

subject to the constraints that (i) the probability masses $m(A^i_{P(B_1)})$ and $m(A^j_{P(B_2)})$ are conserved (i.e., $\sum_{i=1}^{n_{B_1}} m(A^{ij}_{P(Z)}) = m(A^j_{P(B_2)})$, $j = 1, 2, \ldots, n_{B_2}$, and $\sum_{j=1}^{n_{B_2}} m(A^{ij}_{P(Z)}) = m(A^i_{P(B_1)})$, $i = 1, 2, \ldots, n_{B_1}$) and (ii) the probability masses $m(A^{ij}_{P(Z)})$ are larger than or equal to zero. For illustration purposes, the values of $\overline{F}^{P(Z)}_{DEnv}(p_Z) = \overline{F}^{P(Z)}_{DEnv}(0.08)$ and $\underline{F}^{P(Z)}_{DEnv}(p_Z) = \underline{F}^{P(Z)}_{DEnv}(0.22)$ are calculated with reference to the example above. In order to calculate $\overline{F}^{P(Z)}_{DEnv}(0.08)$ by solving maximization problem (13), those focal sets among $A^{ij}_{P(Z)}$, $i = 1, 2, .j = 1, 2$, that intersect interval $[0, p_Z] = [0, 0.08]$ have to be identified. Since in this case $A^{11}_{P(Z)} = [0.02, 0.175]$, $A^{12}_{P(Z)} = [0.06, 0.225]$, $A^{21}_{P(Z)} = [0.04, 0.210]$ and $A^{22}_{P(Z)} = [0.120, 0.270]$ (see above), only focal sets $A^{11}_{P(Z)}$, $A^{12}_{P(Z)}$, and $A^{21}_{P(Z)}$ intersect interval [0, 0.08]; then, only focal sets $A^{11}_{P(Z)}$, $A^{12}_{P(Z)}$, and $A^{21}_{P(Z)}$ and the corresponding probability masses $m(A^{11}_{P(Z)})$, $m(A^{12}_{P(Z)})$, and $m(A^{21}_{P(Z)})$ have to be included in the function $\overline{F}^{P(Z)}(0.08)$ to be maximized. As a consequence, maximization problem (13) becomes:

$$\text{Find } m\left(A^{11}_{P(Z)}\right),\ m\left(A^{12}_{P(Z)}\right),\ m\left(A^{21}_{P(Z)}\right),\ m\left(A^{22}_{P(Z)}\right):$$
$$\overline{F}^{P(Z)}_{DEnv}(0.08) = \max\left\{\overline{F}^{P(Z)}(0.08)\right\}$$
$$= \max\left\{m\left(A^{11}_{P(Z)}\right) + m\left(A^{12}_{P(Z)}\right) + m\left(A^{21}_{P(Z)}\right)\right\} \tag{15}$$

subject to the constraints that (i) $m(A^{11}_{P(Z)}) + m(A^{12}_{P(Z)}) = m(A^1_{P(B_1)}) = 0.35$, $m(A^{21}_{P(Z)}) + m(A^{22}_{P(Z)}) = m(A^2_{P(B_1)}) = 0.65$, $m(A^{11}_{P(Z)}) + m(A^{21}_{P(Z)}) = m(A^1_{P(B_2)}) = 0.45$, $m(A^{12}_{P(Z)}) + m(A^{22}_{P(Z)}) = m(A^2_{P(B_2)}) = 0.55$ and (ii) $m(A^{11}_{P(Z)}), m(A^{12}_{P(Z)}), m(A^{21}_{P(Z)}), m(A^{22}_{P(Z)}) \geq 0$. The optimization process leads to $\overline{F}^{P(Z)}_{DEnv}(0.08) = 0.8$ with $m(A^{11}_{P(Z)}) = 0$, $m(A^{12}_{P(Z)}) = 0.35$, $m(A^{21}_{P(Z)}) = 0.45$ and $m(A^{22}_{P(Z)}) = 0.2$.

Instead, in order to calculate $\underline{F}^{P(Z)}_{DEnv}(0.22)$ by solving minimization problem (14), those focal sets among $A^{ij}_{P(Z)}$, $i = 1, 2, . j = 1, 2$, that are included in interval $[0, p_Z] = [0, 0.22]$ have to be identified. Since in this case $A^{11}_{P(Z)} = [0.02, 0.175]$, $A^{12}_{P(Z)} = [0.06, 0.225]$, $A^{21}_{P(Z)} = [0.04, 0.210]$ and $A^{22}_{P(Z)} = [0.120, 0.270]$ (see above), only focal sets $A^{11}_{P(Z)}$ and $A^{21}_{P(Z)}$ are included in interval [0, 0.22]; then, only $A^{11}_{P(Z)}$ and $A^{21}_{P(Z)}$ and the corresponding probability masses $m(A^{11}_{P(Z)})$ and $m(A^{21}_{P(Z)})$ have to be taken into account in the function $\underline{F}^{P(Z)}(0.22)$ to be minimized. Then, minimization problem (14) becomes:

$$\text{Find } m\left(A^{11}_{P(Z)}\right),\ m\left(A^{12}_{P(Z)}\right),\ m\left(A^{21}_{P(Z)}\right),\ m\left(A^{22}_{P(Z)}\right):$$
$$\underline{F}^{P(Z)}_{DEnv}(0.22) = \min\left\{\underline{F}^{P(Z)}(0.22)\right\}$$
$$= \min\left\{m\left(A^{11}_{P(Z)}\right) + m\left(A^{21}_{P(Z)}\right)\right\} \tag{16}$$

subject to the same constraints as Equation (15). The optimization process leads to $\underline{F}^{P(Z)}_{DEnv}(0.22) = 0.45$ with $m(A^{11}_{P(Z)}) = 0.15$, $m(A^{12}_{P(Z)}) = 0.20$, $m(A^{21}_{P(Z)}) = 0.30$ and $m(A^{22}_{P(Z)}) = 0.35$.

Finally, it is worth noting that in order to construct the entire CDFs $\overline{F}^{P(Z)}_{DEnv}(p_Z)$ and $\underline{F}^{P(Z)}_{DEnv}(p_Z)$ for $P(Z)$, such optimization problems have to be solved for *all* the values p_Z of interest. The resulting upper and lower CDFs, $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$, of the probability (chance) $P(Z)$ of $Z = (B_1 \cap_{ind} B_2)^{ukn}$ are shown in Fig. 3, bottom panel.

3. CASE STUDY

In this section, we present the example FT used for reference. In Section 3.1, the FT structure and BEs uncertainties are described; in Section 3.2, the different states of (objective and epistemic) dependence between the BEs are summarized; in Section 3.3, the numerical indicators used to quantify the effects of such dependences are provided.

3.1 Fault Tree Structure and Basic Events Uncertainties

A simple FT comprised of $n_{BE} = 6$ BEs $\{B_i: i = 1, 2, \ldots, n_{BE} = 6\}$ is considered (Fig. 4). BEs B_1, B_2, and B_3 are linked to event E_1 by junction J_1 (an OR-gate) and BEs B_4, B_5, and B_6 are linked to event E_2 by junction J_2 (also an OR-gate); finally, events E_1 and E_2 are linked to the TE X by junction J_3

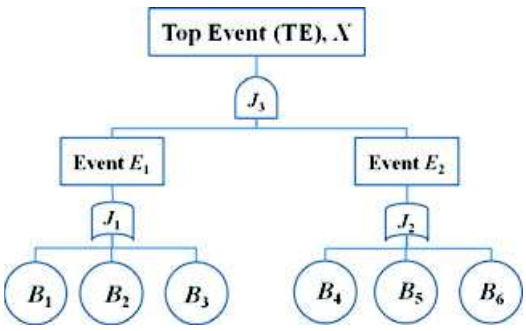


Fig. 4. FT structure.

(an AND-gate):

$$X = E_1 \cap E_2 = (B_1 \cup B_2 \cup B_3) \cap (B_4 \cup B_5 \cup B_6)\,. \tag{17}$$

Letting $\{P(B_i):\ i = 1,\ 2,\ \ldots,\ n_{BE} = 6\}$ denote the probabilities (chances) of BEs $\{B_i\colon i = 1, 2, \ldots, n_{BE} = 6\}$, the probability (chance) $P(X)$ of the TE X is expressed in all generality as follows:

$$P(X) = g_X(P(B_1), P(B_2), P(B_3), P(B_4), P(B_5), P(B_6)), \tag{18}$$

where $g_X(\cdot)$ is a deterministic function of (i) the FT structure (i.e., the logical connections between the BEs) (see Fig. 4) and (ii) the (possible) objective dependences existing between the BEs (see Sections 2 and 3.2).

It is assumed that $\{P(B_i) : i = 1,\ 2,\ \ldots,\ n_{BE} = 6\}$ are epistemically uncertain. Uncertainties about $\{P(B_i) : i = 1, 6\}$ are described using lognormal probability distribution functions $\{f^{P(B_i)}(p_{B_i}) = LN(\mu_i,\ \sigma_i) :\ i = 1,\ 6\}$ with parameter values $\{(\mu_i, \sigma_i)\colon i = 1, 6\}$ as specified in Table I. As an example, B_1 and B_6 could denote failure of an item (e.g., a mechanical component) for which a sufficient amount of informative (failure) data is available for statistical analysis and for accurate characterization of the corresponding epistemic uncertainty by a precise probability distribution. Differently, uncertainties about $\{P(B_i) : i = 2, 3, 5\}$ are represented using (trapezoidal) possibility distributions $\{\pi^{P(B_i)}(p_{B_i}) = TRAP(a_i,\ b_i,\ c_i,\ d_i) :\ i = 2,\ 3,\ 5\}$, with supports $\{[a_i, d_i]\colon i = 2, 3, 5\}$ and cores $\{[b_i, c_i]\colon i = 2, 3, 5\}$ as specified in Table I. By way of example, B_2, B_3, and B_5 could denote events (e.g., human-error-dominated events) for which no data exist and where the (trapezoidal) possibility distributions are constructed based on expert statements alone. Finally, the uncertainty about $P(B_4)$ is described by a finite DS structure, that is, by a set of $n_{B_4} = 4$ intervals (focal elements) $A^j_{P(B_4)} = [\underline{p}^j_{B_4}, \overline{p}^j_{B_4}]$, $j = 1, 2, \ldots, n_{B_4} = 4$, each of which is assigned a probability mass $m(A^j_{P(B_4)})$, $j = 1, 2, \ldots, n_{B_4} = 4$, as specified in Table I. As an example, B_4 could denote failure of an item (e.g., a protective or automation system, a digital instrumentation and control system, a recently-developed technology, ...) for which only sparse pieces of data exist: in such cases, the available information is much more valuable than purely subjective (and often vague) expert judgment, but it is not sufficient for building a precise probability distribution.

Two different cases are considered: "large" (Case A) and "small" (Case B) BE probabilities (chances). In Case A, $\{P(B_i) : i = 1, 2, \ldots, n_{BE} = 6\}$ are of the order of 10^{-1}, whereas in Case B they are of the order of 10^{-3} (Table I). For illustration purposes, Fig. 5 shows the distributions of $\{P(B_i) : i = 1, 2, \ldots, n_{BE} = 6\}$, with reference only to Case B.

3.2 States of Dependence Considered

The following states of objective dependence between the BEs of Section 3.1 are considered in the analysis (Section 2.1): (a) independence (see Equations (1) and (2)), (b) perfect (see Equations (3) and (4)), (c) opposite (see Equations (5) and (6)), (d) positive (see Equations (9) and (10)), (e) negative (see Equations (11) and (12)), and (f) unknown dependence (see Equations (7) and (8)). In addition, the following states of epistemic dependence between the probabilities (chances) of the BEs of Section 3.1 are considered in the analysis (Section 2.2): (i) independence, (ii) perfect, and (iii) unknown dependence.

Two classes of analyses are performed (Section 4):

1. assuming unknown epistemic dependence (iii. above) between the probabilities (chances) of the BEs, the effects of different states (a–f above) of objective dependence between the BEs are analyzed;
2. assuming objective independence (a. above) between the BEs, the effects of different states (i.–iii. above) of epistemic dependence between the probabilities (chances) of the BEs are analyzed.

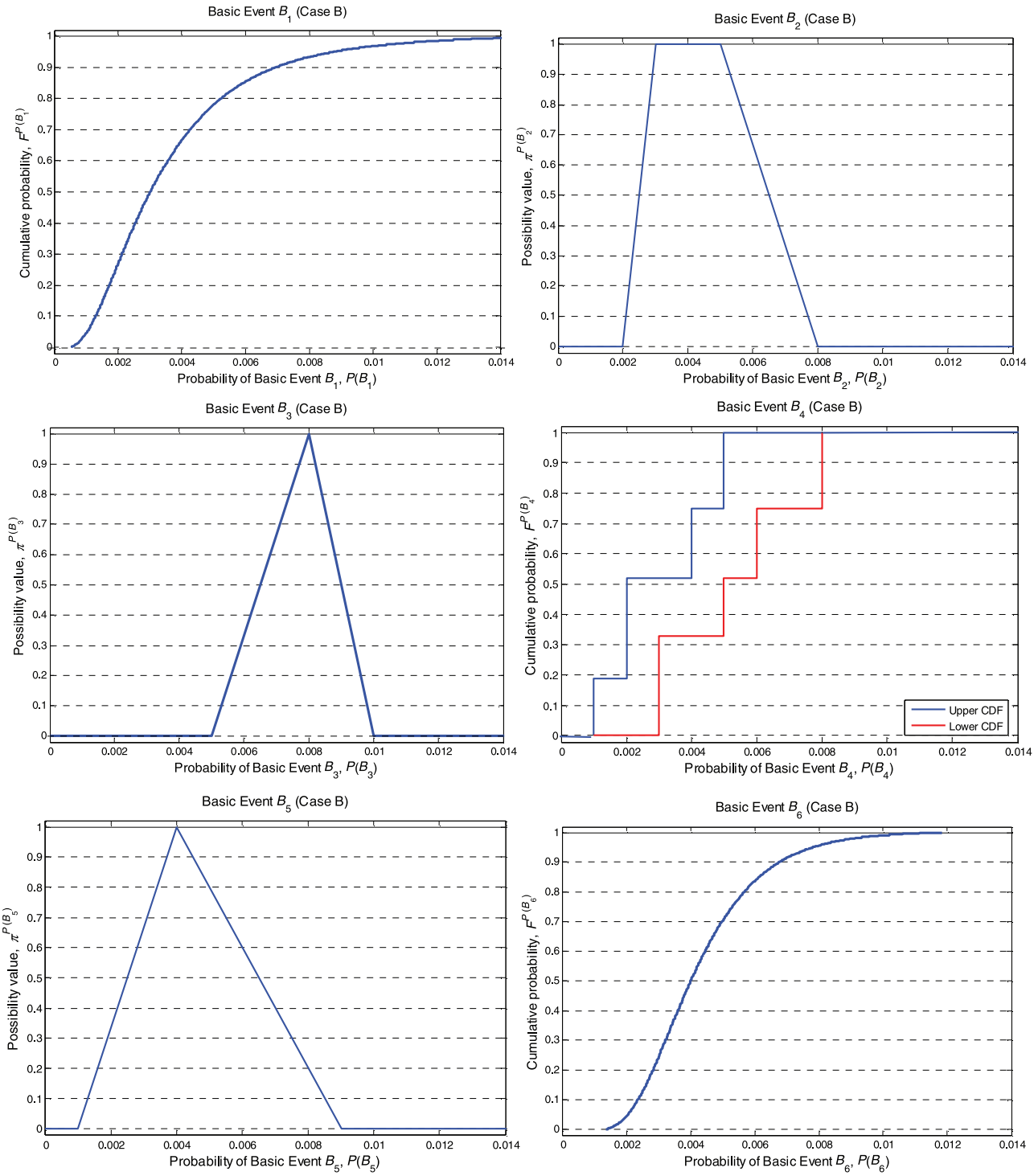


Fig. 5. Distributions of $\{P(B_i) : i = 1, 2, \ldots, n_{BE} = 6\}$ for Case B.

Table I. Characteristics and Parameters of the Distributions of $\{P(B_i): i = 1, 2, \ldots, n_{BE} = 6\}$

$P(B_1)$		
Epistemic uncertainty description		Probability distribution
Distribution shape		Lognormal, $f^{P(B_1)}(p_{B_1}) = LN(\mu_1, \sigma_1)$
Distribution parameters	**Case A**	$\mu_1 = -1.6094, \sigma_1 = 0.3226$
	Case B	$\mu_1 = -5.8091, \sigma_1 = 0.6678$
$P(B_2)$		
Epistemic uncertainty description		Possibility distribution
Distribution shape		Trapezoidal, $\pi^{P(B_2)}(p_{B_2}) = TRAP(a_2, b_2, c_2, d_2)$
Distribution parameters	**Case A**	$a_2 = 1 \times 10^{-1}, b_2 = 1.5 \times 10^{-1}, c_2 = 2.5 \times 10^{-1}, d_2 = 4 \times 10^{-1}$
	Case B	$a_2 = 2 \times 10^{-3}, b_2 = 3 \times 10^{-3}, c_2 = 5 \times 10^{-3}, d_2 = 8 \times 10^{-3}$
$P(B_3)$		
Epistemic uncertainty description		Possibility distribution
Distribution shape		Trapezoidal, $\pi^{P(B_3)}(p_{B_3}) = \mathrm{TRAP}(a_3, b_3, c_3, d_3)$
Distribution parameters	**Case A**	$a_3 = 2.5 \times 10^{-1}, b_3 = 4 \times 10^{-1}, c_3 = 4 \times 10^{-1}, d_3 = 5 \times 10^{-1}$
	Case B	$a_3 = 5 \times 10^{-3}, b_3 = 8 \times 10^{-3}, c_3 = 8 \times 10^{-3}, d_3 = 1 \times 10^{-2}$
$P(B_4)$		
Epistemic uncertainty description		Dempster-Shafer (DS) structure
Distribution shape		$\{(A^j_{P(B_4)}, m(A^j_{P(B_4)})) : j = 1, 2, \ldots, n_{B_4} = 4\}$
Distribution parameters	**Case A**	$\{([5 \times 10^{-2}, 2.5 \times 10^{-1}], 0.19), ([1 \times 10^{-1}, 1.5 \times 10^{-3}], 0.33), ([2.5 \times 10^{-1}, 4 \times 10^{-1}], 0.25), ([2 \times 10^{-1}, 3 \times 10^{-1}], 0.23)\}$
	Case B	$\{([1 \times 10^{-3}, 5 \times 10^{-3}], 0.19), ([2 \times 10^{-3}, 3 \times 10^{-3}], 0.33), ([5 \times 10^{-3}, 8 \times 10^{-3}], 0.25), ([4 \times 10^{-3}, 6 \times 10^{-3}], 0.23)\}$
$P(B_5)$		
Epistemic uncertainty description		Possibility distribution
Distribution shape		Trapezoidal, $\pi^{P(B_5)}(p_{B_5}) = TRAP(a_5, b_5, c_5, d_5)$
Distribution parameters	**Case A**	$a_5 = 5 \times 10^{-2}, b_5 = 2 \times 10^{-1}, c_5 = 2 \times 10^{-1}, d_5 = 4.5 \times 10^{-3}$
	Case B	$a_5 = 1 \times 10^{-3}, b_5 = 4 \times 10^{-3}, c_5 = 4 \times 10^{-3}, d_5 = 9 \times 10^{-3}$
$P(B_6)$		
Epistemic uncertainty description		Probability distribution
Distribution shape		Lognormal, $f^{P(B_6)}(p_{B_6}) = LN(\mu_6, \sigma_6)$
Distribution parameters	**Case A**	$\mu_6 = -1.3863, \sigma_6 = 0.2465$
	Case B	$\mu_6 = -5.2150, \sigma_6 = 0.4214$

Table II summarizes the analyses carried out in the present article (Section 4) together with the corresponding objectives.

For clarity, Table III reports the details of Analyses 1 and 2 (Table II). First, only for illustration purposes the effects of different states of (objective and epistemic) dependences between BEs $\{B_i: i = 1, 2, \ldots, n_{BE} = 6\}$ are demonstrated with reference to very simple configurations (referred to as C1–C5 in Table III). In particular, events $Z = (B_1 \cap B_6)$ (C1), $(B_1 \cap B_5)$ (C2), $(B_2 \cap B_5)$ (C3), $(B_4 \cup B_5)$ (C4), and $(B_2 \cup B_3)$ (C5) are considered in both Analyses 1 and 2 to study whether (and how) the effects of different states of (objective and epistemic) dependence are influenced by the particular logical connection existing between the BEs. Moreover, such analyses are performed in both Case A (namely, "large" BE probabilities-chances) and Case B (namely, "small" BE probabilities-chances) to study whether (and how) the effects of different states of (objective and epistemic) dependence are influenced by the magnitude of the BE probabilities (chances).

Then, the more realistic case involving the FT of Fig. 4 is considered to analyze the effects that (objective and epistemic) dependences between BEs

Table II. Analyses Performed in Section 4, and their Relative Objectives

	States of dependence between the BEs		
	Objective (Section 2.1)	**Epistemic (Section 2.2)**	**Aim of the analysis**
Analysis 1 (Table III and Section 4.1)	(a) independence (b) perfect dependence (c) opposite dependence (d) positive dependence (e) negative dependence (f) unknown dependence	(iii) unknown dependence	Study the effects of different states of objective dependence between the BEs of the FT when the state of epistemic dependence between the probabilities (chances) of the BEs is given (in particular, unknown epistemic dependence is assumed in the present analysis)
Analysis 2 (Table III and Section 4.2)	(a) independence	(i) independence (ii) total (perfect) dependence (iii) unknown dependence	Study the effects of different states of epistemic dependence between the probabilities (chances) of the BEs of the FT when the state of objective dependence between the BEs is given (in particular, objective independence is assumed in the present analysis)

Table III. Details of the Computations Performed in Analyses 1 and 2 (Table II)

Analysis 1 – Unknown (*ukn*) epistemic dependence between the probabilities (chances) of the BEs			
	Configuration	**Events and corresponding states of objective (*obj*) dependence**	**Cases**
Simple configurations: pairs of basic events (BEs)	C1	$Z = (B_1 \cap_{obj} B_6)^{ukn}$ $\quad obj = ind, perf, opp, ukn$ (see Section 2.1)	A, B
	C2	$Z = (B_1 \cap_{obj} B_5)^{ukn}$	
	C3	$Z = (B_2 \cap_{obj} B_5)^{ukn}$	
	C4	$Z = (B_4 \cup_{obj} B_5)^{ukn}$	
	C5	$Z = (B_2 \cup_{obj} B_3)^{ukn}$	
Top event (TE) *X*	T1	$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{ukn}$	B
	T2	Positive (*pos*) objective dependence between B_1 and B_6	
	T3	$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ukn} B_5 \cup_{ind} B_6)]^{ukn}$	
	T4	$X = [(B_1 \cup_{ukn} B_2 \cup_{ukn} B_3) \cap_{ukn} (B_4 \cup_{ukn} B_5 \cup_{ukn} B_6)]^{ukn}$	
Analysis 2 – Objective independence (*ind*) between the BEs			
	Configuration	**Events and corresponding states of epistemic (*epi*) dependence**	**Cases**
Simple configurations: pairs of basic events (BEs)	C1	$Z = (B_1 \cap_{ind} B_6)^{epi}$ $\quad epi = ind, perf, ukn$ (see Section 2.2)	A, B
	C2	$Z = (B_1 \cap_{ind} B_5)^{epi}$	
	C3	$Z = (B_2 \cap_{ind} B_5)^{epi}$	
	C4	$Z = (B_4 \cup_{ind} B_5)^{epi}$	
	C5	$Z = (B_2 \cup_{ind} B_3)^{epi}$	
Top event (TE) *X*	T1	$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{ind}$	B
	T2	$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{perf}$	
	T3	$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{ukn}$	

Notes: "*Obj*" = objective; "*epi*" = epistemic; "*ind*" = independence; "*perf*" = perfect; "*opp*" = opposite; "*ukn*" = unknown.

$\{B_i\colon i = 1, 2, \ldots, n_{BE} = 6\}$ have on the probability (chance) $P(X)$ of the TE X (Table III, Configurations T1–T4 of Analysis 1 and T1–T3 of Analysis 2). These computations are performed only in Case B (namely, "small" BE probabilities-chances) because in realistic safety-critical engineered systems the basic components are usually highly reliable and, thus, the corresponding failure probabilities (chances) are typically very small. In Analysis 1, Configuration T1 represents the reference, baseline case where all the BEs are considered independent. On the opposite, Configuration T4 represents the extreme (most conservative) case where no assumptions about the states of objective dependence between all the BEs are made. Instead, Configurations T2 and T3 represent "intermediate" (and more realistic) cases. In particular, in Configuration T2 positive objective dependence is assumed between BEs B_1 and B_6 (i.e., those events representing failures of mechanical components): this situation is far from unlikely in real systems and may be due to several causes, for example, (i) shared pieces of equipment (e.g., components in different systems are fed from the same electrical bus) or (ii) physical interactions (e.g., failures of some component create extreme environmental stresses, which increase the probability-chance of multiple-component failures). Instead, in Configuration T3 unknown objective dependence is assumed between BE B_4 (i.e., an event representing the failure of a protective or automation system) and BE B_5 (i.e., an event dominated by a human error): in real systems, this situation may occur, for example, when an operator turns off a protection system (event B_4) after failing to correctly diagnose the conditions of a plant (event B_5).

Finally, in Analysis 2 only "extreme" situations are considered: in particular, in Configurations T1, T2, and T3 states of independence, total (perfect) dependence, and unknown epistemic dependence, respectively, are assumed between all the probabilities (chances) of all the BEs of the FT.

3.3 Quantitative Indicators

Two quantitative indicators are here introduced to evaluate the effects that different states of (objective and state-of-knowledge) dependence between the BEs (Section 3.2) have on the probability (chance) $P(Z)$ of an event Z of interest (e.g., in our case the TE X): (i) the interval $[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$ for the 95th percentile $P(Z)^{0.95}$ of $P(Z)$, and (ii) the relative average distance d_Z between the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$.

The interval $[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$ for the 95th percentile $P(Z)^{0.95}$ of $P(Z)$ is defined as:

$$\left[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}\right] = [\left(\overline{F}^{P(Z)}\right)^{-1}(0.95), \left(\underline{F}^{P(Z)}\right)^{-1}(0.95)], \tag{19}$$

where $[\overline{F}^{P(Z)}]^{-1}$ and $[\underline{F}^{P(Z)}]^{-1}$ are the inverse functions of the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$, respectively, of $P(Z)$. It is worth noting that in a risk analysis context, $\overline{p}_Z^{0.95} = (\underline{F}^{P(Z)})^{-1}(0.95)$ is the interesting quantity since it guarantees that the probability $P[P(Z) \leq \overline{p}_Z^{0.95}]$ that the true value of $P(Z)$ is lower than $\overline{p}_Z^{0.95} = (\underline{F}^{P(Z)})^{-1}(0.95)$ is greater than or equal to 0.95. Thus, $\overline{p}_Z^{0.95} = (\underline{F}^{P(Z)})^{-1}(0.95)$ can be interpreted as a conservative assignment of the 95th percentile $P(Z)^{0.95}$ (i.e., a conservative estimate of risk) with respect to the imprecision arising from the input BEs of the FT: obviously, the larger the value of $\overline{p}_Z^{0.95}$, the larger the risk associated to the system.

The relative average distance d_Z between the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ of $P(Z)$ is defined as:

$$\begin{aligned} d_Z &= \frac{\int_0^1 d_Z(\beta)\, d\beta}{E\left[P(Z)^{INS}\right]} \\ &= \frac{\int_0^1 \left[\left(\underline{F}^{P(Z)}\right)^{-1}(\beta) - \left(\overline{F}^{P(Z)}\right)^{-1}(\beta)\right] d\beta}{E\left[P(Z)^{INS}\right]}, \end{aligned} \tag{20}$$

where $[\overline{F}^{P(Z)}]^{-1}$ and $[\underline{F}^{P(Z)}]^{-1}$ are defined above; $d_Z(\beta) = (\underline{F}^{P(Z)})^{-1}(\beta) - (\overline{F}^{P(Z)})^{-1}(\beta)$ is the width of the interval $[\underline{p}_Z^{\beta}, \overline{p}_Z^{\beta}]$ for the βth percentile $P(Z)^{\beta}$ of $P(Z)$ (in other words, $d_Z(\beta)$ is the distance between the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ of $P(Z)$ computed at cumulative probability level β along the real "horizontal" axis; it is straightforward to notice that $d_Z(\beta)$ can take values between 0 and 1 because it is the distance between the upper and lower values of the βth percentile of $P(Z)$, which obviously takes values between 0 and 1); finally, $E[P(Z)^{INS}]$ is the expected value of the probability distribution $f^{P(Z)^{INS}}(p_Z^{INS})$ obtained by transforming the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ of $P(Z)$ according to the principle of insufficient reason.[85] The sampling procedure for estimating $E[P(Z)^{INS}]$ is

i. transform the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ of $P(Z)$ into the (unique) probability distribution $f^{P(Z)^{INS}}(p_Z^{INS})$:[85,86]

a. sample N_{INS} random realizations $\{u_k: k = 1, 2, \ldots, N_{INS}\}$ from a uniform probability distribution on [0, 1) and consider the corresponding intervals $[(\overline{F}^{P(Z)})^{-1}(u_k), (\underline{F}^{P(Z)})^{-1}(u_k)]$, $k = 1, 2, \ldots, N_{INS}$;

b. sample a random realization $p_{Z,k}^{INS}$ for $P(Z)^{INS}$ from a uniform probability distribution on each interval $[(\overline{F}^{P(Z)})^{-1}(u_k), (\underline{F}^{P(Z)})^{-1}(u_k)]$, $k = 1, 2, \ldots, N_{INS}$: the distribution resulting from the collection of the realizations $p_{Z,k}^{INS}$, $k = 1, 2, \ldots, N_{INS}$, is an empirical estimate for $f^{P(Z)^{INS}}(p_Z^{INS})$);

ii. estimate $E[P(Z)^{INS}]$ as $1/.N_{INS} \cdot \sum_{k=1}^{N_{INS}} p_{Z,k}^{INS}$.

Other methods for transforming the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ of $P(Z)$ into a (unique) probability distribution are available in Refs. 36, 85, 87, and 88.

It is worth noting that the quantity d_Z (20) provides a measure of the average distance (i.e., separation) between the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ of $P(Z)$, computed along the real "horizontal" axis. In this sense, it is also an indicator of the uncertainty (i.e., imprecision) "contained" in the distribution of $P(Z)$: the larger the average distance d_Z (20), the larger the uncertainty (imprecision) associated to $P(Z)$.

Finally, notice that the expected value $E[P(Z)^{INS}]$ in Equation (20) is simply chosen as a numerical indicator of the approximate "location" of the upper and lower CDFs $\overline{F}^{P(Z)}$ and $\underline{F}^{P(Z)}$ on the "horizontal" axis: in other words, it is taken as a numerical indicator of the order of magnitude of $P(Z)$. In this view, $E[P(Z)^{INS}]$ serves the main purpose of a normalization factor for the integral $\int_0^1 [(\underline{F}^{P(Z)})^{-1}(\beta) - (\overline{F}^{P(Z)})^{-1}(\beta)]d\beta$, whose magnitude is obviously dependent on the magnitude of $P(Z)$ and, thus, on the magnitude of the BE probabilities (chances). In this way, such normalization factor allows a fair comparison between values of the distance d_Z (20) computed in Cases A and B (Section 3.1), where the BE probabilities (chances) differ by several orders of magnitude.

4. APPLICATION

In this section, the methods described in Section 2 for handling dependences in FTA are applied to the example of Section 3. In particular, Section 4.1 contains the results of Analysis 1 (Table III in Section 3.2), whereas Section 4.2 reports the results of Analysis 2 (Table III in Section 3.2).

4.1 Studying the Effects of Objective (Aleatory) Dependences Between the Basic Events

Table IV reports the values of the indicators $[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$ (19) and d_Z (20) obtained for the events $Z = (B_1 \cap_{obj} B_6)^{ukn}$, $(B_1 \cap_{obj} B_5)^{ukn}$, $(B_2 \cap_{obj} B_5)^{ukn}$, $(B_4 \cup_{obj} B_5)^{ukn}$, and $(B_2 \cup_{obj} B_3)^{ukn}$ (Configurations C1–C5 of Analysis 1 in Table III) under the assumptions of independence ("*obj*" = "*ind*"), perfect ("*obj*" = "*perf*"), opposite ("*obj*" = "*opp*"), and unknown ("*obj*" = "*ukn*") objective dependence, with reference to Cases A and B (Section 3.1); the estimates of $E[P(Z)^{INS}]$ are also shown for completeness. In addition, only for illustration purposes Fig. 6 depicts the upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{obj} B_5)^{ukn}]}$, $\overline{F}^{P[(B_4 \cup_{obj} B_5)^{ukn}]}$, $\underline{F}^{P[(B_1 \cap_{obj} B_5)^{ukn}]}$, and $\underline{F}^{P[(B_4 \cup_{obj} B_5)^{ukn}]}$ obtained for events $(B_1 \cap_{obj} B_5)^{ukn}$ (top panel) and $(B_4 \cup_{obj} B_5)^{ukn}$ (bottom panel), respectively, under the assumptions of independence (solid lines), perfect (dashed lines), opposite (dotted lines), and unknown (dot-dashed lines) objective dependence, with reference to Cases A (left-hand side) and B (right-hand side). Notice that by construction $\overline{F}^{P[(B_1 \cap_{ukn} B_5)^{ukn}]} = \overline{F}^{P[(B_1 \cap_{perf} B_5)^{ukn}]}$ and $\underline{F}^{P[(B_1 \cap_{ukn} B_5)^{ukn}]} = \underline{F}^{P[(B_1 \cap_{opp} B_5)^{ukn}]}$, whereas $\overline{F}^{P[(B_4 \cup_{ukn} B_5)^{ukn}]} = \overline{F}^{P[(B_4 \cup_{opp} B_5)^{ukn}]}$ and $\underline{F}^{P[(B_4 \cup_{ukn} B_5)^{ukn}]} = \underline{F}^{P[(B_4 \cup_{perf} B_5)^{ukn}]}$ (see Equations (7) and (8)): however, only for clarity of illustration the corresponding lines in Fig. 6 are not overlapped.

We start by analyzing those cases where the BEs are linked by AND-gates, that is, $Z = (B_1 \cap_{obj} B_6)^{ukn}$, $(B_1 \cap_{obj} B_5)^{ukn}$, and $(B_2 \cap_{obj} B_5)^{ukn}$ (Configurations C1–C3 in Table III). It can be seen that in Case A the upper bounds $\overline{p}^{0.95}_{(B_1 \cap_{obj} B_6)^{ukn}}$, $\overline{p}^{0.95}_{(B_1 \cap_{obj} B_5)^{ukn}}$, and $\overline{p}^{0.95}_{(B_2 \cap_{obj} B_5)^{ukn}}$ of the 95th percentiles $P[(B_1 \cap_{obj} B_6)^{ukn}]^{0.95}$, $P[(B_1 \cap_{obj} B_5)^{ukn}]^{0.95}$, and $P[(B_2 \cap_{obj} B_5)^{ukn}]^{0.95}$ are 0.1528, 0.1557, and 0.1760, respectively, under the assumption of independence, whereas they are 0.3461, 0.3462, and 0.3941, respectively, under the assumption of unknown dependence. Thus, the assumption of

Table IV. Values of the Indicators $[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$ (19) and d_Z (20) Obtained for the Simple Events $Z = (B_1 \cap_{obj} B_6)^{ukn}$, $(B_1 \cap_{obj} B_5)^{ukn}$, $(B_2 \cap_{obj} B_5)^{ukn}$, $(B_4 \cup_{obj} B_5)^{ukn}$, and $(B_2 \cup_{obj} B_3)^{ukn}$ (Configurations C1–C5 of Analysis 1 in Table III) Under the Assumptions of Independence, Perfect, Opposite, and Unknown Objective Dependence, with Reference to Cases A and B; the Estimates for $E[P(Z)^{INS}]$ are Also Reported for Completeness

Analysis 1 – Unknown (*ukn*) epistemic dependence between the probabilities (chances) of the BEs					
		State of objective (*obj*) dependence			
Event Z	**Indicators**	**Independence (*ind*)**	**Perfect (*perf*)**	**Opposite (*opp*)**	**Unknown (*ukn*)**
		Case A			
$(B_1 \cap_{obj} B_6)^{ukn}$ (C1)	$E[P(Z)^{INS}]$	0.0583	0.1954	0	0.1069
	d_Z	0.8634	0.6321	/	3.6672
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.0492, 0.1528]	[0.2205, 0.3461]	0	[0, 0.3461]
$(B_1 \cap_{obj} B_5)^{ukn}$ (C2)	$E[P(Z)^{INS}]$	0.0553	0.1627	0	0.1068
	d_Z	1.4779	1.8426	/	3.8630
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.0243, 0.1557]	[0.1564, 0.3462]	0	[0, 0.3462]
$(B_2 \cap_{obj} B_5)^{ukn}$ (C3)	$E[P(Z)^{INS}]$	0.0715	0.2068	0	0.1573
	d_Z	1.6629	3.0140	/	4.3991
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.0188, 0.1760]	[0.1220, 0.3941]	0	[0, 0.3941]
$(B_4 \cup_{obj} B_5)^{ukn}$ (C4)	$E[P(Z)^{INS}]$	0.3933	0.2645	0.4538	0.4219
	d_Z	0.9325	0.5493	1.1871	1.3495
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.3100, 0.6670]	[0.2500, 0.4401]	[0.3302, 0.8401]	[0.2500, 0.8401]
$(B_2 \cup_{obj} B_3)^{ukn}$ (C5)	$E[P(Z)^{INS}]$	0.5272	0.3873	0.6251	0.5750
	d_Z	0.5161	0.2419	0.7644	0.9542
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.4519, 0.6970]	[0.3910, 0.4961]	[0.4911, 0.8941]	[0.3910, 0.8941]
		Case B			
$(B_1 \cap_{obj} B_6)^{ukn}$ (C1)	$E[P(Z)^{INS}]$	2.01×10^{-5}	3.00×10^{-3}	0	1.84×10^{-3}
	d_Z	1.3339	67.0056	/	182.6408
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[1.41 \times 10^{-5}, 9.21 \times 10^{-5}]$	$[3.43 \times 10^{-3}, 8.19 \times 10^{-3}]$	0	$[0, 8.19 \times 10^{-3}]$
$(B_1 \cap_{obj} B_5)^{ukn}$ (C2)	$E[P(Z)^{INS}]$	1.84×10^{-5}	2.71×10^{-3}	0	1.83×10^{-3}
	d_Z	1.2028	101.9268	/	198.2254
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[8.75 \times 10^{-6}, 7.85 \times 10^{-5}]$	$[2.56 \times 10^{-3}, 8.80 \times 10^{-3}]$	0	$[0, 8.80 \times 10^{-3}]$
$(B_2 \cap_{obj} B_5)^{ukn}$ (C3)	$E[P(Z)^{INS}]$	2.62×10^{-5}	4.14×10^{-3}	0	3.15×10^{-3}
	d_Z	1.7034	164.6245	/	240.1765
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[5.68 \times 10^{-6}, 7.01 \times 10^{-5}]$	$[2.44 \times 10^{-3}, 7.88 \times 10^{-3}]$	0	$[0, 7.88 \times 10^{-3}]$
$(B_4 \cup_{obj} B_5)^{ukn}$ (C4)	$E[P(Z)^{INS}]$	8.93×10^{-3}	5.19×10^{-3}	9.00×10^{-3}	8.33×10^{-3}
	d_Z	1.0216	0.4700	1.0325	1.1676
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[6.59 \times 10^{-3}, 1.67 \times 10^{-2}]$	$[5.00 \times 10^{-3}, 8.76 \times 10^{-3}]$	$[6.40 \times 10^{-3}, 1.68 \times 10^{-2}]$	$[5.00 \times 10^{-3}, 1.68 \times 10^{-2}]$
$(B_2 \cup_{obj} B_3)^{ukn}$ (C5)	$E[P(Z)^{INS}]$	1.25×10^{-2}	7.74×10^{-3}	1.25×10^{-2}	1.15×10^{-2}
	d_Z	0.6381	0.2047	0.6468	0.8076
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[9.83 \times 10^{-3}, 1.78 \times 10^{-2}]$	$[7.82 \times 10^{-3}, 9.92 \times 10^{-3}]$	$[9.82 \times 10^{-3}, 1.79 \times 10^{-2}]$	$[7.82 \times 10^{-3}, 1.79 \times 10^{-2}]$

independence would lead to underestimating the upper bounds of the 95th quantiles (and, thus, the risk associated to the system) by 2.27, 2.22, and 2.24 times, respectively. These considerations are reflected also by the analysis of the relative average distances $d_{(B_1 \cap_{obj} B_6)^{ukn}}$, $d_{(B_1 \cap_{obj} B_5)^{ukn}}$, and $d_{(B_2 \cap_{obj} B_5)^{ukn}}$ between the upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{obj} B_6)^{ukn}]}$, $\overline{F}^{P[(B_1 \cap_{obj} B_5)^{ukn}]}$, $\overline{F}^{P[(B_2 \cap_{obj} B_5)^{ukn}]}$, $\underline{F}^{P[(B_1 \cap_{obj} B_6)^{ukn}]}$, $\underline{F}^{P[(B_1 \cap_{obj} B_5)^{ukn}]}$, and $\underline{F}^{P[(B_2 \cap_{obj} B_5)^{ukn}]}$, respectively. Actually, as before the assumption

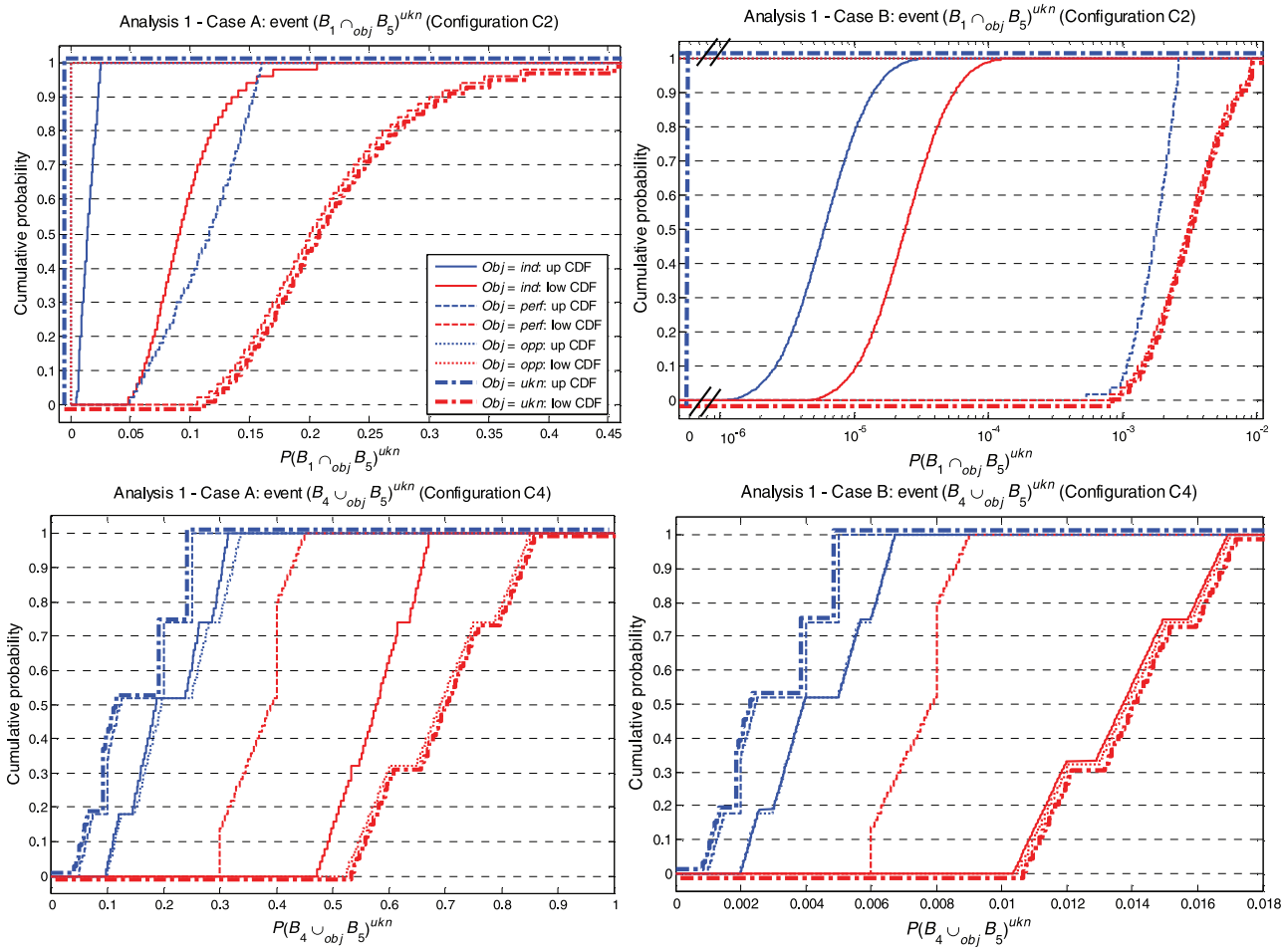


Fig. 6. Upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{obj} B_5)^{ukn}]}$, $\overline{F}^{P[(B_4 \cup_{obj} B_5)^{ukn}]}$, $\underline{F}^{P[(B_1 \cap_{obj} B_5)^{ukn}]}$, and $\underline{F}^{P[(B_4 \cup_{obj} B_5)^{ukn}]}$ obtained for events $(B_1 \cap_{obj} B_5)^{ukn}$ (top panel) and $(B_4 \cup_{obj} B_5)^{ukn}$ (bottom panel), respectively, under the assumptions of independence (solid lines), perfect (dashed lines), opposite (dotted lines), and unknown (dot-dashed lines) objective dependence, with reference to Case A (left-hand side) and B (right-hand side). Top, right-hand side: the value $P[(B_1 \cap_{obj} B_5)^{ukn}] = 0$ in Case B is represented out of scale at about 6×10^{-7} for clarity of illustration.

of independence leads to underestimating the uncertainty (imprecision) "contained" in the distributions of the probabilities $P[(B_1 \cap_{obj} B_6)^{ukn}]$, $P[(B_1 \cap_{obj} B_5)^{ukn}]$, and $P[(B_2 \cap_{obj} B_5)^{ukn}]$ by 4.25, 2.61, and 2.65 times, respectively.

This underestimation is much more significant in Case B. Actually, the values of $\overline{p}^{0.95}_{(B_1 \cap_{obj} B_6)^{ukn}}$, $\overline{p}^{0.95}_{(B_1 \cap_{obj} B_5)^{ukn}}$, and $\overline{p}^{0.95}_{(B_2 \cap_{obj} B_5)^{ukn}}$ are 9.2078×10^{-5}, 6.9995×10^{-5}, and 7.0080×10^{-5}, respectively, under the assumption of independence, whereas they are 8.1876×10^{-3}, 8.8002×10^{-3}, and 7.8810×10^{-3}, respectively, under the assumption of unknown dependence. Thus, the assumption of independence leads to underestimating the upper bounds of the 95th quantiles (and, thus, the risk associated to the system) by 89.02, 125.70, and 112.60 times, respectively. Again, these considerations are reflected by the analysis of the relative average distances $d_{(B_1 \cap_{obj} B_6)^{ukn}}$, $d_{(B_1 \cap_{obj} B_5)^{ukn}}$, and $d_{(B_2 \cap_{obj} B_5)^{ukn}}$. Actually, as before the assumption of independence leads to underestimating the uncertainty (imprecision) associated to the distributions of $P[(B_1 \cap_{obj} B_6)^{ukn}]$, $P[(B_1 \cap_{obj} B_5)^{ukn}]$, and $P[(B_2 \cap_{obj} B_5)^{ukn}]$ by 136.89, 164.80, and 140.99 times, respectively. A visual representation of these results is given in Fig. 6, top panel: actually, it can be seen that the upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{ukn} B_5)^{ukn}]}$ and $\underline{F}^{P[(B_1 \cap_{ukn} B_5)^{ukn}]}$ of $P[(B_1 \cap_{ukn} B_5)^{ukn}]$ (dashed lines) completely envelop the upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{ind} B_5)^{ukn}]}$ and $\underline{F}^{P[(B_1 \cap_{ind} B_5)^{ukn}]}$ of $P[(B_1 \cap_{ind} B_5)^{ukn}]$ (solid lines)

in both Cases A (left-hand side) and B (right-hand side).

The facts that (i) the assumption of objective independence leads to a consistent underestimation of risk and (ii) such underestimation is more dramatic in Case B than in Case A are explained as follows. The probability (chance) of the conjunction of two independent events, say B_1 and B_5, is given by the product of the corresponding probabilities (chances) $P(B_1)$ and $P(B_5)$, that is, $P(B_1 \cap_{ind} B_5) = P(B_1).P(B_5)$ (see Equation (1)): thus, if $P(B_1)$ and $P(B_5)$ are of the order of 10^{-n}, then $P(B_1 \cap_{ind} B_5)$ is of the order of 10^{-2n}. Instead, if no assumption at all about the state of objective dependence between B_1 and B_5 can be made, only (extreme and best possible) lower and upper bounds on $P(B_1 \cap B_5)$ can be computed as $P(B_1 \cap_{ukn} B_5) = [\underline{P}(B_1 \cap_{ukn} B_5), \overline{P}(B_1 \cap_{ukn} B_5)] = [\underline{P}(B_1 \cap_{opp} B_5), \overline{P}(B_1 \cap_{perf} B_5)] = [\max\{P(B_1) + P(B_5) - 1, 0\}, \min\{P(B_1), P(B_5)\}]$ (see Equation (7)). In this case, if $P(B_1)$ and $P(B_5)$ are of the order of 10^{-n}, then the upper bound $\overline{P}(B_1 \cap_{ukn} B_5) = \min\{P(B_1), P(B_5)\}$ (which represents the most conservative estimate of risk) is still of the order of 10^{-n}. As a consequence, $\overline{P}(B_1 \cap_{ukn} B_5) \approx 10^{-n}$ is approximately n orders of magnitude larger than $P(B_1 \cap_{ind} B_5) \approx 10^{-2n}$, which explains also why the difference between $P(B_1 \cap_{ind} B_5)$ and $\overline{P}(B_1 \cap_{ukn} B_5)$ dramatically increases as $P(B_1)$ and $P(B_5)$ decrease (i.e., as n increases).

Different situations arise in the cases where the BEs are linked by OR-gates, that is, $Z = (B_4 \cup_{obj} B_5)^{ukn}$ and $(B_2 \cup_{obj} B_3)^{ukn}$ (Configurations C4 and C5 in Table III). It can be seen that in Case A the values of $\overline{p}^{0.95}_{(B_4 \cup_{obj} B_5)^{ukn}}$ and $\overline{p}^{0.95}_{(B_2 \cup_{obj} B_3)^{ukn}}$ are 0.6670 and 0.6970, respectively, under the assumption of independence, whereas they are 0.8401 and 0.8941, respectively, under the assumption of unknown dependence. Thus, the assumption of independence leads to underestimating the upper bounds of the 95th quantiles (and, thus, the risk associated to the system) by about 1.26 and 1.28 times, respectively. These considerations are reflected also by the values of the relative average distances $d_{(B_4 \cup_{obj} B_5)^{ukn}}$ and $d_{(B_2 \cup_{obj} B_3)^{ukn}}$ between the upper and lower CDFs $\overline{F}^{P[(B_4 \cup_{obj} B_5)^{ukn}]}$, $\overline{F}^{P[(B_2 \cup_{obj} B_3)^{ukn}]}$, $\underline{F}^{P[(B_4 \cup_{obj} B_5)^{ukn}]}$, and $\underline{F}^{P[(B_2 \cup_{obj} B_3)^{ukn}]}$, respectively. Actually, as before, the assumption of independence leads to underestimating the uncertainty (imprecision) "contained" in the distributions of $P[(B_4 \cup_{obj} B_5)^{ukn}]$ and $P[(B_2 \cup_{obj} B_3)^{ukn}]$ by 1.45 and 1.85 times. Notice that the magnitude of such underestimations is not negligible, but it is much less relevant than for the cases where BEs are linked by AND-gates.

In Case B, the values of $\overline{p}^{0.95}_{(B_4 \cup_{obj} B_5)^{ukn}}$ and $\overline{p}^{0.95}_{(B_2 \cup_{obj} B_3)^{ukn}}$ are 1.6685×10^{-2} and 1.7772×10^{-2}, respectively, under the assumption of independence, whereas they are 1.6763×10^{-2} and 1.7881×10^{-2}, respectively, under the assumption of unknown dependence. Thus, in this case the assumption of independence leads to a very slight underestimation of the upper bounds of the 95th quantiles (and, thus, of the risk associated to the system), that is, only by about 1.01 and 1.02 times, respectively. Instead, the values of the relative average distances $d_{(B_4 \cup_{obj} B_5)^{ukn}}$ and $d_{(B_2 \cup_{obj} B_3)^{ukn}}$ are 1.0216 and 0.6381, respectively, under the assumption of independence, whereas they are 1.1676 and 0.8076, respectively, under the assumption of unknown dependence: in other words, the uncertainty (imprecision) associated to distributions of $P[(B_4 \cup_{obj} B_5)^{ukn}]$ and $P[(B_2 \cup_{obj} B_3)^{ukn}]$ is underestimated by about 1.14 and 1.27 times. Thus, although the risk estimates are comparable, the underestimation of the uncertainty (imprecision) associated to the distributions of $P[(B_4 \cup_{obj} B_5)^{ukn}]$ and $P[(B_2 \cup_{obj} B_3)^{ukn}]$ is not negligible. A visual representation of these results is given in Fig. 6, bottom right-hand side. Actually, it can be seen that the lower CDFs $\underline{F}^{P[(B_4 \cup_{ukn} B_5)^{ukn}]}$ (dashed line) and $\underline{F}^{P[(B_4 \cup_{ind} B_5)^{ukn}]}$ (solid line) (i.e., the CDFs used to estimate the upper bounds of the 95th quantiles of $P[(B_4 \cup_{ukn} B_5)^{ukn}]$ and $P[(B_4 \cup_{ind} B_5)^{ukn}]$, respectively) almost coincide; on the contrary, the upper CDF $\overline{F}^{P[(B_4 \cup_{ukn} B_5)^{ukn}]}$ (dashed line) lies consistently above the upper CDF $\overline{F}^{P[(B_4 \cup_{ind} B_5)^{ukn}]}$ (solid line).

These results are explained as follows. The probability (chance) of the disjunction of two independent events, say B_4 and B_5, is given by $P(B_4 \cup_{ind} B_5) = P(B_4) + P(B_5) - P(B_4).P(B_5)$ (see Equation (2)). Instead, if no assumptions at all about the state of objective dependence between B_4 and B_5 can be made, only (extreme and best possible) lower and upper bounds on $P(B_4 \cup B_5)$ can be computed as $P(B_4 \cup_{ukn} B_5) = [\underline{P}(B_4 \cup_{ukn} B_5), \overline{P}(B_4 \cup_{ukn} B_5)] = [\underline{P}(B_4 \cup_{perf} B_5), \overline{P}(B_4 \cup_{opp} B_5)] = [\max\{P(B_4), P(B_5)\}, \min\{1, P(B_4) + P(B_5)\}]$ (see Equation (8)). If both $P(B_4)$ and $P(B_5)$ are of the order of 10^{-n} (with $n \gg 1$, like in the present Case B), then $P(B_4 \cup_{ind} B_5) = P(B_4) + P(B_5) - P(B_4) \times P(B_5) \approx P(B_4) + P(B_5) = 2 \times 10^{-n}$. In addition, it is evident that $P(B_4 \cup_{ukn} B_5) =$

$[\max\{P(B_4), P(B_5)\}, \min\{1, P(B_4) + P(B_5)\}] \approx [10^{-n}, 2 \times 10^{-n}]$. This means that if both $P(B_4)$ and $P(B_5)$ are quite small (i.e., if $n >> 1$), then the value of $P(B_4 \cup_{ind} B_5)$ is comparable to that of $\overline{P}(B_4 \cup_{ukn} B_5)$, that is, $P(B_4 \cup_{ind} B_5) \approx \overline{P}(B_4 \cup_{ukn} B_5) \approx 2 \times 10^{-n}$: in other words, two radically different assumptions about the state of objective dependence between B_4 and B_5 provide a comparable risk estimate. On the contrary, the uncertainty (imprecision) "contained" in the distributions of $P(B_4 \cup_{ind} B_5)$ and $P(B_4 \cup_{ukn} B_5)$ is obviously quite different: actually, the interval $P(B_4 \cup_{ukn} B_5) \approx [10^{-n}, 2 \times 10^{-n}]$ "completely envelops" the estimate $P(B_4 \cup_{ind} B_5) \approx 2 \times 10^{-n}$.

Similar analyses are performed on the probability (chance) $P(X)$ of the TE X of the FT in Fig. 4. Table V reports the values of the indicators $[\underline{p}_X^{0.95}, \overline{p}_X^{0.95}]$ (19) and d_X (20) obtained for $P(X)$ under different assumptions of objective dependence between the BEs (Configurations T1–T4 in Table III), with reference to Case B; the estimates for $E[P(X)^{INS}]$ are also shown for completeness. For illustration purposes, Fig. 7 depicts the upper and lower CDFs $\overline{F}^{P(X)}$ and $\underline{F}^{P(X)}$ obtained for $P(X)$ under different assumptions of objective dependence between the BEs (Configurations T1–T4 in Table III).

These results confirm the considerations drawn by the analysis of the simple Configurations C1–C5 in Table III. For example, it can be seen that the values of the upper bound $\overline{p}_X^{0.95}$ on the 95th quantile $P(X)^{0.95}$ are 7.2275×10^{-4} and 8.9766×10^{-3} in Configurations T1 (where all the BEs are considered independent) and T2 (where BEs B_1 and B_6 are considered positively dependent). This means that neglecting a hypothetical state of positive dependence between only one pair of BEs linked by an AND-gate is sufficient for underestimating the upper bound $\overline{p}_X^{0.95}$ of the 95th quantile $P(X)^{0.95}$ (and, thus, the risk associated to the system) by 12.42 times. On the contrary, in Configuration T3 (where no indication at all about the state of objective dependence between BEs B_4 and B_5 is available), the value of $\overline{p}_X^{0.95}$ is 7.7580×10^{-4}: thus, in this case *even* assuming unknown objective dependence between a couple of BEs linked by an OR-gate leads to overestimating the risk associated to the system only by about 1.07 times with respect to the "baseline" assumption of independence. Finally, Configuration T4 represents the "extreme" case where unknown objective dependence is assumed between all the BEs of the FT: notice that since in the present Analysis 1 unknown epistemic dependence is also assumed between the probabilities (chances) of all the BEs, Configuration T4 provides the most "uncertain" and, thus, conservative estimate for $P(X)$. Actually, the values of $\overline{p}_X^{0.95}$ and d_X are 2.5923×10^{-2} and 72.7040, respectively, that is, 35.87 and 44.14 times larger than those obtained under the "baseline" assumption of objective independence between all the BEs (Configuration T1).

Some considerations are in order with respect to the results obtained. It has been shown that the assumption of objective independence between BEs linked by AND-gates very often leads to a significant underestimation of (i) the risk associated to the system (here represented by the upper bound $\overline{p}_X^{0.95}$ of the 95th quantile $P(X)^{0.95}$ of $P(X)$) and (ii) the uncertainty (imprecision) "contained" in the distribution of $P(X)$ (here represented by the relative average distance d_X between the upper and lower CDFs $\overline{F}^{P(X)}$ and $\underline{F}^{P(X)}$ of the TE probability-chance $P(X)$). In more detail, it can be seen that when the BE probabilities (chances) are of the order of 10^{-1} (like in the present Case A), the assumption of objective independence leads to underestimating risk and uncertainty by 2.22–2.27 times and 2.61–4.21 times, respectively, with respect to the assumption of unknown objective dependence. Instead, if the BE probabilities (chances) are of the order of 10^{-2}–10^{-3} (like in the present Case B), the assumption of objective independence leads to underestimating risk and uncertainty by 89–125 times and 136–164 times, respectively, with respect to the assumption of unknown objective dependence. Thus, the effects of objective dependences between BEs linked by AND-gates becomes more and more dramatic as the BE probabilities (chances) decrease: this poses serious concerns in the risk assessment of complex systems where the components are highly reliable and, thus, characterized by very small failure probabilities (chances).

Instead, it has been shown that the assumption of objective independence between BEs linked by OR-gates leads to a slight underestimation of both risk and uncertainty. In particular, it can be seen that when the BE probabilities (chances) are of the order of 10^{-1} (like in the present Case A), the assumption of objective independence leads to underestimating risk and uncertainty by 1.26–1.28 times and 1.45–1.85 times, respectively, with respect to the assumption of unknown objective dependence. Instead, if the BE probabilities (chances) are of the

Table V. Values of the Indicators $[\underline{p}_X^{0.95}, \overline{p}_X^{0.95}]$ (19) and d_X (20) obtained for $P(X)$ Under Different Assumptions of Objective Dependence Between the BEs (Configurations T1–T4 in Table III), with Reference to Case B; the Estimates for $E[P(X)^{INS}]$ Are Also Reported

Analysis 1 – Unknown epistemic dependence between the probabilities (chances) of the BEs Case B

Top Event (TE) X (configuration, Table III)	Indicators		
	$E[P(X)^{INS}]$	$\mathbf{d_X}$	$[\underline{\mathbf{p}}_{\mathbf{X}}^{0.95}, \overline{\mathbf{p}}_{\mathbf{X}}^{0.95}]$
$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{ukn}$ (T1)	2.8725×10^{-4}	1.6472	$[7.3617 \times 10^{-5}, 7.2275 \times 10^{-4}]$
Positive (*pos*) objective dependence between B_1 and B_6 (T2)	2.2574×10^{-3}	15.3945	$[6.5629 \times 10^{-5}, 8.9766 \times 10^{-3}]$
$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ukn} B_5 \cup_{ind} B_6)]^{ukn}$ (T3)	2.8998×10^{-4}	1.7324	$[6.1237 \times 10^{-5}, 7.7580 \times 10^{-4}]$
$X = [(B_1 \cup_{ukn} B_2 \cup_{ukn} B_3) \cap_{ukn} (B_4 \cup_{ukn} B_5 \cup_{ukn} B_6)]^{ukn}$ (T4)	1.0463×10^{-2}	72.7040	$[3.5735 \times 10^{-5}, 2.5923 \times 10^{-2}]$

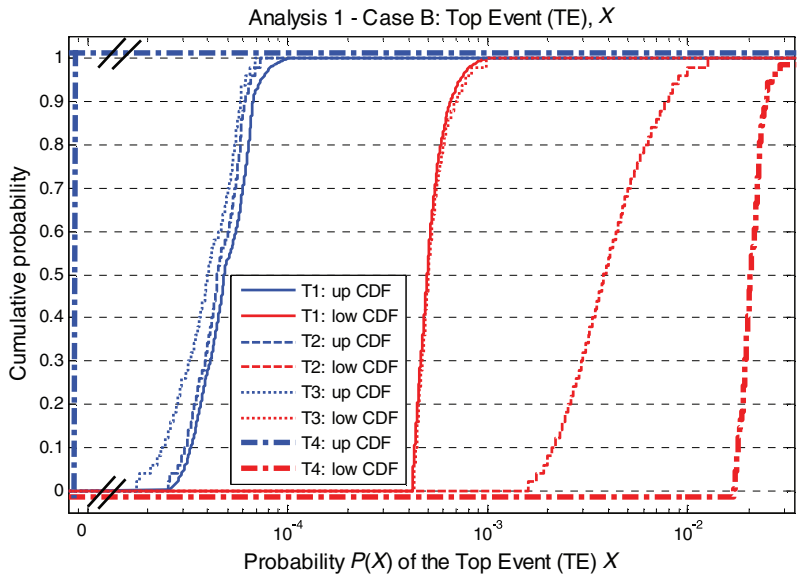


Fig. 7. Upper and lower CDFs $\overline{F}^{P(X)}$ and $\underline{F}^{P(X)}$ obtained for $P(X)$, with reference to Case B under different assumptions of objective dependence between the BEs (Configurations T1–T4 in Table III). The value $P(X) = 0$ is represented out of scale at about 1×10^{-5} for clarity of illustration.

order of 10^{-2}–10^{-3} (like in the present Case B), the assumption of objective independence does not lead to a remarkable underestimation of risk, whereas it causes a nonnegligible underestimation of uncertainty (i.e., by 1.14–1.27 times with respect to the assumption of unknown objective dependence). Based on these considerations, it can be concluded that (i) the assumption of objective independence between BEs linked by OR-gates leads to a slight underestimation of risk only when the BE probabilities (chances) are relatively large (e.g., of the order of 10^{-1}) and (ii) the relevance of the underestimation of uncertainty does not change dramatically as the BE probabilities (chances) change. These considerations makes the treatment of dependences between BEs linked by OR-gates much less critical than for AND-gates.

4.2 Studying the Effects of State-of-Knowledge (Epistemic) Dependences Between the Probabilities (Chances) of the Basic Events

Table VI reports the values of the indicators $[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$ (19) and d_Z (20) obtained for the events $Z = (B_1 \cap_{\text{ind}} B_6)^{\text{epi}}$, $(B_1 \cap_{ind} B_5)^{epi}$, $(B_2 \cap_{ind} B_5)^{epi}$, $(B_4 \cup_{ind} B_5)^{epi}$ and $(B_2 \cup_{ind} B_3)^{epi}$ (Configurations C1–C5 of Analysis 2 in Table III) under the assumptions of independence ("*epi*" = "*ind*"), perfect ("*epi*" = "*perf*"), and unknown ("*epi*" = "*ukn*") epistemic dependence, with reference to Cases A and B; the estimates for $E[P(Z)^{INS}]$ are also reported for completeness. In addition, only for illustration purposes, Fig. 8 shows the upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{ind} B_5)^{epi}]}$, $\overline{F}^{P[(B_4 \cup_{ind} B_5)^{epi}]}$, $\underline{F}^{P[(B_1 \cap_{ind} B_5)^{epi}]}$, and $\underline{F}^{P[(B_4 \cup_{ind} B_5)^{epi}]}$ obtained for events $(B_1 \cap_{ind} B_5)^{epi}$

Table VI. Values of the Indicators $[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$ (19) and d_Z (20) Obtained for Events $Z = (B_1 \cap_{ind} B_6)^{epi}$, $(B_1 \cap_{ind} B_5)^{epi}$, $(B_2 \cap_{ind} B_5)^{epi}$, $(B_4 \cup_{ind} B_5)^{epi}$, and $(B_2 \cup_{ind} B_3)^{epi}$ (Configurations C1–C5 of Analysis 2 in Table III) Under the Assumptions of Independence, Perfect, and Unknown Epistemic Dependence, with Reference to Cases A and B

Analysis 2 – Objective independence (*ind*) between the BEs				
		State of epistemic (*epi*) dependence		
Event Z	**Indicators**	**Independence (*ind*)**	**Perfect (*perf*)**	**Unknown (*ukn*)**
		Case A		
$(B_1 \cap_{ind} B_6)^{epi}$ **(C1)**	$E[P(Z)^{INS}]$	0.0543	0.0576	0.0583
	d_Z	0	0	0.9270
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	0.0974	0.1230	[0.0492, 0.1528]
$(B_1 \cap_{ind} B_5)^{epi}$ **(C2)**	$E[P(Z)^{INS}]$	0.0474	0.0510	0.0553
	d_Z	0.8993	0.9389	1.7242
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.0503, 0.1216]	[0.0634, 0.1467]	[0.0243, 0.1557]
$(B_2 \cap_{ind} B_5)^{epi}$ **(C3)**	$E[P(Z)^{INS}]$	0.0609	0.0622	0.0715
	d_Z	1.4874	1.5152	1.9523
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.0254, 0.1551]	[0.0283, 0.1717]	[0.0188, 0.1760]
$(B_4 \cup_{ind} B_5)^{epi}$ **(C4)**	$E[P(Z)^{INS}]$	0.3817	0.3740	0.3933
	d_Z	0.6510	0.6393	0.9608
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.3786, 0.6423]	[0.3933, 0.6618]	[0.3100, 0.6670]
$(B_2 \cup_{ind} B_3)^{epi}$ **(C5)**	$E[P(Z)^{INS}]$	0.5192	0.5178	0.5272
	d_Z	0.4239	0.4229	0.5241
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	[0.4707, 0.6798]	[0.4813, 0.6932]	[0.4519, 0.6970]
		Case B		
$(B_1 \cap_{ind} B_6)^{epi}$ **(C1)**	$E[P(Z)^{INS}]$	1.62×10^{-5}	2.01×10^{-5}	2.01×10^{-5}
	d_Z	0	0	1.6603
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	4.36×10^{-5}	6.72×10^{-5}	$[1.41 \times 10^{-5}, 9.21 \times 10^{-5}]$
$(B_1 \cap_{ind} B_5)^{epi}$ **(C2)**	$E[P(Z)^{INS}]$	1.69×10^{-5}	1.96×10^{-5}	1.85×10^{-5}
	d_Z	0.9112	0.9943	1.3109
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[2.38 \times 10^{-5}, 6.09 \times 10^{-5}]$	$[3.45 \times 10^{-5}, 7.85 \times 10^{-5}]$	$[8.75 \times 10^{-6}, 7.88 \times 10^{-5}]$
$(B_2 \cap_{ind} B_5)^{epi}$ **(C3)**	$E[\overline{P}(Z)^{INS}]$	2.43×10^{-5}	2.49×10^{-5}	2.62×10^{-5}
	d_Z	1.4878	1.5251	1.8371
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[1.01 \times 10^{-5}, 6.19 \times 10^{-5}]$	$[1.13 \times 10^{-5}, 6.87 \times 10^{-5}]$	$[5.68 \times 10^{-6}, 7.01 \times 10^{-5}]$
$(B_4 \cup_{ind} B_5)^{epi}$ **(C4)**	$E[P(Z)^{INS}]$	8.69×10^{-3}	8.65×10^{-3}	8.93×10^{-3}
	d_Z	0.7266	0.7237	1.0499
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[8.38 \times 10^{-3}, 1.59 \times 10^{-2}]$	$[8.82 \times 10^{-3}, 1.67 \times 10^{-2}]$	$[6.59 \times 10^{-3}, 1.67 \times 10^{-2}]$
$(B_2 \cup_{ind} B_3)^{epi}$ **(C5)**	$E[P(Z)^{INS}]$	1.22×10^{-2}	1.22×10^{-2}	1.25×10^{-2}
	d_Z	0.5289	0.5298	0.6502
	$[\underline{p}_Z^{0.95}, \overline{p}_Z^{0.95}]$	$[1.05 \times 10^{-2}, 1.72 \times 10^{-2}]$	$[1.07 \times 10^{-2}, 1.76 \times 10^{-2}]$	$[9.83 \times 10^{-3}, 1.78 \times 10^{-2}]$

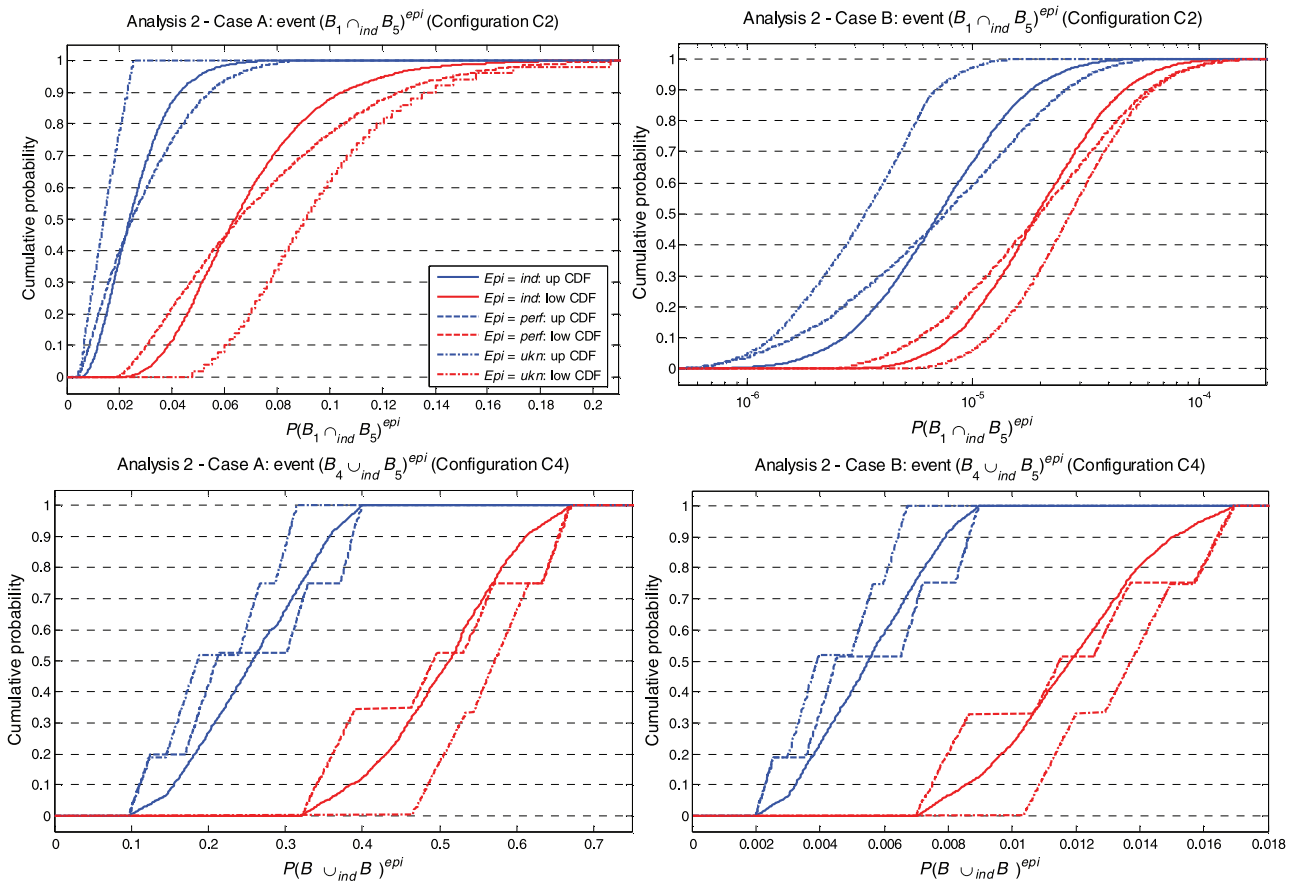


Fig. 8. Upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{ind} B_5)^{epi}]}$, $\overline{F}^{P[(B_4 \cup_{ind} B_5)^{epi}]}$, $\underline{F}^{P[(B_1 \cap_{ind} B_5)^{epi}]}$, and $\underline{F}^{P[(B_4 \cup_{ind} B_5)^{epi}]}$ obtained for events $(B_1 \cap_{ind} B_5)^{epi}$ (top panel) and $(B_4 \cup_{ind} B_5)^{epi}$ (bottom panel), respectively, under the assumptions of independence (solid lines), perfect (dashed lines), and unknown (dot-dashed lines) epistemic dependence, with reference to Cases A (left-hand side) and B (right-hand side).

(top panel) and $(B_4 \cup_{ind} B_5)^{epi}$ (bottom panel), respectively, under the assumptions of independence (solid lines), perfect (dashed lines), and unknown (dot-dashed lines) epistemic dependence, with reference to Cases A (left-hand side) and B (right-hand side).

We start by analyzing the cases where the BEs are linked by AND-gates and we refer only to event $Z = (B_1 \cap_{ind} B_5)^{epi}$ (C2) for brevity sake. It can be seen that in Case A the values of the upper bound $\overline{p}^{0.95}_{(B_1 \cap_{ind} B_5)^{epi}}$ of the 95th percentile $P[(B_1 \cap_{ind} B_5)^{epi}]^{0.95}$ are 0.1216, 0.1467, and 0.1557 under the assumptions of independence, total (perfect) and unknown epistemic dependence, respectively. Thus, the assumption of epistemic independence would lead to underestimating the upper bound of the 95th quantile (and, thus, the risk associated to the system) by 1.21 and 1.28 times with respect to the assumptions of total and unknown epistemic dependence, respectively; in addition, notice that the assumption of perfect dependence produces estimates of the upper bound of the 95th quantile that are comparable to those obtained under the assumption of unknown dependence. These considerations are reflected also by the analysis of the values of the relative average distance $d_{(B_1 \cap_{ind} B_5)^{epi}}$ between the upper and lower CDFs $\overline{F}^{P[(B_1 \cap_{ind} B_5)^{epi}]}$ and $\underline{F}^{P[(B_1 \cap_{ind} B_5)^{epi}]}$. Actually, as before the assumption of epistemic independence leads to underestimating the uncertainty (imprecision) "contained" in the distribution of $P[(B_1 \cap_{ind} B_5)^{epi}]$ by about 1.04 and 1.92 times with respect to the assumptions of perfect and unknown epistemic dependence, respectively. Similar considerations can be drawn from the analyses of events $(B_1 \cap_{ind} B_6)^{epi}$ and $(B_2 \cap_{ind} B_5)^{epi}$.

No significant differences can be found here between the results obtained in Cases A and B. For example, in Case B, the assumption of epistemic

independence leads to underestimating the upper bounds of the 95th quantiles (and, thus, the risk associated to the system) by 1.287 and 1.290 times with respect to the assumptions of total and unknown epistemic dependence, respectively; in addition, the estimates produced by the assumptions of total and unknown epistemic dependence are almost identical as before.

Very similar considerations (and results) can be drawn by the analysis of those cases where the BEs are linked by OR-gates, that is, $Z = (B_4 \cup_{ind} B_5)^{epi}$ and $(B_2 \cup_{ind} B_3)^{epi}$ (Configurations C4 and C5 in Table III) in both Cases A and B: thus, we analyze only event $(B_4 \cup_{ind} B_5)^{epi}$ with reference to Case A for brevity. It can be seen that the assumption of independence leads to underestimating the upper bounds of the 95th quantiles (and, thus, the risk associated to the system) by 1.03 and 1.04 times with respect to the assumptions of total and unknown dependence, respectively.

These results are pictorially confirmed by Fig. 8: actually, it can be seen that the upper and lower CDFs of $P[(B_1 \cap_{ind} B_5)^{epi}]$ (top panel) and $P[(B_4 \cup_{ind} B_5)^{epi}]$ (bottom panel) obtained under the assumption of unknown epistemic dependence (dot-dashed lines) completely envelop those obtained under the assumptions of independence (solid lines) and perfect dependence (dashed lines) in both Cases A (left-hand side) and B (right-hand side) (i.e., they obviously represent more conservative estimates of the bounding distributions). In addition, it is worth noting that the lower (resp., upper) CDFs obtained under the assumption of perfect epistemic dependence, i.e., $\underline{F}^{P[(B_1 \cap_{ind} B_5)^{perf}]}$ and $\underline{F}^{P[(B_4 \cup_{ind} B_5)^{perf}]}$ (resp., $\overline{F}^{P[(B_1 \cap_{ind} B_5)^{perf}]}$ and $\overline{F}^{P[(B_4 \cup_{ind} B_5)^{perf}]}$), are very close to those produced by the assumption of unknown epistemic dependence, that is, $\underline{F}^{P[(B_1 \cap_{ind} B_5)^{ukn}]}$ and $\underline{F}^{P[(B_4 \cup_{ind} B_5)^{ukn}]}$ (resp., $\overline{F}^{P[(B_1 \cap_{ind} B_5)^{ukn}]}$ and $\overline{F}^{P[(B_4 \cup_{ind} B_5)^{ukn}]}$) in the region where the cumulative probability is very close to the "extreme" upper bound 1 (resp., lower bound 0). In other words, the CDFs produced under assumptions of perfect and unknown epistemic dependence are almost identical in the range of extreme probabilities-chances (i.e., extreme quantiles) that are of particular interest in the risk assessment of complex, highly reliable systems.

Similar analyses were performed on $P(X)$. Table VII reports the values of the indicators $[\underline{p}_X^{0.95}, \overline{p}_X^{0.95}]$ (19) and d_X (20) obtained for $P(X)$ under different assumptions of epistemic dependence between the probabilities (chances) of the BEs (Configurations T1–T3 of Analysis 2 in Table III), with reference to Case B; the estimates for $E[P(X)^{INS}]$ are also shown for completeness. For illustration purposes, Fig. 9 depicts the upper and lower CDFs $\overline{F}^{P(X)}$ and $\underline{F}^{P(X)}$ obtained for $P(X)$ assuming independence (solid lines), perfect (dashed lines), and unknown (dot-dashed lines) epistemic dependence between the probabilities (chances) of all the BEs (Configurations T1–T3 of Analysis 2 in Table III).

It can be seen that the values of the upper bound $\overline{p}_X^{0.95}$ of the 95th percentile $P(X)^{0.95}$ are 4.4030×10^{-4}, 6.4111×10^{-4}, and 7.2275×10^{-4} under the assumptions of independence, total dependence, and unknown dependence, respectively. Thus, the assumption of independence would lead to underestimating the upper bound of the 95th quantile (and, thus, the risk associated to the system) by 1.456 and 1.641 times with respect to the assumptions of total and unknown dependence, respectively. This is reflected by the analysis of the indicator d_X: the assumption of epistemic independence leads to underestimating d_X by 1.02 and 2.56 times, with respect to the assumptions of total and unknown epistemic dependence.

Some considerations are in order with respect to the results obtained. It has been shown that the assumption of epistemic independence between the probabilities (chances) of BEs linked by AND-gates very often leads to an underestimation of (i) the risk associated to the system (here represented by the upper bound of the 95th quantile of the TE probability-chance) and (ii) the "imprecision" contained in the distribution of the TE probability-chance (here represented by the relative average distance between the upper and lower CDFs of the TE probability-chance). In particular, in the analysis of Configurations C1–C5 it is shown that when the BE probabilities (chances) are of the order of 10^{-1} (like in the present Case A), the assumption of epistemic independence leads to underestimating risk and uncertainty by 1.11–1.57 times and 1.02–1.92 times, respectively, with respect to the assumptions of total and unknown epistemic dependence. Similarly, if the BE probabilities (chances) are of the order of 10^{-2}–10^{-3} (like in the present Case B), the assumption of epistemic independence leads to underestimating risk and uncertainty by 1.11–2.10 times

Table VII. Values of the Indicators $[\underline{p}_X^{0.95}, \overline{p}_X^{0.95}]$ (19) and d_X (20) Obtained for $P(X)$ Under the Assumptions of Independence, Perfect, and Unknown Epistemic Dependence (Configurations T1–T3 of Analysis 2 in Table III), with Reference to Cases A and B

Analysis 2 – Objective independence (*ind*) between the BEs Case B			
		Indicators	
Top Event (TE) X (configuration, Table III)	$E[P(X)^{INS}]$	d_X	$[\underline{p}_X^{0.95}, \overline{p}_X^{0.95}]$
$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{ind}$ (T1)	2.1571×10^{-4}	0.8576	$[1.9821 \times 10^{-4}, 4.4030 \times 10^{-4}]$
$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{perf}$ (T2)	2.3119×10^{-4}	0.8781	$[3.1555 \times 10^{-4}, 6.4111 \times 10^{-4}]$
$X = [(B_1 \cup_{ind} B_2 \cup_{ind} B_3) \cap_{ind} (B_4 \cup_{ind} B_5 \cup_{ind} B_6)]^{ukn}$ (T3)	2.8725×10^{-4}	2.1935	$[7.3617 \times 10^{-5}, 7.2275 \times 10^{-4}]$

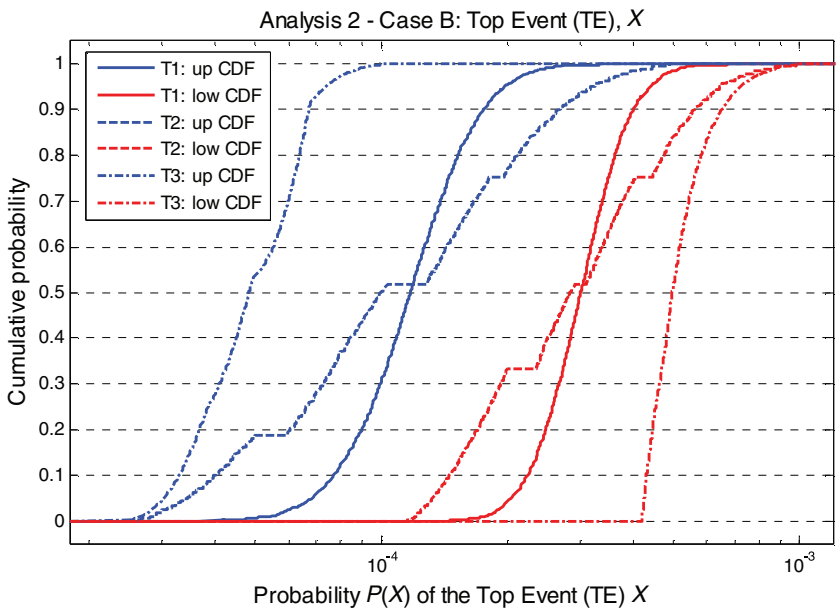


Fig. 9. Upper and lower CDFs $\overline{F}^{P(X)}$ and $\underline{F}^{P(X)}$ obtained for $P(X)$ under the assumptions of independence (solid lines), perfect (dashed lines), and unknown (dot-dashed lines) epistemic dependence (Configurations T1–T3 of Analysis 2 in Table III), with reference to Case B.

and 1.03–1.44 times, respectively, with respect to the assumptions of total and unknown epistemic dependence.

Similar results are obtained for BEs linked by OR-gates. In particular, it can be seen that when the BE probabilities (chances) are of the order of 10^{-1} (like in the present Case A), the assumption of independence leads to underestimating risk and uncertainty by 1.02–1.04 times and 1.01–1.48 times, respectively, with respect to the assumptions of total and unknown epistemic dependence. If the BE probabilities (chances) are of the order of 10^{-2}–10^{-3} (like in the present Case B), the assumption of epistemic independence leads to underestimating risk and uncertainty by 1.025–1.05 times and 1.01–1.44 times, respectively, with respect to the assumptions of total and unknown epistemic dependence.

Finally, in the analysis of the probability (chance) of the TE of the FT in Fig. 4 it is shown that assuming epistemic independence between the probabilities (chances) of all the BEs leads to underestimating risk and uncertainty by 1.456–1.641 and 1.02–2.56 times, respectively, with respect to the assumptions of total and unknown epistemic dependence. A final remark is in order with respect to the fact that in all the cases considered, the 95th quantile estimates produced under the assumption of perfect dependence are comparable to those obtained under the hypothesis of unknown dependence.

On the basis of these considerations, it can be concluded that (i) the effects of epistemic dependence are in general nonnegligible (in particular, in the estimation of small probabilities-chances and extreme quantiles), but they are quantitatively less

relevant and critical than those of objective dependence (see Section 4.1); (ii) the effects of epistemic dependence are not influenced dramatically by the type of logical connection existing between the BEs, and (iii) the effects of epistemic dependence are not modified significantly by the magnitude of the BE probabilities (chances). These considerations demonstrate that epistemic dependences cannot be neglected in the risk assessment of complex, safety-critical engineering systems (in particular, when small probabilities-chances and extreme quantiles have to be estimated); however, their effects are likely to be overwhelmed by those of objective dependences (if present).

5. DISCUSSION AND CONCLUSIONS

In this article, the effects of objective and state-of-knowledge dependences between the BEs of a FT have been quantified. Two types of analyses have been carried out on a FT with six BEs:

1. assuming unknown epistemic dependence between the probabilities (chances) of the BEs, the effects of different states of objective dependence between the BEs have been quantified;
2. assuming objective independence between the BEs, the effects of different states of epistemic dependence between the probabilities (chances) of the BEs have been studied.

With respect to analysis 1 above, it has been shown that:

- the assumption of objective independence between the BEs linked by AND-gates always leads to a serious underestimation of (i) the risk associated to the system (here represented by the upper bound of the 95th quantile of the TE probability-chance) and (ii) the uncertainty (imprecision) "contained" in the (distribution of the) TE probability-chance (here represented by the relative average distance between the upper and lower CDFs of the TE probability-chance) with respect to the assumptions of perfect and unknown objective dependence: actually, the corresponding estimates may differ even by several orders of magnitude;
- this underestimation becomes more and more dramatic as the BE probabilities (chances) get smaller: this poses serious concerns in the risk assessment of complex systems where the components are highly reliable and, thus, characterized by very small failure probabilities (chances);
- the assumption of objective independence between BEs linked by OR-gates may lead to a *slight* underestimation of both risk and the uncertainty. In particular:
  - the assumption of objective independence between BEs leads to a slight underestimation of risk only when the BE probabilities (chances) are relatively large (e.g., of the order of 10^{-1}); otherwise, when the BE probabilities (chances) are quite small (e.g., of the order of 10^{-2}–10^{-3}), the assumption of independence produces risk estimates that are comparable even to those provided by the assumption of unknown dependence;
  - the assumption of objective independence between BEs always leads to a slight underestimation of the uncertainty (imprecision) "contained" in the distribution of the TE probability (chance);
  - the effects of objective dependence between BEs linked by OR-gates are not influenced dramatically by the magnitude of the BE probabilities (chances).

Based on the considerations above, it can be concluded that:

- the treatment of objective dependences between BEs linked by AND-gates is much more critical than for OR-gates;
- unknown (or, at least, perfect) objective dependence should be assumed between BEs linked by AND-gates, in particular if the corresponding probabilities (chances) are very small (e.g., of the order of 10^{-3}–10^{-2}): this leads to obtaining conservative risk estimates;
- objective dependences between BEs linked by OR-gates can be in general neglected if the corresponding probabilities (chances) are very small (e.g., around 10^{-3}–10^{-2}).

With respect to analysis 2 above, it has been shown that:

- the assumption of epistemic independence between the probabilities (chances) of the BEs leads to a nonnegligible underestimation of the risk associated to the system (here represented by the upper bound of the 95th quantile of the TE probability-chance) with respect to the

assumptions of perfect and unknown epistemic dependence: this is particularly evident in the estimation of small probabilities (chances) and extreme quantiles that are of paramount importance in the risk assessment of complex, highly reliable systems;

- the estimates for the upper bound of the 95th quantile of the TE probability (chance) produced by the assumptions of perfect and unknown epistemic dependence are *comparable*;
- the effects of epistemic dependence between the BE probabilities (chances) are quantitatively less relevant and critical than those of objective dependence between the BEs: they may differ by several orders of magnitude;
- the effects of epistemic dependence are not modified significantly by the magnitude of the BE probabilities (chances);
- the effects of epistemic dependence are not influenced dramatically by the type of logical connection existing between the BEs.

Based on the considerations above, it can be concluded that:

- the conditions of epistemic dependence between some BE probabilities (chances) should not be neglected when small probabilities (chances) and extreme quantiles have to be estimated: with respect to that, unknown (or, at least, perfect) epistemic dependences should be assumed in order to obtain conservative risk estimates;
- if objective dependences are also present (e.g., between BEs linked by AND-gates and characterized by very small probabilities-chances), the effects of epistemic dependence are likely to be overwhelmed by those of objective dependence.

ACKNOWLEDGMENTS

The authors are grateful to the two anonymous reviewers for their useful comments and suggestions, which have allowed improving the article.

REFERENCES

1. Henley EJ, Kumamoto H. Probabilistic Risk Assessment. New York: IEEE Press, 1992.
2. USNRC. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. NUREG-1855, Washington, DC: US Nuclear Regulatory Commission, 2009.
3. NASA. Risk-Informed Decision Making Handbook. NASA/SP-2010-576—Version 1.0. Washington, DC: Office of Safety and Mission Assurance, NASA Headquarters, 2010.
4. Epstein S, Rauzy A. Can we trust PRA? Reliability Engineering & System Safety, 2005; 88(3):195–205.
5. Cepin M. Analysis of truncation limit in probabilistic safety assessment. Reliability Engineering & System Safety, 2005; 87(3):395–403.
6. Lindley DV, Singpurwalla ND. Reliability (and fault tree) analysis using expert opinions. Journal of the American Statistical Association, 1986; 81(393):87–90.
7. Apostolakis GE. The concept of probability in safety assessment of technological systems. Science, 1990; 250(4986):1359–1364.
8. Aven T. Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective. Chichester: Wiley, 2003.
9. Helton JC, Oberkampf W. Alternative representations of epistemic uncertainties. Reliability Engineering and System Safety, 2004; 85(1–3):1–10.
10. Limbourg P, de Rocquigny E. Uncertainty analysis using evidence theory – Confronting level-1 and level-2 approaches with data availability and computational constraints, Reliability Engineering and System Safety, 2010; 95(5):550–564.
11. Apostolakis GE, Kaplan S. Pitfalls in risk calculations. Reliability Engineering, 1981; 2(2):135–145.
12. Huang D, Chen T, Wang MJ. A fuzzy set approach for event tree analysis. Fuzzy Sets and Systems, 2001; 118:153–165.
13. NUREG-CR-6850. EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology. US Nuclear Regulatory Commission, 2005.
14. USNRC. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis. NUREG-1.174 – Revision 1, Washington, DC: US Nuclear Regulatory Commission, 2002.
15. Aven T. On the need for restricting the probabilistic analysis in risk assessments to variability. Risk Analysis, 2010; 30(3):354–360.
16. Aven T. Interpretations of alternative uncertainty representations in a reliability and risk analysis context. Reliability Engineering & System Safety, 2011; 96(3):353–360.
17. Aven T, Steen R. The concept of ignorance in a risk assessment and risk management context. Reliability Engineering and System Safety, 2010; 95(11):1117–1122.
18. Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliability Engineering and System Safety, 2010; 96(1): 64–74.
19. Ferson S, Ginzburg L, Akcakaya R. Whereof one cannot speak: When input distributions are unknown. Applied Biomathematics Report, Setauket, NY: Applied Biomathematics Inc., 1998. Available at http://www.ramas.com/whereof.pdf.
20. Klir GJ, Yuan B. Fuzzy Sets and Fuzzy Logic: Theory and Applications. Upper Saddle River, NJ: Prentice-Hall, 1995.
21. Tanaka H, Fan LT, Lai FS. Fault tree analysis by fuzzy probability. IEEE Transactions on Reliability, 1983; 32:453–457.
22. Liang GS, Wang MJJ. Fuzzy fault tree analysis using failure possibility. Microelectronics Reliability, 1993; 33(4): 583–597.
23. Huang HZ, Tong X, Zuo M. Posbist fault tree analysis of coherent systems. Reliability Engineering and System Safety, 2004; 84(2):141–148.
24. Yuhua D, Datao Y. Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis. Journal of Loss Prevention in the Process Industries, 2005; 18: 83–88.

25. Ferdous R, Khan F, Veitch B, Amyotte PR. Methodology for computer aided fuzzy fault tree analysis. Process Safety and Environmental Protection, 2009; 87:217–226.
26. Misra KB, Weber GG. A new method for fuzzy fault tree analysis. Microelectronics Reliability, 1989; 29(2):195–216.
27. Soman KP, Misra KB. Fuzzy fault tree analysis using resolution identity and extension principle. International Journal of Fuzzy Mathematics, 1993; 1:193–212.
28. Suresh PV, Babar AK, Venkat Raj V. Uncertainty in fault tree analysis: A fuzzy approach. Fuzzy Sets and Systems, 1996; 83:135–141.
29. Baudrit C, Dubois D. Practical representations of incomplete probabilistic knowledge. Computational Statistics & Data Analysis, 2006; 51(1):86–108.
30. Baudrit C, Dubois D, Guyonnet D. Joint propagation and exploitation of probabilistic and possibilistic information in risk assessment. IEEE Transactions on Fuzzy Systems, 2006; 14(5):593–608.
31. Baudrit C, Dubois D, Perrot N. Representing parametric probabilistic models tainted with imprecision. Fuzzy Sets and System, 2008; 159(15):1913–1928.
32. Dubois D. Possibility theory and statistical reasoning. Computational Statistics & Data Analysis, 2006; 51:47–69.
33. Dubois D, Prade H. Possibility Theory: An Approach to Computerized Processing of Uncertainty. New York: Plenum Press, 1988.
34. Baraldi P, Zio E. A combined Monte Carlo and possibilistic approach to uncertainty propagation in event tree analysis. Risk Analysis, 2008; 28(5):1309–1326.
35. Flage R, Baraldi P, Ameruso F, Zio E, Aven T. Handling epistemic uncertainties in fault tree analysis by probabilistic and possibilistic approaches. Pp. 1761–1768 in Bris R, Guedes Soares C, Martorell S (eds). Reliability, Risk and Safety: Theory and Applications. Supplement Proceedings of the European Safety and Reliability Conference 2009 (ESREL 2009), Prague, Czech Republic, 7–10 September 2009. Boca Raton: Taylor & Francis, 2010.
36. Flage R, Baraldi P, Zio E, Aven T. Possibility-probability transformation in comparing different approaches to the treatment of epistemic uncertainties in a fault tree analysis. Pp. 714–721 in Ale B, Papazoglu IA, Zio E (eds). Reliability, Risk and Safety – Proceedings of the European Safety and Reliability (ESREL) 2010 Conference, Rhodes, Greece, 5–9 September 2010. London, UK: Taylor & Francis Group, 2010.
37. Limbourg P, Savic R, Petersen J, Kochs HD. Fault tree analysis in an early design stage using the Dempster-Shafer theory of evidence. Pp. 713–722 in Aven T, Vinnem JE (eds). Risk, Reliability and Societal Safety—Proceedings of the European Safety and Reliability (ESREL) 2007 Conference, Stavanger, Norway. London, UK: Taylor & Francis Group, 2007.
38. Limbourg P, Savić R, Petersen J, Kochs H-D. Modelling uncertainty in fault tree analyses using evidence theory. Journal of Risk and Reliability, 2008; 222(3):291–301.
39. Ferson S, Kreinovich V, Ginzburg L, Sentz K, Myers DS. Constructing probability boxes and Dempster-Shafer structures. Sandia National Laboratories, Technical Report SAND2002–4015, Albuquerque, NM, 2003.
40. Ferson S, Nelsen RB, Hajagos J, Berleant DJ, Zhang J, Tucker WT, Ginzburg LR, Oberkampf WL. Dependence in probabilistic modeling, Dempster-Shafer theory, and probability bounds analysis. Technical Report SAND2004–3072, Albuquerque, NM, 2004.
41. Helton JC, Johnson JD, Oberkampf WL, Storlie CB. A sampling-based computational strategy for the representation of epistemic uncertainty in model predictions with evidence theory. Computer Methods in Applied Mechanics and Engineering, 2007; 196:3980–3998.
42. Helton JC, Johnson JD, Oberkampf WL, Sallaberry CJ. Representation of analysis results involving aleatory and epistemic uncertainty. Sandia National Laboratories, Technical Report SAND2008–4379, Albuquerque, NM, 2008.
43. Sentz K, Ferson S. Combination of evidence in Dempster-Shafer theory. Sandia National Laboratories, Technical Report SAND 2002–0835, Albuquerque, NM, 2002.
44. Shafer G. A Mathematical Theory of Evidence. Princeton, NJ: Princeton University Press, 1976.
45. Ferson S, Hajagos JG. Arithmetic with uncertain numbers: Rigorous and (often) best possible answers. Reliability Engineering and System Safety, 2004; 85:135–152.
46. Ferson S, Tucker WT. Sensitivity in risk analyses with uncertain numbers. Technical Report SAND2006–2801, Setauket, NY, 11733, 2006.
47. Ferson S, Kreinovich V, Hajagos J, Oberkampf W, Ginzburg L. Experimental uncertainty estimation and statistics for data having interval uncertainty. Technical Report SAND2007-0939, Setauket, NY, 11733, 2007.
48. Ferson S, Van den Brink P, Estes TL, Gallagher K, O'Connor R, Verdonck F. Bounding uncertainty analyses. In Warren-Hicks WJ, Hart A. Application of Uncertainty Analysis to Ecological Risks of Pesticides. Pensacola and Boca Raton, FL: SETAC and CRC Press, 2010.
49. Moore RE. Methods and Applications of Interval Analysis. Philapdelphia, PA: SIAM, 1979.
50. USNRC. Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis. Technical report NUREG/CR-5801 (SAND91-7087), Washington, DC: Division of Safety Issue Resolution, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1993.
51. USNRC. Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding. Technical report NUREG/CR-6268, Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2007.
52. Zio E. Computational Methods for Reliability and Risk Analysis. Singapore: World Scientific Publishing, 2009.
53. Watts DJ. A simple model of global cascades on random networks. Proceedings of the National Academy of Science USA, 2002; 99(9):5766–5771.
54. Guimerà R, Arenas A, Dìaz-Guilera A, Giralt F. Dynamical properties of model communication networks. Physical Review E, 2002; 66: 026704.
55. Sansavini G, Hajj MR, Puri IK, Zio E. A deterministic representation of cascade spreading in complex networks. EPL, 2009; 87(4):1–4, art. no. 48004.
56. Zio E, Sansavini G. Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Transactions on Reliability, 2011; 60(1):94–101.
57. Zio E, Sansavini G. Component criticality in failure cascade processes of network systems. Risk Analysis, 2011; 31(8):1196–1210.
58. Fréchet M. Généralisations du théorème des probabilités totales. Fundamenta Mathematica, 1935; 25:379–387.
59. Frank MJ, Nelsen RB, Schweizer B. Best-possible bounds for the distribution of a sum-a problem of Kolmogorov. Probability Theory and Related Fields, 1987; 74:199–211.
60. Sadiq R, Saint-Martin E, Kleiner Y. Predicting risk of water quality failures in distribution networks under uncertainties using fault-tree analysis. Urban Water, 2008; 5(4):287–304.
61. Berleant D, Goodman-Strauss C. Bounding the results of arithmetic operations on random variables of unknown dependency using intervals. Reliable Computing, 1998; 4:147–165.
62. Berleant D, Zhang J. Representation and problem solving with distribution envelope determination (DEnv). Reliability Engineering and System Safety, 2004; 85:153–168.
63. Berleant D, Zhang J. Using Pearson correlation to improve envelopes around the distributions of functions. Reliable Computing, 2004; 10:139–161.

64. Berleant D, Xie L, Zhang J. Statool: A tool for distribution envelope determination (DEnv), an interval-based algorithm for arithmetic on random variables. Reliable Computing, 2003; 9(2):91–108.
65. Berleant D, Anderson G, Goodman-Strauss C. Arithmetic on bounded families of distributions: A DEnv algorithm tutorial. Pp. 183–210 in Hu C, Kearfott RB, de Korvin A and Kreinovich V (eds). Knowledge Processing with Interval and Soft Computing. London, UK: Springer-Verlag, 2008.
66. Vaurio JK. Treatment of general dependencies in system fault-tree and risk analysis. IEEE Transactions on Reliability, 2002; 51(3):278–287.
67. Vaurio JK. Consistent mapping of common cause failure rates and alpha factors. Reliability Engineering and System Safety, 2007; 92(5):628–645.
68. Karanki DR, Dang VN. Quantification of uncertainty in fault tree analysis with correlated basic events. Pp. 1619–1628 in Ale B, Papazoglu IA, Zio E (eds). Reliability, Risk and Safety – Proceedings of the European Safety and Reliability (ESREL) 2010 Conference, Rhodes, Greece, 5–9 September 2010. London, UK: Taylor & Francis Group, 2010.
69. Li H. Hierarchical Risk Assessment of Water Supply Systems. Ph.D. thesis, Loughborough University, Leicestershire, UK, 2007.
70. Ferdous R, Khan F, Sadiq R, Amyotte P, Veitch B. Fault and event tree analyses for process systems risk analysis: Uncertainty handling formulations. Risk Analysis, 2011; 31(1):86–107.
71. Zhang Q. A general method dealing with correlations in uncertainty propagation in fault trees. Reliability Engineering and System Safety, 1989; 26(3):231–247.
72. Zhang Q. A method dealing with correlations in uncertainty propagation by using traditional correlation coefficients. Reliability Engineering and System Safety, 1993; 41(2):107–114.
73. Rushdi AM, Kafrawy KF. Uncertainty propagation in fault tree analyses using an exact method of moments. Microelectronics and Reliability, 1988; 28:945–965.
74. Kafrawy KF, Rushdi AM. Uncertainty analysis of fault tree with statistically correlated failure data. Microelectronics and Reliability, 1990; 30:157–175.
75. Karanki DR, Jadhav PA, Chandrakar A, Srividya A, Verma AK. Uncertainty analysis in PSA with correlated input parameters. International Journal of Systems Assurane Engineering Management, 2010; 1:66–71.
76. Huang B, Du X. A robust design method using variable transformation and Gauss-Hermite integration. International Journal for Numerical Methods in Engineering, 2006; 66:1841–1858.
77. Kalos MH, Whitlock PA. Monte Carlo Methods. Volume I: Basics. New York: Wiley, 1986.
78. Marseguerra M, Zio E. Basics of the Monte Carlo Method with Application to System Reliability. Hagen, Germany: LiLoLe–Verlag GmbH, 2002.
79. Karanki DR, Kushwaha HS, Verma AK, Ajit S. Uncertainty analysis based on probability bounds (P-Box) approach in probabilistic safety assessment. Risk Analysis, 2009; 29(5):662–675.
80. Regan HM, Ferson S, Berleant D. Equivalence of five methods for bounding uncertainty. International Journal of Approximate Reasoning, 2004; 36:1–30.
81. Tonon F. Using random set theory to propagate epistemic uncertainty through a mechanical system. Reliability Engineering and System Safety, 2004; 85:169–181.
82. Couso I, Moral S. Independence concepts in evidence theory. International Journal of Approximate Reasoning, 2010; 51:748–758.
83. Couso I, Moral S, Walley P. Examples of independence for imprecise probabilities. Pp. 121–130 in de Cooman G, Cozman FF, Moral S, Walley P (eds). Proceedings of the First International Symposium on Imprecise Probability and Their Applications. Imprecise Probabilities Project, Universiteit Gent, Belgium, 1999.
84. Couso I, Moral S, Walley P. A survey of concepts of independence for imprecise probabilities. Risk Decision and Policy, 2000; 5:165–181.
85. Dubois D, Prade H, Sandri S. On possibility/probability transformations. Pp. 103–112 in Lowen R, Roubens M (eds). Fuzzy Logic: State of the Art. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1993.
86. Smets P. Constructing the pignistic probability function in a context of uncertainty. Pp. 29–39 in Henrion M, Shachter RD, Kanal LN, Lemmer JF (eds). Uncertainty in Artificial Intelligence 5. Amsterdam, The Netherlands: North-Holland Publishing Co., 1990.
87. Dubois D, Foulloy L, Mauris G, Prade H. Probability-possibility transformations, triangular fuzzy sets, and probabilistic inequalities. Reliable Computing, 2004; 10:273–297.
88. Dubois D, Prade H, Smets P. A definition of subjective possibility. International Journal of Approximate Reasoning, 2008; 48:352–364.

E. Ferrario
Chair on Systems Science and
the Energetic Challenge,
European Foundation for New Energy,
Electricité de France,
École Centrale Paris–Supelec,
Grande Voie des Vignes,
92295 Chatenay Malabry, France
e-mail: elisa.ferrario@ecp.fr

N. Pedroni
Chair on Systems Science and
the Energetic Challenge,
European Foundation for New Energy,
Electricité de France,
École Centrale Paris–Supelec,
Grande Voie des Vignes,
92295 Chatenay Malabry, France
e-mails: nicola.pedroni@ecp.fr,
nicola.pedroni@supelec.fr

E. Zio
Chair on Systems Science and
the Energetic Challenge,
European Foundation for New Energy,
Electricité de France,
École Centrale Paris–Supelec,
Grande Voie des Vignes,
92295 Chatenay Malabry, France;
Politecnico di Milano,
20133 Milano, Italy
e-mails: enrico.zio@ecp.fr, enrico.zio@supelec.fr,
enrico.zio@polimi.it

Analysis of the Robustness and Recovery of Critical Infrastructures by Goal Tree–Success Tree: Dynamic Master Logic Diagram, Within a Multistate System-of-Systems Framework, in the Presence of Epistemic Uncertainty

In this paper, we evaluate the robustness and recovery of connected critical infrastructures (CIs) under a system-of-systems (SoS) framework taking into account: (1) the dependencies among the components of an individual CI and the interdependencies among different CIs; (2) the variability in component performance, by a multistate model; and (3) the epistemic uncertainty in the probabilities of transitions between different components states and in the mean values of the holding-times distributions, by means of intervals. We adopt the goal tree success tree–dynamic master logic diagram (GTST–DMLD) for system modeling and perform the quantitative assessment by Monte Carlo simulation. We illustrate the approach by way of a simplified case study consisting of two interdependent infrastructures (electric power system and gas network) and a supervisory control and data acquisition (SCADA) system connected to the gas network.
[DOI: 10.1115/1.4030439]

Keywords: critical infrastructures, electric power system, gas distribution network, SCADA, robustness, recovery time, multistate, goal tree success tree–dynamic master logic diagram, Monte Carlo simulation, epistemic uncertainty, imprecise probability, interval analysis

1 Introduction

CIs, e.g., transportation, electric power, water, gas, and communication systems, interact on the basis of complex relationships that cross the single-infrastructure boundary. This exposes CIs to the risk that a failure in an infrastructure can have negative impacts on another interconnected one. For example, CIs are becoming more and more dependent on information technologies that, on one hand, provide control and support their increasing efficiency but, on the other hand, create new vulnerabilities [1]. As an additional example from the field, the widespread power electric blackout that occurred in the Midwest and Northeast of the United States and Ontario, Canada, on August 2003, affected the serviceability of the water system at Cleveland, OH, due to the lack of power needed to operate the water pumping stations [2]. Analyzing and understanding the interdependences existing among infrastructure systems is fundamental for the safe operation and control of these SoSs.

We adopt an SoS framework of analysis to evaluate the SoS robustness and recovery properties, considering the dependencies among the components of a CI and the interdependencies among different CIs. For a more realistic representation, we utilize a multistate model for consideration of the different degrees of damage that the individual components may experience [3]. Transitions between different states of damage occur stochastically (aleatory uncertainty), and epistemic uncertainty affects the associated transition probabilities due to insufficient knowledge and information on the components' degradation behavior [4–6]. Indeed, safety-CIs are highly reliable, and thus, undergo few degradations to failure, such that it is difficult to estimate damage levels and transition probabilities [7–11].

For illustration purpose, we adapt the framework of analysis to a case study proposed in [1], in which the system considered consists of two interdependent infrastructures (gas and electric power networks), and a SCADA system connected to the gas network. To measure the robustness and recovery capacity of the system, we look at the steady-state probability distributions of the supply of gas and electricity at the demand nodes and the time needed to recover the SoS from the worst scenario to a level in which all the demand nodes are satisfied, respectively.

We propose a hierarchical model description of the system logic and functionality by GTST–DMLD [12], extending its representation characteristics to evaluate the physical flows of gas and electricity through the interdependent infrastructures. We adopt intervals to describe the epistemic uncertainty in the probabilities of transition between different components states and in the mean values of the holding-time distributions [13–21], and we use interval analysis to calculate the (uncertain) probabilities of the states of all

Manuscript received July 29, 2014; final manuscript received January 14, 2015; published online July 1, 2015. Assoc. Editor: Alba Sofi.

Copyright © 2015 by ASME

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

the components of the CIs [22–27]. Finally, we employ Monte Carlo simulation [28,29] for the probabilistic evaluation of the SoS performance.

The paper is organized as follows: In Sec. 2, the case study is presented; in Sec. 3, the SoS modeling by GTST–DMLD is illustrated; Sec. 4 details the procedural steps to evaluate the SoS performance under epistemic uncertainty are given; in Sec. 5, results of the analysis are shown and discussed; and in Sec. 6, a conclusion is provided.

2 Case Study

The case study is taken from Ref. [1] and it deals with two interconnected infrastructures, i.e., a natural gas distribution network and an electricity generation/distribution network (Fig. 1, top, solid and dashed lines, respectively). The gas distribution network is supported by a SCADA system (Fig. 1, top, dotted lines). The objective of this interconnected SoS is to provide the necessary amount of gas and electricity (hereafter also called "product") to four demand nodes (end-nodes); namely, D1 and D2 (gas), and L1 and L2 (electricity).

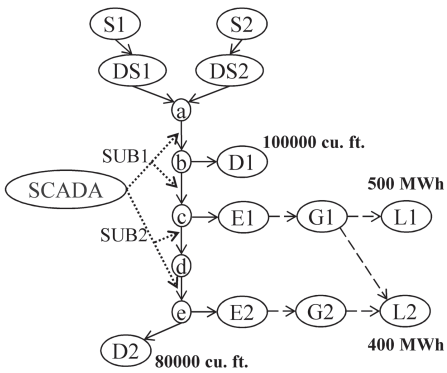
The gas distribution network, supplied by two sources of gas (namely, S1 and S2, that are connected to the network by arcs S1_DS1 and S2_DS2, respectively), provides gas to the end-nodes D1 and D2 and to two nodes of the electricity network (E1 and E2). Once the gas enters into nodes E1 and E2, it is transformed into electrical energy that flows through arcs E1_G1 and E2_G2 (representing the electric power generation stations) to supply the end-nodes of electricity (L1 and L2); notice that the demand L2 can be supplied by both electrical generations E1_G1 and E2_G2. The assumption is made that the gas–electricity transformation occurs with a constant coefficient, i.e., 100 cu. ft. ($1\,\text{cu.ft} \approx 0.028\,\text{m}^3$) of natural gas produces 1 MWh of electricity [1].

A SCADA system controls the gas flow through arcs a_b, b_c, c_d, and d_e. It is assumed that: (1) the SCADA has two core subsystems controlling different sets of arcs (in particular, the first one—SUB1—refers to links a_b and b_c, whereas the second one—SUB2—controls arcs c_d and d_e) and (2) the SCADA is always provided with electric power [1].

The capacities of the arcs of the gas and electricity networks (determining the maximum flows of gas or electricity supported by the arcs) can be deterministic (i.e., fixed constant values) or stochastic (i.e., randomly evolving in time) (Fig. 1, bottom). The stochastic capacities give rise to a multistate model that reflects the possibly different degrees of damage of the arcs. In contrast, the SCADA system-state is defined by a binary random variable, whose values one and zero represent its complete and partial functioning, respectively. For example, when the state of the SCADA subsystem SUB1 (controlling arcs a_b and b_c) is zero, the capacity of these arcs decreases because of the incorrect information provided by the SCADA subsystem (even if the arcs are not subject to a direct damage). On the basis of the two states of the SCADA subsystems, two different vectors of capacities are identified for each arc a_b, b_c, c_d, and d_e as illustrated in Fig. 1 (bottom).

In the following, we generically denote the value of the state of a component (i.e., the capacity of the arcs) as $\zeta^{c,i}$, $i \in \{1, 2, \ldots, \mathrm{S}^c\}$, where c indicates the component of interest and i is the state number (when $i = 1$, the component is in the worst state, whereas when $i = \mathrm{S}^c$, it is in the best state); S^c is the total number of states for that component. For example, component S1_DS1 has $\mathrm{S}^{\mathrm{SI_DSI}} = 4$ possible states of gas capacity: $\zeta^{\mathrm{SI_DSI},1} = 90{,}000$ cu. ft., $\zeta^{\mathrm{SI_DSI},2} = 95{,}000$ cu. ft., $\zeta^{\mathrm{SI_DSI},3} = 100{,}000$ cu. ft., $\zeta^{\mathrm{SI_DSI},4} = 105{,}000$ cu. ft. The total number of components in the SoS is referred to as NC.

Changes in the arc capacities are due to random failures or recovery actions. The state transitions over time are modeled by



Arc capacities

Deterministic	Stochastic	
DS1_a: 100000 cu. ft.	S1_DS1: [90, 95, 100, 105]*10^3 cu. ft.	E1_G1: [600, 800] MWh
DS2_a: 200000 cu. ft.	S2_DS2: [100, 160, 200]*10^3 cu. ft.	E2_G2: [0, 250, 400] MWh
b_D1: 100000 cu. ft.	SUB1: [0, 1]	SUB2: [0, 1]
c_E1: 80000 cu. ft.	*If SUB1 = 0*	*If SUB2 = 0*
e_E2: 40000 cu. ft	a_b: [0, 40, 90, 130, 170, 210, 250]*10^3 cu. ft.	c_d: [0, 10, 20, 40, 60, 80, 90]*10^3 cu. ft.
e_D2: 110000 cu. ft	b_c: [0, 40, 60, 80, 100, 120, 140]*10^3 cu. ft.	d_e: [0, 10, 20, 40, 60, 80, 90]*10^3 cu. ft.
G1_L1: 500 MWh	*If SUB1 = 1*	*If SUB2 = 1*
G1_L2: 400 MWh	a_b: [0, 50, 100, 150, 200, 250, 300]*10^3 cu. ft.	c_d: [0, 20, 30, 50, 70, 90, 100]*10^3 cu. ft.
G2_L2: 400 MWh	b_c: [0, 70, 90, 110, 130, 150, 170]*10^3 cu. ft.	d_e: [0, 20, 30, 50, 70, 90, 100]*10^3 cu. ft.

Fig. 1 Top: Interdependent gas (solid lines) and electric (dashed lines) infrastructures and SCADA system (dotted lines) [1]; the quantities demanded by the end-nodes D1, D2, L1, and L2 are reported in bold. Bottom: deterministic and stochastic arc capacities ($1\,\text{cu.ft} \approx 0.028\,\text{m}^3$).

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

Markov and semi-Markov processes as in Ref. [1]. Semi-Markov processes are adopted to represent the evolution of the capacities of the gas supply links (S1_DS1 and S2_DS2), whereas Markov processes are used for all the other arcs. Both Markov and semi-Markov processes for a generic component c, $c = 1, 2, \ldots, \mathrm{NC}$, are defined by a transition probability matrix $\mathbf{P}^c = \{p_{ij}^c{:}i, j = 1, 2, \ldots, \mathrm{S}^c\}$, where p_{ij}^c is the one-step probability of transition from state i to state j. In addition, the semi-Markov processes are characterized by a matrix of continuous probability distribution (e.g., normal), $\mathbf{T}^c = \{\mathrm{th}_{ij}^c \approx N(\mu_{ij}^c, \sigma_{ij}^c){:}i, j = 1, 2, \ldots, \mathrm{S}^c\}$, for the holding time, i.e., for the time of residence in state i before performing a transition to state j. The total number of components in the SoS described by the semi-Markov processes is referred to as NS.

Differently from Ref. [1], we take into account the epistemic uncertainty affecting the transition probabilities and the holding-time distributions of the Markov and semi-Markov processes, respectively. In particular, intervals $[\underline{p}_{ij}^c, \bar{p}_{ij}^c]$, $c = 1, 2, \ldots, \mathrm{NC}$, $i, j = 1, \ldots, \mathrm{S}^c$, (instead of fixed constant values) are used to describe the state transition probabilities for both Markov and semi-Markov processes (matrices $\mathbf{P}^c$, $c = \mathrm{S1_DS1}, \mathrm{S2_DS2}$, a_b, b_c, c_d, d_e, SCADA, E1_G1 and E2_G2, in Fig. 2 with respect to the states defined in Fig. 1, bottom) [30–35]. The holding-time distributions for the components modeled by the semi-Markov processes are considered normal with epistemically uncertain mean (described by an interval $[\underline{\mu}_{ij}^c, \bar{\mu}_{ij}^c]$) and fixed standard deviation, σ_{ij}^c (matrices $\mathbf{T}^c$, $c = \mathrm{S1_DS1}, \mathrm{S2_DS2}$, in Fig. 2); this level-2 hierarchical representation produces a family of normal probability distributions characterized by the same standard deviation, but different mean values: such a bundle of distributions is often referred to as distributional probability-box (p-box) [36–41]. Notice that we have considered a single value instead of an interval of values for the standard deviation sinply to reduce the computational time of the simulation, but this does not represent a limitation of the approach.

In the present work, the demand nodes are not given the same importance: in particular, D1 is more important than L1; on its turn, L1 is more important than both D2 and L2 (which instead are equally important). These assumptions are made to illustrate and motivate the logical repartition of electricity and gas flows in the network and its representation in the GTST–DMLD given in Sec. 3.

The objectives of the analysis are to determine the cumulative distribution functions (CDFs) of: (1) the product delivered to the demand nodes (i.e., D1, D2, L1, and L2) at the steady-state and (2) the time needed to recover the SoS from the worst scenario. As the state transition probabilities of the network components are affected by epistemic uncertainty and are described by intervals, $[\underline{p}_{ij}^c, \bar{p}_{ij}^c]$, $c = 1, 2, \ldots, \mathrm{NC}$, $i, j = 1, \ldots, \mathrm{S}^c$, the corresponding component steady-state probabilities are also affected by epistemic uncertainty and are represented by intervals of possible values, $[\Pi_{\min}^{c,i}, \Pi_{\max}^{c,i}]$, $c = 1, 2, \ldots, \mathrm{NC}$, $i = 1, 2, \ldots, \mathrm{S}^c$. As a consequence, a set of CDFs corresponding to the set of possible steady-state probabilities within the intervals $[\Pi_{\min}^{c,i}, \Pi_{\max}^{c,i}]$, $c = 1, 2, \ldots, \mathrm{NC}$, $i = 1, \ldots, \mathrm{S}^c$ is obtained for each demand node. For the same reason (i.e., for the presence of the epistemic uncertainty in the state transition probabilities and in the mean of the components holding-time distributions), a set of CDFs for the recovery time of the system is obtained in correspondence to the set of possible state transition probabilities.

$c =$ S1_DS1 (Semi-Markov)

$$\mathbf{P}^c = \begin{vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ [0.002; 0.008] & [0.002; 0.008] & 0 & [0.998; 1] \\ [0.002; 0.008] & [0.002; 0.008] & [0.998; 1] & 0 \end{vmatrix}$$

$$\mathbf{T}^c = \begin{vmatrix} - & \mathrm{N}([2; 6], 1) & - & - \\ - & - & \mathrm{N}([2; 6], 1) & - \\ \mathrm{N}([7; 13], 3) & \mathrm{N}([7; 13], 3) & - & \mathrm{N}([17; 23], 2) \\ \mathrm{N}([7; 13], 3) & \mathrm{N}([7; 13], 3) & \mathrm{N}([17; 23], 2) & - \end{vmatrix}$$

$c =$ S2_DS2 (Semi-Markov)

$$\mathbf{P}^c = \begin{vmatrix} 0 & 1 & 0 \\ [0; 0.02] & 0 & [0.98; 1] \\ [0; 0.02] & [0.98; 1] & 0 \end{vmatrix}$$

$$\mathbf{T}^c = \begin{vmatrix} - & \mathrm{N}([2; 6], 1) & - \\ \mathrm{N}([7; 13], 3) & - & \mathrm{N}([2; 6], 1) \\ \mathrm{N}([7; 13], 3) & \mathrm{N}([17; 23], 2) & - \end{vmatrix}$$

$c =$ a_b, b_c, c_d, d_e (Markov)

$$\mathbf{P}^c = \begin{vmatrix} [0.04; 0.06] & [0.04; 0.06] & [0.04; 0.06] & [0.04; 0.06] & [0.1; 0.3] & [0.1; 0.3] & [0.3; 0.5] \\ [0.04; 0.06] & [0.04; 0.06] & [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.1; 0.3] & [0.3; 0.5] \\ [0.04; 0.06] & [0.04; 0.06] & [0.04; 0.06] & [0.1; 0.3] & [0.1; 0.3] & [0.04; 0.06] & [0.3; 0.5] \\ [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.04; 0.06] & [0.3; 0.5] \\ [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.04; 0.06] & [0.3; 0.5] \\ [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.1; 0.3] & [0.04; 0.06] & [0.04; 0.06] & [0.3; 0.5] \\ [0.0005; 0.0015] & [0.0005; 0.0015] & [0.0005; 0.0015] & [0.0015; 0.0025] & [0.0015; 0.0025] & [0.002; 0.004] & [0.985; 0.995] \end{vmatrix}$$

$c =$ SCADA (Markov)
(states of SUB1 and SUB2: 0 0, 0 1, 1 0, 1 1)

$$\mathbf{P}^c = \begin{vmatrix} [0.7; 0.9] & [0.03; 0.05] & [0.03; 0.05] & [0.02; 0.22] \\ [0.05; 0.15] & [0.3; 0.5] & [0.2; 0.4] & [0.1; 0.3] \\ [0.05; 0.15] & [0.2; 0.4] & [0.3; 0.5] & [0.1; 0.3] \\ [0.0005; 0.0007] & [0.0001; 0.0003] & [0.0001; 0.0003] & [0.998; 1] \end{vmatrix}$$

$c =$ E2_G2 (Markov)

$$\mathbf{P}^c = \begin{vmatrix} [0.1; 0.3] & [0.05; 0.15] & [0.6; 0.8] \\ 0 & [0.1; 0.3] & [0.7; 0.9] \\ [0.0004; 0.0006] & [0.0004; 0.0006] & [0.998; 1] \end{vmatrix}$$

$c =$ E1_G1 (Markov)

$$\mathbf{P}^c = \begin{vmatrix} [0.05; 0.15] & [0.89; 0.91] \\ [0; 0.002] & [0.998; 1] \end{vmatrix}$$

Fig. 2 Holding-time distributions (matrices $\mathbf{T}^c$) for the arcs described by semi-Markov processes: each element of the matrix represents a normal distribution with uncertain (interval) mean and fixed standard deviation. State transition probability matrices ($\mathbf{P}^c$) for the arcs described by Markov and semi-Markov processes: each element of the matrix represents an interval for the corresponding transition probability.

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

3 SoS Modeling

3.1 GTST—DMLD: Basic Concepts. The GTST–DMLD is a goal-oriented method based on a hierarchical framework [12]. It gives a comprehensive description of the systems in terms of functions (qualities), objects (parts), and their relationships (interactions). The first description is provided by the goal tree (GT), the second by the success tree (ST), and the third by the DMLD [12].

The GT identifies the hierarchy of the qualities of the system comprising the objective of the analysis, i.e., the goal, organizing them in functions that are in turn subdivided into other functions, etc. The hierarchy is built by answering questions on "how" the subfunctions can attain the parent functions (looking at the hierarchy from top to bottom) and on "why" the functions are needed (looking at the hierarchy from bottom to top). Two types of qualities, i.e., main and support functions, are considered: the former directly contributes to achieving the goal, whereas the latter supports the realization of the former [42].

The ST represents the hierarchy of the objects of the system, from the entire system to the parts necessary to attain the last levels of the GT. This hierarchy is built identifying the elements that are "part of" the parent objects. As for the GT, two types of objects are distinguished also in the ST: main and support. The former is directly contributing to the achievement of the main functions, whereas the latter is needed for the operation of the former [42].

The DMLD is an extension of the master logic diagram (MLD) [12] introduced to model the dynamic behavior of a physical system. It describes the interactions between parts, functions, and parts and functions in the form of a dependency matrix, and it includes the dynamics by means of time-dependent fuzzy logic rules [12].

A conceptual sketch of GTST–DMLD is given in Fig. 3. The GT is drawn at the top, the ST tree on the left, and the DMLD is represented by filled dots at the intersections between vertical and horizontal lines, to indicate the possible dependencies between the elements on the left and on the top. Several types of logic gates can be used to represent the time-dependent fuzzy logic rules, and different dependency-matrix nodes to describe the probabilities and degrees of truth in the relationships [12]. Figure 4 gives an example of dependency of an element C on two elements A and B by the "AND" gate in a DMLD [12]. In this case, the output value of the element C is the minimum value between the inputs A and B. Replacing the "AND" gate with an "OR" gate, the output value will be the maximum between the input values.

Further details on the *construction* of the GTST–DMLD modeling and its *applications* are not given here for the sake of brevity: the interested reader is referred to the cited literature [12,42].

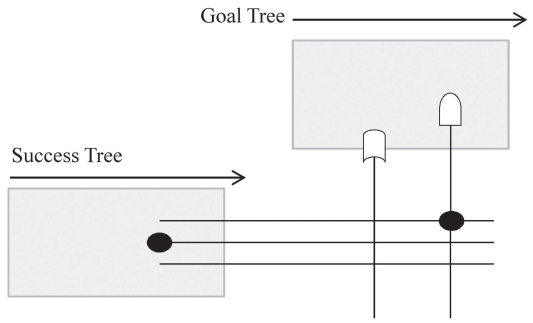


Fig. 3 Conceptual sketch of GTST–DMLD: the filled dots indicate the possible dependencies between the objects (filled dot on the left) and between the objects and functions (filled dot on the right), the logic gates indicate how a given function depends on the input values

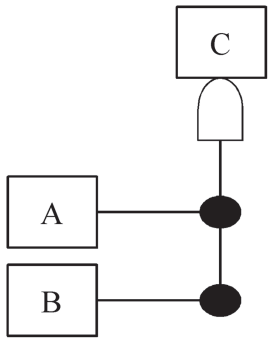


Fig. 4 Example of an element C that depends on two elements A and B by an "AND" gate

In Sec. 3.2, the adaptation of the GTST–DMLD for modeling interconnected networked infrastructures is illustrated.

3.2 GTST—DMLD for Interconnected Networked Infrastructures. In this section, we adapt the GTST–DMLD presented in Sec. 3.1, in general terms, for an adequate representation of interconnected networked infrastructures, and in particular, of the ones making the SoS of our case study in Sec. 2. Specifically, we introduce new concepts in order to model in the diagram not only the dependency relations between the components but also the ways in which the flows of gas and electricity are partitioned into the network on the basis of: (1) the importance of the demand nodes, (2) the amount of product necessary to satisfy each demand, (3) the constraints of the arc capacities, and (4) the information provided by the SCADA system. In the following, first, we explain the notation adopted in the GTST–DMLD, and then, we apply it to the case study of interest.

In the present work, we distinguish between three main types of dependency: *direct*, *indirect*, and *constraint-based* dependencies, as illustrated in Figs. 5 and 6. The first ones, pictorially represented by a dot, express the fact that the product of the element on the bottom passes straight into the element on the top. Indirect dependencies, represented by a hexagon, capture the relations between arcs that share the same input flow, but whose outputs are not related. This type of dependencies is important for the optimal allocation of the product in the network: for example, it is used to describe those cases where the flow exceedance in an arc can be better partitioned into another arc that is not directly connected to it, but that shares one of the inputs (see the example of Fig. 5(*b*)). Finally, constraint-based dependencies, depicted by a triangle, are employed to take into account those relations that do not involve an exchange of physical product, but rather a transfer of information which may impact the state of the connected element. Finally, it is worth noting that in the model, we adopt the symbol of triangle also to represent some physical constraints posed by the problem, such as the maximum flow required by a demand node.

It is worth mentioning that since in the present case we are interested in analyzing the flows passing through the network (and not just the dependency relations), the inputs of an arc are flows and the output is (generally) the sum of the flow inputs. For this reason, in this context, the "AND" gate assumes a different meaning than that in Ref. [12] (see the previous Sec. 3.1): in particular, the output value is the sum of the input values and it is represented by a "+" in the middle of the gate, as shown in the following examples (Figs. 5 and 6). We can then distinguish between the "logical" gates studied by Hu and Modarres [12] and the "physical" gates proposed in the present work: the first ones are needed to highlight the logical connections between the elements that take part/role in a given structure or function of interest; the second ones are used to evaluate the physical flow distribution in the system. Examples of the types of dependencies (direct, indirect, and constraint-based) associated to the physical gates are shown in the following.

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

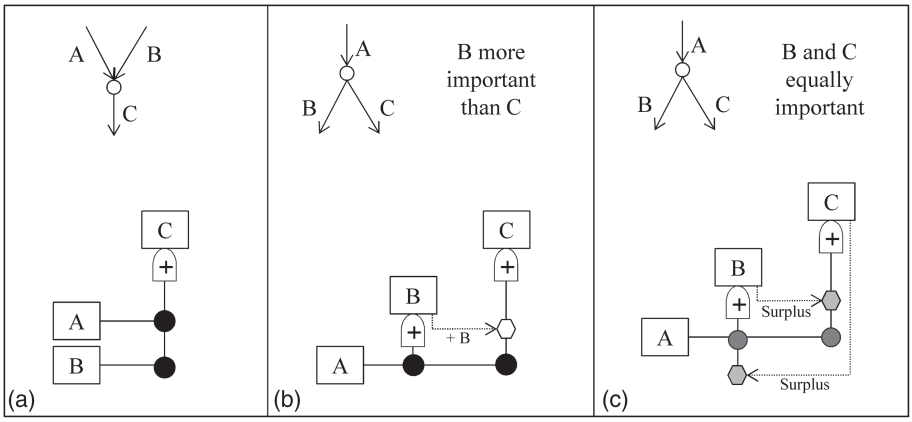


Fig. 5 Examples of direct and indirect dependencies with respect to possible graph representations

For clarity of illustration, in Fig. 5, examples of two types of direct and indirect dependencies are given, with respect to different graph representations. Notice that nodes are neglected and just the relations between arcs are considered. Fig. 5(*a*) shows the dependence of arc C on two input arcs A and B: arc C receives all the input products from A and B (e.g., if the flows in arcs A and B are 50 and 70 units, respectively, the flow in arc C is 120 units); this complete direct dependence is depicted by a black dot. Fig. 5(*b*) and (*c*) describes the same "physical" situation (i.e., an input arc A and two output arcs B and C), but with different relative importance of the arcs. Two different cases are illustrated. In the first case (Fig. 5(*b*)), arc B is more important than C: thus, in this situation, the flow from A supplies first arc B until its demand is satisfied, and then arc C: e.g., if the flow in arc A is 100 units and both arcs B and C need 80 units, arc B will receive 80 units—demand fully satisfied—and arc C, the rest, i.e., 20 units—demand partially satisfied. Arc C is dependent on arc B, as the flow that can reach C depends on the quantity given to B. In the second case (Fig. 5(*c*)), arcs B and C are equally important: thus, the input flow (A) is divided into equal parts on the basis of the number of output arcs (i.e., two in this example); with respect to the numeric example above, both arcs B and C will receive 50 units—demands partially satisfied. Arcs B and C are reciprocally dependent, as the product distributed to one of them depends on that delivered to the other one. The dependency between arcs B and C is "indirect" for both cases, as the output of an arc is not the input of the other one and vice versa. In the case of Fig. 5(*b*), the flow that enters into C is given by the difference between the entire flow from A (direct dependency) and the flow given to B (indirect dependency); this concept is illustrated in the GTST–DMLD by the symbol of direct dependency from A to C (dot) and the symbol of indirect dependency from B to C (hexagon). In particular, for a quantitative evaluation of the model, a white hexagon is introduced to reduce the input flow from arc A by the quantity of product given to arc B: in this view, the white hexagon assumes the value of the flow in B with a negative sign. The flow given to B can be the entire flow of A or a lower value depending on the constraints and arc capacity (see the following example in Fig. 6). In the case of Fig. 5(*c*), the flow from A is divided into equal parts: this condition is represented by a gray dot. However, this equal partition of the flow may not represent the optimal one, as some output arcs may require less flow than the one allocated according to this criterion, e.g., if the flow in arc A is 100 units and arcs B and C need 80 and 20 units, respectively, giving 50 units to both arcs is not a good allocation of the resource, as B is partially satisfied and some product (i.e., 30 units) given to arc C is wasted. Thus, to optimize the repartition of the flow, indirect dependencies are adopted: they are directed from an output arc to all the other output arcs that share the same input. In this case, the "surplus flow" is a positive quantity and it is represented by a gray hexagon (to distinguish it from the "negative" white hexagon of the example in Fig. 5(*b*)).

Notice that the graphical representation of Fig. 5(*b*) and (*c*) is identical; however, the partition of the flux from A is completely different in the two cases: this means that the graphical representation alone cannot be used to describe the repartition of the flows in the network according to different criteria. On the contrary, the DMLD can capture and represent this aspect, which is useful in the quantitative evaluation of system performance.

In Fig. 6, examples of two types of constraint-based dependencies are given, with respect to different possible graph representations. Figure 6(*a*) depicts the same situation as Fig. 5(*a*), with an additional arc D whose behavior impacts on the state of arc C (however, notice that D is not an input to C). This dependency is represented by a gray triangle, and it means that the output of C can be modified on the basis of the state of arc D. In the present case study, this constraint-based dependency is used to model the SCADA system that can decrease the actual flow of the controlled arc if it is in a damage state. Figure 6(*b*) represents the same situation of Fig. 5(*c*) with the addition of another arc (D) sequential to arc C. In this case, there is not a "real dependency" from arc D to arc C, but we adopt the symbol of constraint-based dependency (triangle) as a partitioning constraint to represent the fact that the capacity (or the demand) of arc D can limit the amount of flow

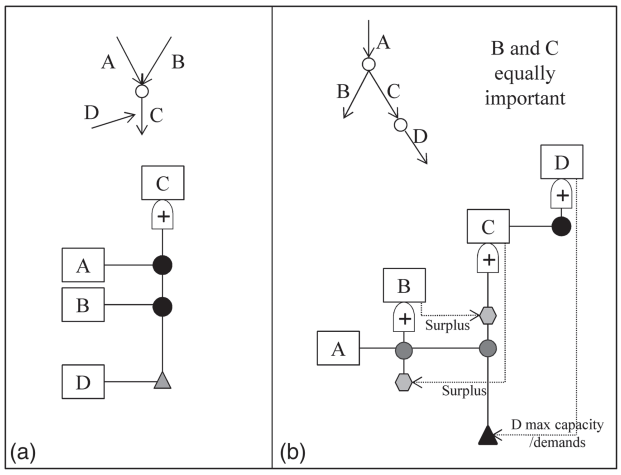


Fig. 6 Examples of constraint-based dependencies with respect to possible graph representations

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

in input to arc C, e.g., if the flow in arc A is 100 units, the capacity of arc C is 50 units, and arcs B and D need 80 and 20 units, respectively; the repartition of the flow is as follows: first 100 units from A are equally divided between arcs B and C (50 units each) and the surplus (if there is) is partitioned between arcs B and C, then the constraint-based dependency is considered (i.e., arc D needs 20 units), and the new surplus is given to arc B (i.e., the exceedance of 30 units from arc C is directed to arc B). This partitioning constraint is represented in the DMLD by a black triangle, and it is needed to control the input flow partitioned in different arcs and guarantee that it is not higher than necessary.

Finally, another type of constraint is taken into account, i.e., the one related to the capacity of the arcs: when the flow in input to an arc is higher than the capacity of the arc itself, the output flow will be equal to the capacity of the arc. The arc capacity can be deterministic or stochastic, and in the GTST–DMLD, it is represented by a gray or dot-filled rectangle, respectively (see Fig. 7).

In Fig. 7, the GTST–DMLD of the case study in Sec. 2 is shown.

The GT on the top represents the main goal of the SoS, related to the supply of the demands of gas and electricity: the objective is achieved if the corresponding nodes D1, D2, L1, and L2 receive the required amount of gas and electricity, respectively. In the present case study, we limit the analysis to the last level of the GT, i.e., we analyze the performance of each demand, without investigating a global indicator of the SoS.

The ST is composed of the main hierarchies of the gas and electricity networks (that directly provide the demand nodes with gas and electricity to achieve the goal function) and of the support hierarchy of the SCADA system (that is needed for the control of the gas network, and therefore, it is not directly involved in the achievement of the goal function); given its support role, it is represented in a parallel dashed branch connected to the gas hierarchy.

The DMLD is represented by the relationships between objects of the ST or between objects of the ST and functions of the GT. It allows determining the goal function by the evaluation of all the dependencies from the bottom to the top of the diagram, following the rules explained above for the direct, indirect, and constraint-based dependencies. For example, arc a_b depends on two arcs, DS1_a and DS2_b, connected by direct dependencies (Fig. 7). Thus, the output of a_b is given by the sum of the corresponding input values, i.e., DS1_a + DS2_b. This value may, then,

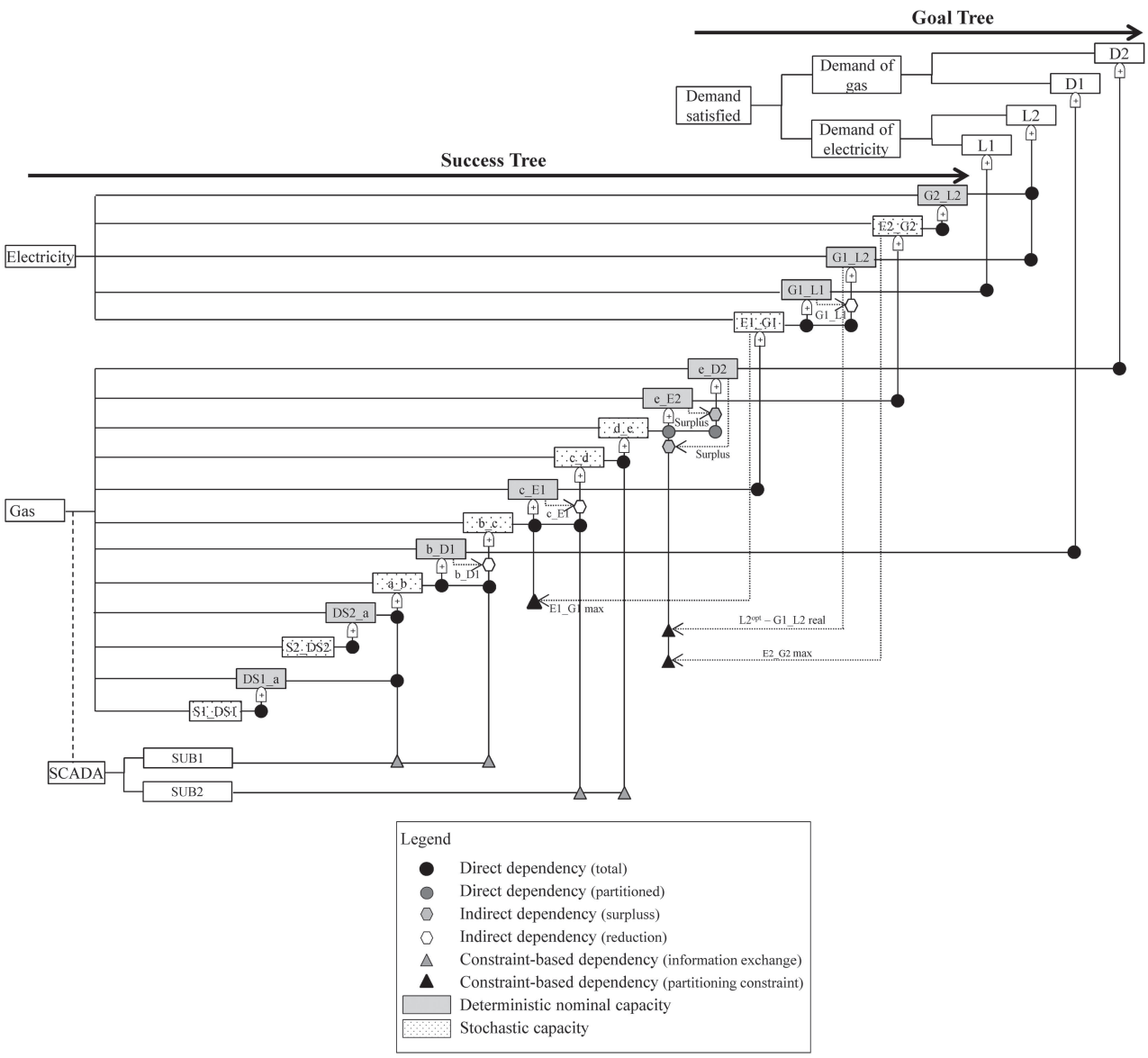


Fig. 7 GTST–DMLD of the case study in Sec. 2 corresponding to the graph of Fig. 1

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

be modified by the constraint-based dependency of the SCADA system and by the (stochastic) capacity of arc a_b itself.

4 Evaluation of the SoS Performance

In this section, we illustrate the evaluation of the performance of the SoS, described in Sec. 2, in the presence of epistemic uncertainties (represented by intervals) affecting the components' state transition probabilities and the mean values of the holding-time distributions. As already mentioned in Sec. 2, the system performance is quantified in terms of: (1) robustness, measured by the steady-state probability distributions of the product delivered at the demand nodes (see Sec. 4.1) and (2) recovery capacity, measured by the time needed to recover the SoS from the worst scenario (see Sec. 4.2). Appendix A gives a brief overview of imprecise (interval) probabilities.

4.1 Robustness. To compute the steady-state probability distributions of the product delivered at the demand nodes, the following three main steps are carried out:

1. *Processing the epistemic uncertainties by interval analysis*: this step leads to the evaluation of the intervals of the steady-state probabilities $[\Pi^{c,i}_{\min}, \Pi^{c,i}_{\max}]$, $i = 1, 2, \ldots, \mathrm{S}^c$, for the states of each component ($c = 1, 2, \ldots, \mathrm{NC}$) of the SoS.
2. *Evaluation of the SoS performance (i.e, robustness) by Monte Carlo simulation*: this step leads to the determination of a set of CDFs of the product delivered at each demand node at steady-state, one for each possible combination of steady-state probabilities ranging within the intervals $[\Pi^{c,i}_{\min}, \Pi^{c,i}_{\max}]$, $i = 1, 2, \ldots, \mathrm{S}^c$ (found at step 1 above).
3. *Postprocessing the results obtained at the previous step 2*: this step leads to the identification of two extreme upper and lower CDFs that bound the set of CDFs produced at step 2 above.

In more details:

1. Solve the following optimization problems for the lower (resp., upper) bounds $\Pi^{c,i}_{\min}$ (resp., $\Pi^{c,i}_{\max}$), $c = 1, 2, \ldots, \mathrm{NC}$, for each row i, $i = 1, 2, \ldots, \mathrm{S}^c$, of the transition probability matrix $\mathbf{P}^c$ (that is composed of probability intervals $[\underline{p}^c_{ij}, \bar{p}^c_{ij}]$, $i, j = 1, 2, \ldots, \mathrm{S}^c$):

$$\Pi^{c,i}_{\min} = \min_{p^c_{ij}, j=1,2,\ldots,\mathrm{S}^c} \{\Pi^{c,i}\}, \quad \forall\ i = 1, 2, \ldots, \mathrm{S}^c, \quad c = 1, 2, \ldots, \mathrm{NC} \tag{1}$$

$$\Pi^{c,i}_{\max} = \max_{p^c_{ij}, j=1,2,\ldots,\mathrm{S}^c} \{\Pi^{c,i}\}, \quad \forall\ i = 1, 2, \ldots, \mathrm{S}^c, \quad c = 1, 2, \ldots, \mathrm{NC}$$

such that

$$p^c_{ij} \in [\underline{p}^c_{ij}, \bar{p}^c_{ij}] \tag{2}$$

$$\sum_{j=1}^{\mathrm{S}^c} p^c_{ij} = 1 \tag{3}$$

$$\mathbf{\Pi}^c = \mathbf{\Pi}^c \cdot \mathbf{P}^c \tag{4}$$

The constraint of Eq. (2) means that the transition probability from state i to state j is not known precisely and can take values in the interval $[\underline{p}^c_{ij}, \bar{p}^c_{ij}]$ [27]; the constraint of Eq. (3) refers to a fundamental property of Markov and semi-Markov processes, i.e., the states for each component are exhaustive [43]; finally, Eq. (4) reports the definition of steady-state probability for a Markov process [43]. Notice that the sum of the elements of the vector $\mathbf{\Pi}^c$ is equal to 1. In the case of a semi-Markov process, the output of Eq. (4), i.e., $\mathbf{\Pi}^c$, is weighted by the expected time of residence, τ^i, in a given state, i, before performing a transition [44]: $\xi^{c,i} = \Pi^{c,i} \cdot \tau^i / \sum_{j=1}^{\mathrm{S}^c} \Pi^{c,j} \cdot \tau^j$ for $i = 1, \ldots, \mathrm{S}^c$. Notice that the optimization problems (Eq. (1)) can be solved by performing an exhaustive greedy search within the probability intervals $[\underline{p}^c_{ij}, \bar{p}^c_{ij}]$, if the dimensions of the corresponding transition probability matrices are relatively small (e.g., below 4×4), otherwise, alternative intelligent techniques should be sought, e.g., metaheuristic methods such as genetic algorithms (GAs) [27]. In this work, we resort to GAs for arcs a_b, b_c, c_d, and d_e (whose transition probability matrices are 7×7), whereas we perform an exhaustive search for all the other arcs. In Appendix B, the operative steps to obtain the lower and upper bounds of the steady-state probabilities (i.e., $[\mathbf{\Pi}^c_{\min}, \mathbf{\Pi}^c_{\max}]$) by performing an exhaustive search are detailed, and the need to resort to alternative intelligent techniques when the dimension of the transition probability matrix increases is discussed.
2. Identify the CDFs of the product delivered at each demand node at steady-state for all the possible combinations of components steady-state probabilities found at step 1 above:

   a. For each component c, $c = 1, 2, \ldots, \mathrm{NC}$, let the steady-state probabilities, $\Pi^{c,i}$, $i = 1, 2, \ldots, \mathrm{S}^c$, range within the corresponding interval $[\Pi^{c,i}_{\min}, \Pi^{c,i}_{\max}]$, $i = 1, 2, \ldots, \mathrm{S}^c$, to obtain a set of Q^c vectors of steady-state probabilities, $\{\mathbf{\Pi}^{c,1}, \mathbf{\Pi}^{c,2}, \ldots, \mathbf{\Pi}^{c,q}, \ldots, \mathbf{\Pi}^{c,\mathrm{Q}^c}\}$: $q = \{1, \ldots, \mathrm{Q}^c\}$, such that $\sum_{i=1}^{\mathrm{S}^c} \Pi^{c,q,i} = 1$, $q = 1, \ldots, \mathrm{Q}^c$. Notice that this gives rise to $\mathrm{Q}^1 * \mathrm{Q}^2 * \cdots * \mathrm{Q}^{\mathrm{NC}} = N_{\mathrm{tot}}$ possible combinations of steady-state probability vectors of the system components, i.e., to N_{tot} steady-state probability vectors for the entire system.
   b. For all the NC components, select one steady-state probability vector among the set $\mathbf{\Pi}^{c,q}$, $c = 1, 2, \ldots, \mathrm{NC}$, $q \in \{1, \ldots, \mathrm{Q}^c\}$ (generated at step *a* above); in other words, this amounts to selecting one of the $\mathrm{Q}^1 * \mathrm{Q}^2 * \cdots * \mathrm{Q}^{\mathrm{NC}} = N_{\mathrm{tot}}$ steady-state probability vectors for the entire SoS.
   c. Fixing the SoS steady-state probability vector selected in step *b*, randomly sample the states $\zeta^{c,i}$ (i.e., the capacities), $i = \in \{1, \ldots, \mathrm{S}^c\}$, of all the components of the system (i.e., arcs). Then, compute the product delivered at the demand nodes propagating the flow in each component of the SoS through the GTST–DMLD (see Sec. 3.2).
   d. Repeat step *c* a large number of times (e.g., 1000 in this work) and obtain the CDF for the product delivered at each demand node.
   e. Repeat steps *c* and *d* for another combination of the steady-state probability vectors, $\mathbf{\Pi}^{c,q}$, $c = 1, 2, \ldots, \mathrm{NC}$, $q \in \{1, \ldots, \mathrm{Q}^c\}$, of all the NC components, until all the N_{tot} possible combinations of the steady-state probability vectors of the SoS are explored.

   At the end of steps *a–e*, an ensemble of CDFs for each demand nodes is obtained, one for each of the N_{tot} possible combinations of steady-state probabilities of the entire SoS.
3. Identify the extreme minimum and maximum CDFs (i.e., the enveloping p-box of the CDFs) of the product delivered at the demand nodes that bound the set of CDFs produced at step 2 above.

4.2 Recovery Time. The time needed to recover the SoS from the worst scenario (i.e., the one characterized by components in the

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

worst state) to a level in which all the demand nodes are satisfied is carried out by three main steps:

1. *Processing the epistemic uncertainties by interval analysis*: this step lead to the identification of K^c transition probability matrices $\mathcal{P}^{c,k}$, $c = 1, 2, \ldots, NC$, $k = 1, 2, \ldots, K^c$, composed of single values; in addition, for the NS components described by semi-Markov process, this step leads to the identification of H^c matrices $\mathbf{Mu}^{c,h}$, $c \in \{1, 2, \ldots, NC\}$, $h \in \{1, 2, \ldots, H^c\}$, composed of single values of the mean of the holding-time distributions.
2. *Evaluation of the SoS performance (i.e., recovery capacity) by Monte Carlo simulation*: this step leads to the determination of a set of CDFs of the time needed to recover the SoS, one for each possible combination of state probability matrices sampled.
3. *Postprocessing the results obtained at the previous step 2*: this step leads to the identification of two extreme upper and lower CDFs that bound the set of CDFs produced at step 2 above.

In more details, step 1 is described in Appendix B (steps B1–B3) and step 2 instead is performed as follows:

a. Randomly select NC matrices $\mathcal{P}^{c,k}$, $c = 1, 2, \ldots, NC$, $k \in \{1, 2, \ldots, K^c\}$, for all the NC components of the SoS and NS matrices $\mathbf{Mu}^{c,h}$, $h \in \{1, 2, \ldots, H^c\}$, for the NS components c described by a semi-Markov process.

b. Set $u = 1$ (counter of the number of simulations).

c. Initialize the state of the components at the worst state ($\zeta^{c,i}$, $i = 1$, $c = 1, 2, \ldots, NC$): in this state, configuration of the SoS, the product delivered to the demand nodes is lower than the optimum required.

d. Initialize the following time variables:

- System simulation time, $t = 0$, starting time of the simulation: this variable represents the current simulation time and is needed to compute the recovery time of the SoS;
- components' state transition time $ts^c = \Delta t$, $c = 1, 2, \ldots, NC$, where Δt is the time step of the simulation ($\Delta t = 1$ in arbitrary units, in this work): these time variables (ts^c, $c = 1, 2, \ldots, NC$) are needed to determine if the component c can perform a state transition at a given time step t, as illustrated in the next step *e*; they are set to one, since at this time step, all the components perform the first state transition.

e. Set $t = t + \Delta t$: if $t = ts^c$, then the component c, $c \in \{1, \ldots, NC\}$, performs a state transition: then, randomly sample its new state from the matrix $\mathcal{P}^{c,k}$ ($k \in \{1, \ldots, K^c\}$) selected at step *a* and update the variable ts^c as follows:

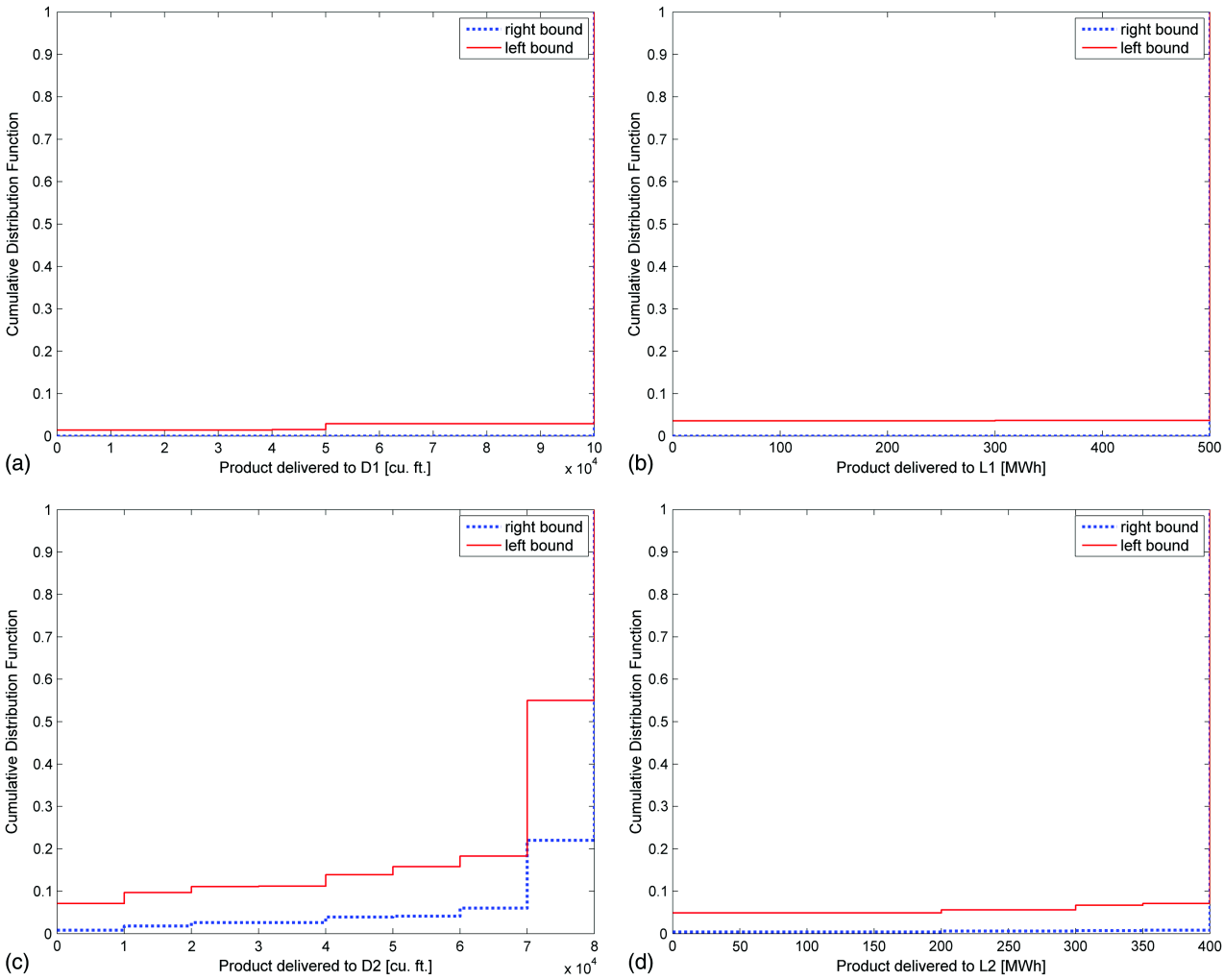


Fig. 8 Right (dotted line) and left (solid line) cumulative distribution functions of the product delivered to the nodes D1, D2, L1, and L2 at the steady-state (1 cu. ft. ≈ 0.028 m³)

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

Table 1 Upper and lower probabilities that the product delivered to the demand nodes (D1, D2, L1, and L2) exceeds the corresponding requested threshold value (1 cu. ft. $\approx$ 0.028 m^3)

D1 $\geq d_1^* = 95{,}000$ cu. ft. [lower, upper]	D2 $\geq d_2^* = 75{,}000$ cu. ft. [lower, upper]	L1 $\geq l_1^* = 475$ MWh [lower, upper]	L2 $\geq l_2^* = 375$ MWh [lower, upper]
[0.971, 1]	[0.450, 0.780]	[0.963, 1]	[0.929, 0.992]

- If c is described by a Markov process, $ts^c = ts^c + \Delta t$, since a state transition occurs at each time step.
- If c is described by a semi-Markov process, $ts^c = ts^c + t^*$, where t^* is the time of the next transition that is sampled from the corresponding holding-time distribution with mean value taken from the matrix $\mathbf{Mu}^{c,h}$, $h \in \{1, 2, \ldots, \mathrm{H}^c\}$, selected at the previous step a. The sampled value t^* is rounded to the nearest integer except when it is zero; in this case, the value is rounded to one.

  Check $t = ts^c$ for all the components c, $c = 1, 2, \ldots, \mathrm{NC}$.

f. Evaluate the product delivered to the demand nodes at time t by adopting the GTST–DMLD (see Sec. 3.2), taking into account the state transition of the components in the previous step *e*.

g. Repeat steps *e–f* until the product delivered to the demand nodes is equal to, or higher than, the optimum required: the corresponding value of recovery time (tr^u) is then recorded for the simulation u.

h. Set $u = u + 1$ and repeat steps *c–g* a large number of times (e.g., 1000 in this work).

i. A CDF of the recovery time of the SoS is identified for a combination of state probability matrices $\mathcal{P}^{c,k}$, $c = 1, 2, \ldots, \mathrm{NC}$, $k \in \{1, 2, \ldots, \mathrm{K}^c\}$, selected at step *a*.

j. Repeat the entire procedure (steps *a–i*) a large number of times (e.g., 10,000 in this work) to explore many different combinations of probability matrices $\mathcal{P}^{c,k}$, $c = 1, 2, \ldots, \mathrm{NC}$, $k \in \{1, 2, \ldots, \mathrm{K}^c\}$.

At the end of the procedure, a set of CDFs of the recovery time of the performance of the SoS is obtained.

The results are processed at step 3, where the minimum and maximum CDFs (i.e., the enveloping p-box of the CDFs) of the recovery time that bound the set of CDFs obtained at step 2 above are identified, and the 99th percentile of the distributions is computed as a measure of the recovery time.

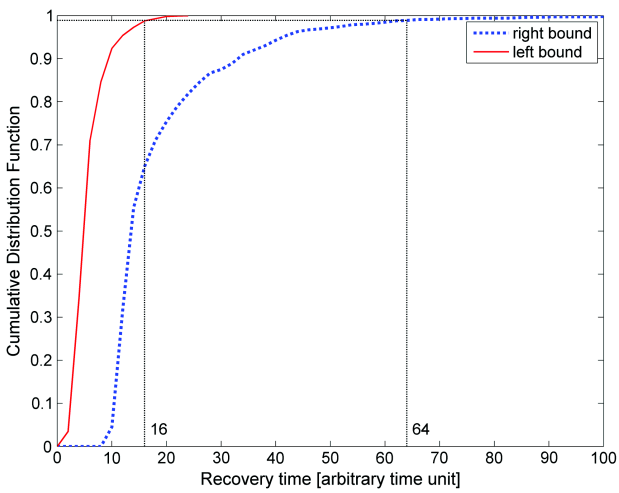


Fig. 9 Right (dotted line) and left (solid line) cumulative distribution functions of the recovery time of the supply of the demand nodes, starting from the worst scenario

5 Results

Figure 8 shows the lower (dotted line) and upper (solid line) CDFs of the gas and the electricity delivered at steady-state to the demand nodes D1, D2 and L1, L2, respectively, obtained by the procedure illustrated in Sec. 4.1. Table 1 reports the corresponding (upper and lower) probabilities that the product delivered to the demand nodes, D1, D2, L1, and L2, exceeds the following threshold values: $d_1^* = 95{,}000$ cu. ft., $d_2^* = 75{,}000$ cu. ft., $l_1^* = 475$ MWh, and $l_2^* = 375$ MWh (i.e., the probabilities that the corresponding demands are satisfied).

It can be seen that in general the probability of satisfying demand nodes D1 and L1 is higher than for nodes D2 and L2: their threshold values are satisfied, in the worst case, with probability equal to 0.971 and 0.963, respectively. On the other hand, node D2 is the least supplied: the upper and lower probabilities which the product delivered to it exceeds the corresponding threshold value are low, i.e., 0.450 and 0.780, respectively. This is due to the fact that node D2 can be satisfied by only one path that presents high epistemic uncertainty in the arc capacities (a_b, b_c, c_d, and d_e). On the other hand, node L2 is satisfied with probability between 0.929 and 0.992 even if it is the farthest node from the input sources (and, thus, more affected by uncertainty due to the uncertainties in the arc capacities): this is due to the presence of two redundant paths that allow its supply by arcs E1_G1 and E2_G2.

Figure 9 illustrates the lower (dotted line) and upper (solid line) CDFs of the time needed to restore the SoS to a level in which all the demand nodes are satisfied, starting from the worst scenario.

The gap between the CDFs reflects the epistemic uncertainty in the transition probability values. In the figure, the 99th percentile of the CDFs is also reported as a measure of the recovery time.

6 Conclusions

In this paper, we have introduced a SoS framework for the analysis of the robustness and recovery of CIs. The analysis by such framework builds on the construction of a GTST–DMLD for system modeling and Monte Carlo simulation for the quantitative evaluation of the system performance at steady-state. The development of the framework in practice has been shown considering the same example created by Ref. [1] consisting of two interdependent infrastructures, gas and electric power networks, and a SCADA system connected to the gas network.

In the original framework of Ref. [1], the analysis of the robustness and recovery capacity of CIs has been performed by adopting network flow algorithms combined with stochastic processes. The adoption of the GTST–DMLD modeling framework makes the analysis of the robustness and recovery capacity of CIs accessible to a different audience than the original work by Ref. [1]. Actually, there is a community of analysts who are much more comfortable using concepts inherent in the GTST–DMLD framework than using methods based on network flow algorithms and stochastic processes. The model put forth by Ref. [1] was based on the analysis methods of operations research, whereas the GTST–DMLD framework has its roots in the reliability and risk

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

analysis of nuclear power plants and complex electromechanical systems.

The framework here developed has shown the capability of representing, modeling, and quantitatively accounting for: (1) the dependencies and interdependencies among the components of a CI and between different CIs, respectively, (2) the variability in the states of the components (by adopting a multistate model), and (3) the epistemic uncertainty in the transition probabilities between different components states (by interval analysis).

The results and insights obtained can help to improve the global SoS performance by improving the structural response of specific arcs that more easily turn into damage states or by developing a more redundant network that allows the supply of the product from different paths.

Appendix A: Imprecise (Interval) Probabilities

To understand the meaning of imprecise probabilities (or interval probabilities), consider an event A. Uncertainty about whether it occurs is represented by a lower probability $\underline{P}(\mathrm{A})$ and an upper probability $\bar{P}(\mathrm{A})$, giving rise to a probability interval $[\underline{P}(\mathrm{A}), \bar{P}(\mathrm{A})]$, where $0 \leq \underline{P}(\mathrm{A}) \leq \bar{P}(\mathrm{A}) \leq 1$. The difference $\Delta P(\mathrm{A}) = \bar{P}(\mathrm{A}) - \underline{P}(\mathrm{A})$ is called the *imprecision* in the representation of the event A. Single-valued probabilities are a special case of no imprecision, and the lower and upper probabilities coincide.

Williams [45] developed a mathematical framework for imprecise probabilities, based on de Finetti's betting interpretation of probability [11]. This foundation was further developed independently by Kuznetsov and Walley (the former only published in Russian), see Refs. [14,15]. Following de Finetti's betting interpretation, the lower probability is interpreted as the maximum price for which one would be willing to buy a bet which pays one if A occurs and zero if not, and the upper probability as the minimum price for which one would be willing to sell the same bet. If the upper and lower values are equal, the interval is reduced to a precise probability. These references, and Ref. [15] in particular, provide an in-depth analysis of imprecise probabilities and their interpretations, with a link to applications to probabilistic reasoning, statistical inference, and decisions.

It is, however, also possible to interpret the lower and upper probabilities using the reference to a standard interpretation of a subjective probability $P(\mathrm{A})$: such an interpretation is indicated by Ref. [46, p. 36]. Consider the subjective probability $P(\mathrm{A})$ and say that the analyst states that his/her assigned degree of belief is greater than the urn chance of 0.10 (the degree of belief of drawing one particular ball from an urn which includes ten balls) and less than the urn chance of 0.5. The analyst is not willing to make any further judgement. Then, the interval [0.10, 0.50] can be considered an imprecision interval for the probability $P(\mathrm{A})$.

Of course, even if the assessor assigns a probability $P(\mathrm{A}) = 0.3$, one may interpret this probability as having an imprecision interval [0.25, 0.34] (as a number in this interval is equal to 0.3 when displaying one digit only), interpreted analogously to the [0.1, 0.5] interval. Hence, imprecision is always an issue in a practical uncertainty analysis context. This imprecision is commonly viewed as a result of measurement problems. The reference to the urn lottery provides a norm to which assessors should aspire, but measurement problems may make the assessor unable to behave according to it (see also the discussion in Ref. [9, p. 32]).

However, other researcher and analysts have a more positive view on the need for such intervals; see the discussions in Refs. [8,22–26]: imprecision intervals are required to reflect phenomena as discussed previously, for example when experts are not willing to express their knowledge more precisely than by using probability intervals.

Imprecise probabilities are also linked to the relative frequency interpretation of probability [10]. The simplest case reflects that the "true" frequentist probability p is in the interval $[\underline{P}(\mathrm{A})\underline{P}, \bar{P}(\mathrm{A})]$ with certainty. More generally and in line with the above interpretations of imprecision intervals based on subjective probabilities $P(\cdot)$, a two-level uncertainty characterization can be formulated (see, e.g., Ref. [13]): $[\underline{P}(\mathrm{A}), \bar{P}(\mathrm{A})]$ is an imprecision interval for the subjective probability $P(a \leq p \leq b)$, where a and b are constants. In the special case that $\underline{P}(\mathrm{A}) = \bar{P}(\mathrm{A})(= q, \text{say})$, we are led to the special case of a $q \cdot 100\%$ credibility interval for p (i.e., with subjective probability q, the true value of p is in the interval $[a, b]$). For further details, the reader is referred to the recent Special Issue on imprecise probabilities appearing in the "Journal of Mechanical Systems and Signal Processing" [30].

Appendix B: Processing Epistemic Uncertainty by Interval Analysis: Detailed Operative Steps

The operative steps carried out to process the epistemic uncertainty by interval analysis, needed for the robustness and recovery analyses of Secs. 4.1 and 4.2, are illustrated in the following.

To recall the notation, the algorithm requires in what follows inputs:

- A state transition probability matrix $\mathbf{P}^c$, $c = 1, \ldots, \mathrm{NC}$, composed of probability intervals $\mathbf{P}^c = \{[\underline{p}^c_{ij}, \bar{p}^c_{ij}]: c = 1, \ldots, \mathrm{NC}, i, j = 1, \ldots, \mathrm{S}^c\}$ for all the NC components c of the system, where i and j are indices representing the state of the component c, and S^c is the total number of states of component c. The state transition probability matrix $\mathbf{P}^c$ assumes this form:

$$\mathbf{P}^c = \begin{array}{c|cccc|} i/j & 1 & 2 & \ldots & \mathrm{S}^c \\ 1 & [\underline{p}^c_{11}, \bar{p}^c_{11}] & [\underline{p}^c_{12}, \bar{p}^c_{12}] & \ldots & [\underline{p}^c_{1S^c}, \bar{p}^c_{1\mathrm{S}^c}] \\ 2 & [\underline{p}^c_{21}, \bar{p}^c_{21}] & [\underline{p}^c_{22}, \bar{p}^c_{22}] & \ldots & [\underline{p}^c_{2\mathrm{S}^c}, \bar{p}^c_{2\mathrm{S}^c}] \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{S}^c & [\underline{p}^c_{\mathrm{S}^c 1}, \bar{p}^c_{\mathrm{S}^c 1}] & [\underline{p}^c_{\mathrm{S}^c 2}, \bar{p}^c_{\mathrm{S}^c 2}] & \ldots & [\underline{p}^c_{\mathrm{S}^c\mathrm{S}^c}, \bar{p}^c_{\mathrm{S}^c\mathrm{S}^c}] \end{array}$$

- A holding time distribution matrix $\mathbf{T}^c$, $c \in \{1, 2, \ldots, \mathrm{NC}\}$, for the NS components described by a semi-Markov process with epistemically uncertain mean μ^c_{ij} represented by an interval of values,

$$\mathbf{T}^c = \{\mathrm{th}^c_{ij} \approx N(\mu^c_{ij}, \sigma^c_{ij}): \mu^c_{ij} \in [\underline{\mu}^c_{ij}, \bar{\mu}^c_{ij}], i, j = 1, \ldots, \mathrm{S}^c\}$$

$$\mathbf{T}^c = \begin{array}{c|cccc|} i/j & 1 & 2 & \ldots & \mathrm{S}^c \\ 1 & \mathrm{N}([\underline{\mu}^c_{11}, \bar{\mu}^c_{11}], \sigma^c_{11}) & \mathrm{N}([\underline{\mu}^c_{12}, \bar{\mu}^c_{12}], \sigma^c_{12}) & \ldots & \mathrm{N}([\underline{\mu}^c_{1S^c}, \bar{\mu}^c_{1\mathrm{S}^c}], \sigma^c_{1\mathrm{S}^c}) \\ 2 & \mathrm{N}([\underline{\mu}^c_{21}, \bar{\mu}^c_{21}], \sigma^c_{21}) & \mathrm{N}([\underline{\mu}^c_{22}, \bar{\mu}^c_{22}], \sigma^c_{22}) & \ldots & \mathrm{N}([\underline{\mu}^c_{2\mathrm{S}^c}, \bar{\mu}^c_{2\mathrm{S}^c}], \sigma^c_{1\mathrm{S}^c}) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \mathrm{S}^c & \mathrm{N}([\underline{\mu}^c_{\mathrm{S}^c 1}, \bar{\mu}^c_{\mathrm{S}^c 1}], \sigma^c_{\mathrm{S}^c 1}) & \mathrm{N}([\underline{\mu}^c_{\mathrm{S}^c 2}, \bar{\mu}^c_{\mathrm{S}^c 2}], \sigma^c_{\mathrm{S}^c 2}) & \ldots & \mathrm{N}([\underline{\mu}^c_{\mathrm{S}^c\mathrm{S}^c}, \bar{\mu}^c_{\mathrm{S}^c\mathrm{S}^c}], \sigma^c_{\mathrm{S}^c\mathrm{S}^c}) \end{array}$$

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

c = S2_DS2 (Semi-Markov)

$\mathbf{P}^c =$

$i\backslash j$	1	2	3
1	0	1	0
2	[0; 0.02]	0	[0.98; 1]
3	[0; 0.02]	[0.98; 1]	0

$i = 2$

All possible combinations for the values of the row $i = 2$

1	2	3	**sum**
0	0	0.98	0.98
0.004	0	0.98	0.984
0.008	0	0.98	0.988
0.012	0	0.98	0.992
0.016	0	0.98	0.996
0.02	0	0.98	1
0.01	0	0.98	0.99
0	0	0.984	0.984
0.004	0	0.984	0.988
0.008	0	0.984	0.992
0.012	0	0.984	0.996
0.016	0	0.984	1
0.02	0	0.984	1.004
0.01	0	0.984	0.994
0	0	0.988	0.988
0.004	0	0.988	0.992
0.008	0	0.988	0.996
0.012	0	0.988	1
…	…	…	…
…	…	…	…

Combinations that give sum 1 for the values of the row $i = 2$

1	0.02	0	0.98
2	0.016	0	0.984
3	0.012	0	0.988
…	…	…	…
$Z^{c,i=2}$	…	…	…

Fig. 10 Exemplification of step B1 for the row $i = 2$ of the probability matrix $\mathbf{P}^c$, c = S2_DS2, to identify $Z^{c,i}$ combinations of transition probability values

By way of example and for clarity of illustration, in the following, we refer to component c = S2_DS2 of Fig. 1, whose transition probability matrix $\mathbf{P}^c$ and holding-time distributions $\mathbf{T}^c$ are reported in Fig. 2.

The algorithm proceeds as follows:

B1. Select a component c, $c \in \{1, 2, \ldots, \mathrm{NC}\}$, and a row i, $i \in \{1, 2, \ldots, \mathrm{S}^c\}$, of matrix $\mathbf{P}^c$ whose dimension is $\mathrm{S}^c \times \mathrm{S}^c$ (see Fig. 10, left): for component c = S2_DS2, $\mathbf{P}^c$ has dimension 3×3. Letting the probabilities p^c_{ij}, $j = 1, 2, \ldots, \mathrm{S}^c$, vary within the corresponding intervals $[\underline{p}^c_{ij}, \bar{p}^c_{ij}]$, identify all the possible combinations of the probability values in row i (Fig. 10, middle, with reference to row $i = 2$). Given the assumption that the component states are exhaustive [Eq. (3) in Sec. 4], only those combinations of probabilities guaranteeing $\sum_{j=1}^{\mathrm{S}^c} p^c_{ij} = 1$ are considered (Fig. 10, right). The total number of suitable combination for row i is referred to as $Z^{c,i}$.

If component c is described by a semi-Markov process, select also row i of matrix $\mathbf{T}^c$. Letting the mean values, μ^c_{ij}, $j = 1, 2, \ldots, \mathrm{S}^c$, of the holding-time distributions vary within the corresponding intervals $[\underline{\mu}^c_{ij}, \bar{\mu}^c_{ij}]$, identify all the possible combinations of the mean values of row i (Fig. 11). The total number of combinations obtained for the mean is referred to as $\mathrm{M}^{c,i}$ for row i.

c = S2_DS2 (Semi-Markov)

$\mathbf{T}^c =$

i\j	1	2	3
1	–	N([2; 6], 1)	–
2	N([7; 13], 3)	–	N([2; 6], 1)
3	N([7; 13], 3)	N([17; 23], 2)	–

$i = 2$

All possible combinations for the mean values of the row $i = 2$

7	0	2	1
8	0	2	2
9	0	2	3
10	0	2	4
11	0	2	5
12	0	2	6
13	0	2	7
7	0	3	8
8	0	3	9
9	0	3	10
10	0	3	11
11	0	3	12
12	0	3	13
13	0	3	14
7	0	4	15
8	0	4	16
9	0	4	17
10	0	4	18
11	0	4	19
…	…	…	…
…	…	…	$\mathrm{M}^{c,i=2}$

Fig. 11 Exemplification of step B1 for the row $i = 2$ of the holding-time distribution matrix $\mathbf{T}^c$, c = S2_DS2, to identify $\mathrm{M}^{c,i}$ combinations of mean values

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

c = S2_DS2 (Semi-Markov)

Combinations that give sum 1 for the values of the row $i = 1$

$Z^{c,i=1}=1$

0	1	0

Combinations that give sum 1 for the values of the row $i = 2$

$Z^{c,i=2}=7$

0.02	0	0.98
0.016	0	0.984
0.012	0	0.988
0.008	0	0.992
0.004	0	0.996
0	0	1
0.01	0	0.99

Combinations that give sum 1 for the values of the row $i = 3$

$Z^{c,i=3}=7$

0.02	0.98	0
0.016	0.984	0
0.012	0.988	0
0.008	0.992	0
0.004	0.996	0
0	1	0
0.01	0.99	0

Transition probability matrices:

$\mathcal{P}^{c,1} =$

$i\backslash j$	1	2	3
1	0	1	0
2	0.02	0	0.98
3	0.02	0.98	0

$\cdots$

$\mathcal{P}^{c,\mathrm{K}^c} =$

$i\backslash j$	1	2	3
1	0	1	0
2	0.01	0	0.99
3	0.01	0.99	0

Fig. 12 Exemplification of step B2 to identify a set transition probability matrix $\mathcal{P}^{c,k}$, $k = 1, \ldots, \mathrm{K}^c$, for component c = S2_DS2, given the $\sum_{i=1}^{\mathrm{S}^c} Z^{c,i}$ vectors obtained at step B1

Repeat this step B1 for all the rows $i = 1, 2, \ldots, \mathrm{S}^c$ of the matrices $\mathbf{P}^c$ and $\mathbf{T}^c$.

At the end of this step, $\sum_{i=1}^{\mathrm{S}^c} Z^{c,i}$, $c \in \{1, \ldots, \mathrm{NC}\}$, vectors of probability values, and $\sum_{i=1}^{\mathrm{S}^c} M^{c,i}$, $c \in \{1, \ldots, \mathrm{NC}\}$, vectors of mean values, are obtained. For example, in Fig. 12 (top), 15 transition probability vectors ($\sum_{i=1}^{\mathrm{S}^c} Z^{c,i} = 15$, c = S2_DS2, $i = 1, \ldots, \mathrm{S}^c = 3$) are obtained for component S2_DS2: one vector for row $i = 1\,(Z^{c,1} = 1)$, seven vectors for row $i = 2\,(Z^{c,2} = 7)$, and seven vectors for row $i = 3\,(Z^{c,3} = 7)$.

B2. Obtain K^c transition probability matrices $\mathcal{P}^{c,k}$ $[\mathrm{S}^c \times \mathrm{S}^c]$, $k = 1, \ldots, \mathrm{K}^c$, for component c, $c \in \{1, \ldots, \mathrm{NC}\}$, by performing the combinations of all the $\mathrm{Z}^{c,i}$ vectors obtained for all the rows i, $i = 1, \ldots, \mathrm{S}^c$, at the previous step B1 (Fig. 12, bottom).

If the component c is described by a semi-Markov process, find also H^c matrices $\mathbf{Mu}^{c,h}$ $[\mathrm{S}^c \times \mathrm{S}^c]$, $h = 1, 2, \ldots, \mathrm{H}^c$, of the mean values of the holding-time distribution by performing the combinations of all the $\mathrm{M}^{c,i}$ vectors obtained for all the rows i, $i = 1, \ldots, \mathrm{S}^c$, at the previous step B1.

B3. Repeat steps B1—B2 for each component ($c = 1, 2, \ldots, \mathrm{NC}$) of the SoS. All the NC components are, then, associated with a set of possible transition probabilities matrices $\mathcal{P}^{c,k}$, $k = 1, \ldots, \mathrm{K}^c$ (resulting from the imprecise transition probabilities). In addition, the components described by a semi-Markov process (i.e., NS components) are also associated with a set of H^c matrices, $\mathbf{Mu}^{c,h}$, $h = 1, 2, \ldots, \mathrm{H}^c$, containing the mean values of the corresponding holding time distributions.

Steps B1–B3 above are needed in the evaluation of the recovery time, and they precede step 2 of the algorithm of Sec. 4.2. Instead, in order to evaluate the steady-state probabilities necessary to perform the robustness analysis of Sec. 4.1, the procedure continues as follows:

B4. Select a component c and compute the steady-state probability vectors $\mathbf{\Pi}^{c,k}$ (or $\xi^{c,k}$ if c is described by a semi-Markov process), $k = 1, \ldots, \mathrm{K}^c$, one for each transition probability matrix $\mathcal{P}^{c,k}$, $k = 1, \ldots, \mathrm{K}^c$, obtained at the previous step B3. If component c is described by a Markov process, Eq. (4) (Sec. 4.1) is adopted; otherwise, if component c is described by a semi-Markov process, the output of Eq. (4) is weighted by the expected time of residence, τ^i, in a given state i, $i = 1, \ldots, \mathrm{S}^c$ [44]: $\xi^{c,k,i} = \Pi^{c,k,i} \cdot \tau^i / \sum_{j=1}^{\mathrm{S}^c} \Pi^{c,k,j} \cdot \tau^j$, $i = 1, \ldots, \mathrm{S}^c$, $k = 1, \ldots, \mathrm{K}^c$. For illustration purposes, Fig. 13 shows examples of the matrices $\mathcal{P}^{c,k}$, $k \in \{1, \ldots, \mathrm{K}^c\}$, and $\mathbf{Mu}^{c,h}$, $h \in \{1, \ldots, \mathrm{H}^c\}$ for component c = S2_DS2. Then, the procedure for evaluating the steady-state probability vectors $\mathbf{\Pi}^{c,k}$ and $\boldsymbol{\xi}^{c,k}$ for Markov and semi-Markov processes, respectively, is detailed.

B5. Compute the minimum and maximum steady-state probabilities $\Pi_{\min}^{c,i}$ and $\Pi_{\max}^{c,i}$, $c = 1, 2, \ldots, \mathrm{NC}$, for each row (i.e., component state) i, $i = 1, \ldots, \mathrm{S}^c$, as follows:

$\Pi_{\min}^{c,i} = \min_k(\Pi^{c,1,i}, \Pi^{c,2,i}, \ldots, \Pi^{c,k,i}, \ldots, \Pi^{c,\mathrm{K}^c,i})$ and $\Pi_{\max}^{c,i} = \max_k(\Pi^{c,1,i}, \Pi^{c,2,i}, \ldots, \Pi^{c,k,i}, \ldots, \Pi^{c,\mathrm{K}^c,i})$, if component c is described by a Markov process, or $\Pi_{\min}^{c,i} = \min_k(\xi^{c,1,i}, \xi^{c,2,i}, \ldots, \xi^{c,k,i}, \ldots, \xi^{c,\mathrm{K}^c,i})$ and $\Pi_{\max}^{c,i} = \max_k(\xi^{c,1,i}, \xi^{c,2,i}, \ldots, \xi^{c,k,i}, \ldots, \xi^{c,\mathrm{K}^c,i})$, if component c is described by a semi-Markov process. Each component c, $c = 1, 2, \ldots, \mathrm{NC}$, is then associated with a vector of imprecise (interval) steady-state probabilities

$$\mathbf{\Pi}^c \in \begin{array}{c|c|} i & \\ 1 & [\Pi_{\min}^{c,i=1}, \Pi_{\max}^{c,i=1}] \\ 2 & [\Pi_{\min}^{c,i=2}, \Pi_{\max}^{c,i=2}] \\ \ldots & \ldots \\ \mathrm{S}^c & [\Pi_{\min}^{c,i=\mathrm{S}^c}, \Pi_{\max}^{c,i=\mathrm{S}^c}] \end{array}$$

B6. Letting the steady-state probabilities $\Pi^{c,i}$, $i = 1, 2, \ldots, \mathrm{S}^c$, of component c vary within the corresponding intervals $[\Pi_{\min}^{c,i}, \Pi_{\max}^{c,i}]$, identify all the possible combinations of the probability values to obtain a set of Q^c steady-state probability vectors (obviously the sum of the components of each vector is equal to one) (see step 2a of Sec. 4.1).

B7. Repeat steps B4—B6 for each component ($c = 1, 2, \ldots, \mathrm{NC}$) of the SoS.

Notice that in the procedure above (steps B1—B7), extreme lower and upper steady-state probabilities $\mathbf{\Pi}_{\min}^c$ and $\mathbf{\Pi}_{\max}^c$, respectively, are obtained by resorting to a exhaustive greedy search: this amounts to identifying (in principle) all the possible combinations between (in principle) all the possible probability values in the corresponding intervals. For example, in step B1, the probabilities p_{ij}^c are allowed to range within their intervals $[\underline{p}_{ij}^c, \bar{p}_{ij}^c]$: for the

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

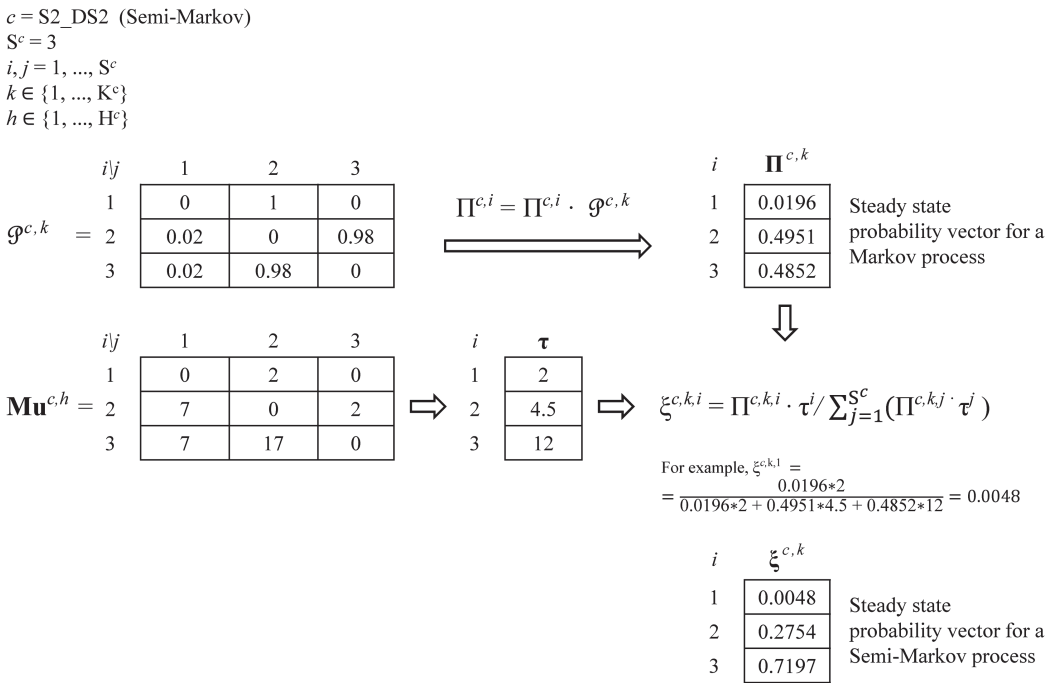


Fig. 13 Exemplification of step B4 to identify the steady-state probability vectors for Markov and semi-Markov processes

sake of practical computation, we identify, e.g., seven discrete values within each interval $[\underline{p}^c_{ij}, \bar{p}^c_{ij}]$. If we assume that the number of states is $S^c = 3$, then the total number of possible combinations between the transition probability values is 343; if the number of states is 7, i.e., $S^c = 7$, the number of possible combinations increases to 823,543. Obviously, the higher the number of discrete values taken within the intervals $[\underline{p}^c_{ij}, \bar{p}^c_{ij}]$ the more precise the results, but the more prohibitive the computational cost. For these reasons, when the dimension of the transition probability matrix increases, we need to resort to alternative (intelligent) techniques: in other words, in order to obtain the lower and upper steady-state probabilities $\mathbf{\Pi}^c_{\min}$ and $\mathbf{\Pi}^c_{\max}$, respectively, we do not analyze all the possible combinations between all values of $p^c_{ij} \in [\underline{p}^c_{ij}, \bar{p}^c_{ij}]$; instead, we intelligently explore only those combinations that driving the search appear as the most "promising" for the maximization and minimization of $\mathbf{\Pi}^c$. In this work, we resort to GAs for the analysis of arcs a_b, b_c, c_d, and d_e, the transition probability matrices of which have size 7×7. In particular, we run the MATLAB function "ga" twice to find the minimum and maximum steady-state probability vectors $\mathbf{\Pi}^c_{\min}$ and $\mathbf{\Pi}^c_{\max}$, respectively. In more details, Eq. (4) of Sec. 4.1 represents the function to be optimized (i.e., minimized and maximized, respectively) by the GA, Eq. (3) of Sec. 4.1 represents the equality constraints to satisfy, and Eq. (2) shows the upper and lower bounds of the transition probabilities p^c_{ij} needed in Eq. (4).

Acknowledgment

The authors thank the anonymous referees for their critical comments that has helped improve the paper.

References

[1] Nozick, L. K., Turnquist, M. A., Jones, D. A., Davis, J. R., and Lawton, C. R., 2005, "Assessing the Performance of Interdependent Infrastructures and Optimising Investments," Int. J. Crit. Infrastruct., **1**(2–3), pp. 144–154.
[2] Adachi, T., and Ellingwood, B. R., 2008, "Serviceability of Earthquake-Damaged Water Systems: Effects of Electrical Power Availability and Power Backup Systems on System Vulnerability," Reliab. Eng. Syst. Saf., **93**(1), pp. 78–88.
[3] Ferrario, E., and Zio, E., 2014, "Goal Tree Success Tree-Dynamic Master Logic Diagram and Monte Carlo Simulation for the Safety and Resilience Assessment of a Multistate System of Systems," Eng. Struct., **59**, pp. 411–433.
[4] Apostolakis, G., 1990, "The Concept of Probability in Safety Assessments of Technological Systems," Science, **250**(4986), pp. 1359–1364.
[5] NASA, 2010, "Risk-Informed Decision Making Handbook," Technical Report No. NASA/SP-2010-576, Version 1.0.
[6] US NRC, 2009, "Guidance on the Treatment of Uncertainties Associated With PRAs in Risk-Informed Decision Making," Technical Report No. NUREG-1855, US Nuclear Regulatory Commission, Washington, DC.
[7] Sallak, M., Schon, W., and Aguirre, F., 2013, "Reliability Assessment for Multi-State Systems under Uncertainties Based on the Dempster-Shafer Theory," IIE Trans., **45**(9), pp. 995–1007.
[8] Aven, T., and Zio, E., 2011, "Some Considerations on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making," Reliab. Eng. Syst. Saf., **96**(1), pp. 64–74.
[9] Bernardo, J. M., and Smith, A. F. M., 1994, *Bayesian Theory*, Wiley, Chichester.
[10] Coolen, F. P. A., and Utkin, L. V., 2007, "Imprecise Probability: A Concise Overview," Risk, Reliability and Societal Safety, Three Volume Set: Proceedings of the European Safety and Reliability Conference 2007 (ESREL 2007), Stavanger, Norway, June 25–27, 2007, T. Aven, and J. E. Vinnem, eds., Taylor & Francis, London, pp. 1959–1966.
[11] De Finetti, B., 1974, *Theory of Probability*, Wiley, New York.
[12] Hu, Y. S., and Modarres, M., 1999, "Evaluating System Behavior Through Dynamic Master Logic Diagram (DMLD) Modeling," Reliab. Eng. Syst. Saf., **64**(2), pp. 241–269.
[13] Kozine, I. O., and Utkin, L. V., 2002, "Processing Unreliable Judgements With an Imprecise Hierarchical Model," Risk Decis. Policy, **7**(3), pp. 325–339.
[14] Kuznetsov, V. P., 1991, *Interval Statistical Models*, Radio i Svyaz, Moscow (in Russian).
[15] Walley, P., 1991, *Statistical Reasoning With Imprecise Probabilities*, Chapman and Hall, New York.
[16] Beer, M., and Ferson, S., 2013, "Special Issue of Mechanical Systems and Signal Processing "Imprecise Probabilities—What Can They Add to Engineering Analyses?"," Mech. Syst. Signal Process., **37**(1–2), pp. 1–3.
[17] Beer, M., Ferson, S., and Kreinovich, V., 2013, "Imprecise Probabilities in Engineering Analyses," Mech. Syst. Signal Process., **37**(1–2), pp. 4–29.
[18] Blockley, D., 2013, "Analysing Uncertainties: Towards Comparing Bayesian and Interval Probabilities'," Mech. Syst. Signal Process., **37**(1–2), pp. 30–42.
[19] Crespo, L. G., Kenny, S. P., and Giesy, D. P., 2013, "Reliability Analysis of Polynomial Systems Subject to P-Box Uncertainties," Mech. Syst. Signal Process., **37**(1–2), pp. 121–136.
[20] Jalal-Kamali, A., and Kreinovich, V., 2013, "Estimating Correlation Under Interval Uncertainty," Mech. Syst. Signal Process., **37**(1–2), pp. 43–53.

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

[21] Mehl, C. H., 2013, "P-Boxes for Cost Uncertainty Analysis," Mech. Syst. Signal Process., **37**(1–2), pp. 253–263.
[22] Ferson, S., and Ginzburg, L. R., 1996, "Different Methods Are Needed to Propagate Ignorance and Variability," Reliab. Eng. Syst. Saf., **54**(2–3), pp. 133–144.
[23] Ferson, S., and Hajagos, J. G., 2004, "Arithmetic With Uncertain Numbers: Rigorous and (Often) Best Possible Answers," Reliab. Eng. Syst. Saf., **85**(1–3), pp. 135–152.
[24] Ferson, S., Kreinovich, V., Hajagos, J., Oberkampf, W., and Ginzburg, L., 2007, "Experimental Uncertainty Estimation and Statistics for Data Having Interval Uncertainty," Sandia National Laboratories, Setauket, New York, SAND2007-0939.
[25] Ferson, S., Moore, D. R. J., Van Den Brink, P. J., Estes, T. L., Gallagher, K., Connor, R. O., and Verdonck, F., 2010, "Bounding Uncertainty Analyses," *Application of Uncertainty Analysis to Ecological Risks of Pesticides*, W. J. Warren-Hicks, and A. Hart, eds., CRC Press, Boca Raton, pp. 89–122.
[26] Ferson, S., and Tucker, W. T., 2006, "Sensitivity in Risk Analyses With Uncertain Numbers," Sandia National Laboratories, Setauket, New York, *SAND2006-2801*.
[27] Buckley, J. J., 2004, "Fuzzy Markov Chains," *Fuzzy Probabilities and Fuzzy Sets for Web Planning*, Springer, Berlin, pp. 35–43.
[28] Kalos, M. H., and Whitlock, P. A., 1986, *Monte Carlo Methods. Volume 1: Basics*, Wiley, New York.
[29] Zio, E., 2013, *The Monte Carlo Simulation Method for System Reliability and Risk Analysis* (Springer Series in Reliability Engineering), Springer, London.
[30] MSSP, 2013, "Special Issue of Mechanical Systems and Signal Processing "Imprecise Probabilities-What Can They Add to Engineering Analyses?"," Mech. Syst. Signal Process., **37**(1–2), pp. 1–263.
[31] Muscolino, G., and Sofi, A., 2013, "Bounds for the Stationary Stochastic Response of Truss Structures With Uncertain-but-Bounded Parameters," Mech. Syst. Signal Process., **37**(1–2), pp. 163–181.
[32] Pannier, S., Waurick, M., Graf, W., and Kaliske, M., 2013, "Solutions to Problems With Imprecise Data—An Engineering Perspective to Generalized Uncertainty Models," Mech. Syst. Signal Process., **37**(1–2), pp. 105–120.
[33] Reid, S. G., 2013, "Probabilistic Confidence for Decisions Based on Uncertain Reliability Estimates," Mech. Syst. Signal Process., **37**(1–2), pp. 229–239.
[34] Sankararaman, S., and Mahadevan, S., 2013, "Distribution Type Uncertainty Due to Sparse and Imprecise Data," Mech. Syst. Signal Process., **37**(1–2), pp. 182–198.
[35] Zhang, H., Dai, H., Beer, M., and Wang, W., 2013, "Structural Reliability Analysis on the Basis of Small Samples: An Interval Quasi-Monte Carlo Method," Mech. Syst. Signal Process., **37**(1–2), pp. 137–151.
[36] Ferson, S., 2005, *Bayesian Methods in Risk Assessment*, Applied Biomathematics, Setauket, New York, www.ramas.com/bayes.pdf.
[37] Karanki, D. R., Kushwaha, H. S., Verma, A. K., and Ajit, S., 2009, "Uncertainty Analysis Based on Probability Bounds (P-Box) Approach in Probabilistic Safety Assessment," Risk Anal., **29**(5), pp. 662–675.
[38] Limbourg, P., and De Rocquigny, E., 2010, "Uncertainty Analysis Using Evidence Theory—Confronting Level-1 and Level-2 Approaches With Data Availability and Computational Constraints," Reliab. Eng. Syst. Saf., **95**(5), pp. 550–564.
[39] Möller, B., Graf, W., and Beer, M., 2003, "Safety Assessment of Structures in View of Fuzzy Randomness," Comput. Struct., **81**(15), pp. 1567–1582.
[40] Pedroni, N., and Zio, E., 2012, "Empirical Comparison of Methods for the Hierarchical Propagation of Hybrid Uncertainty in Risk Assessment, in Presence of Dependences," Int. J. Uncertainty Fuzziness Knowledge Based Syst., **20**(4), pp. 509–557.
[41] Pedroni, N., Zio, E., Ferrario, E., Pasanisi, A., and Couplet, M., 2013, "Hierarchical Propagation of Probabilistic and Non-Probabilistic Uncertainty in the Parameters of a Risk Model," Comput. Struct., **126**, pp. 199–213.
[42] Brissaud, F., Barros, A., Bérenguer, C., and Charpentier, D., 2011, "Reliability Analysis for New Technology-Based Transmitters," Reliab. Eng. Syst. Saf., **96**(2), pp. 299–313.
[43] Zio, E., 2009, *Computational Methods for Reliability and Risk Analysis, Series on Quality, Reliability and Engineering Statistics*, World Scientific Publishing, Singapore.
[44] Barry, L. N., 1995, *Stochastic Modeling: Analysis and Simulation*, McGraw-Hill, New York.
[45] Williams, P. M., 1976, "Indeterminate Probabilities," *Formal Methods in the Methodology of Empirical Sciences*, M. Przełęcki, K. Szaniawski, R. Wójcicki, and G. Malinowski, eds., Reidel, Dordrecht, Holland, pp. 229–246.
[46] Lindley, D. V., 2006, *Understanding Uncertainty*, Wiley, Hoboken, NJ.

Downloaded From: http://risk.asmedigitalcollection.asme.org/ on 07/23/2015 Terms of Use: http://asme.org/terms

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Comparing Network-Centric and Power Flow Models for the Optimal Allocation of Link Capacities in a Cascade-Resilient Power Transmission Network

Yi-Ping Fang, Nicola Pedroni, and Enrico Zio, *Senior Member, IEEE*

***Abstract*—In this paper, we tackle the problem of searching for the most favorable pattern of link capacity allocation that makes a power transmission network resilient to cascading failures with limited investment costs. This problem is formulated within a combinatorial multiobjective optimization framework and tackled by evolutionary algorithms. Two different models of increasing complexity are used to simulate cascading failures in a network and quantify its resilience: a complex network model [namely, the Motter–Lai (ML) model] and a more detailed and computationally demanding power flow model [namely, the ORNL–Pserc–Alaska (OPA) model]. Both models are tested and compared in a case study involving the 400-kV French power transmission network. The results show that cascade-resilient networks tend to have a nonlinear capacity–load relation: In particular, heavily loaded components have smaller unoccupied portions of capacity, whereas lightly loaded links present larger unoccupied portions of capacity (which is in contrast with the linear capacity–load relation hypothesized in previous works of literature). Most importantly, the optimal solutions obtained using the ML and OPA models exhibit consistent characteristics in terms of phrase transitions in the Pareto fronts and link capacity allocation patterns. These results provide incentive for the use of computationally cheap network-centric models for the optimization of cascade-resilient power network systems, given the advantages of their simplicity and scalability.**

***Index Terms*—Capacity optimization, cascading failures, complex network theory model, evolutionary algorithm (EA), power flow model, power transmission network.**

I. Introduction

OUR modern society has come to depend on large-scale critical infrastructures (CIs) to deliver resources and services to consumers and businesses in an efficient manner. These CIs are complex networks of interconnected functional and structural elements. Large-scale outages on these real-world complex networks, although infrequent, are increasingly disastrous to our society, with estimates of direct costs up to billions of dollars and inestimable indirect costs. Typical examples include blackouts in power transmission networks [1]–[3], financial bankruptcy [4], telecommunication outages [5], and catastrophic failures in socioeconomic systems [6], [7].

Research regarding modeling, prediction, and mitigation of cascading failures in CIs, whereby small initial disturbances may propagate through the whole infrastructure system, has addressed the problem in different ways, including physical models for describing cascading-failure phenomena [8]–[11], control and defense strategies against cascading failures [12]–[14], analytical calculation of capacity parameters [15], and modeling of real-world data [16].

In particular, various problems concerning the robustness and functionality of CI systems (ranging from power outages and Internet congestion to affordability of public transportation) are ultimately determined by the extent to which the CI capability matches supply and demand under realistic conditions [17]. In this respect, the following two issues are closely related to each other and of significant interest: 1) how to improve network resilience to cascading failures; and 2) how to design CI systems with reasonably limited cost. In most circumstances, high resilience and low cost are conflicting objectives and cannot be simultaneously achieved. For instance, a network whose components have high capacity can be highly resilient to failures; however, this type of components is often characterized by high costs.

Continuous effort has been made to model the capacity–load relationship of CI systems and to enhance the CI performance with limited cost. A homogeneous capacity–load relationship model has been widely used in the study of CIs [8], [9], [12]–[14], [18], whereby the capacity of a link (node) is assumed to be proportional to the initial flow of the link (node; note that some of the studies focus on link modeling, whereas others concentrate on modeling node behavior). However, it has been argued by Kim and Motter that this is unrealistic, and empirical data suggest that the relationship between capacity and load of transmission lines is nonlinear [17], [19]: Heavily loaded lines usually have a lower tolerance parameter than lightly loaded lines. Most recently, Wang and Kim [20] proposed a (nonlinear) two-step function for the relationship between the capacity and load of network vertices. Although based on an oversimplified model, it has been shown efficient to prevent cascades by protecting highest-load vertices. Li *et al.* [21] introduced a more complex heuristic capacity model whereby vertices with both higher loads and larger degrees are paid more extra capacities. It is shown that this model can achieve better network robustness than previous models under the same amount of available resources.

Manuscript received February 23, 2014; revised June 3, 2014; accepted July 27, 2014.

Y.-P. Fang and N. Pedroni are with the Chair on Systems Science and the Energetic Challenge, École Centrale Paris and Supélec, 92290 Châtenay-Malabry, France (e-mail: yiping.fang@ecp.fr; nicola.pedroni@ecp.fr).

E. Zio is with the Chair on Systems Science and the Energetic Challenge, École Centrale Paris and Supélec, 92290 Châtenay-Malabry, France, and also with the Department of Energy, Politecnico di Milano, 20133 Milan, Italy (e-mail: enrico.zio@ecp.fr; enrico.zio@supelec.fr; enrico.zio@polimi.it).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSYST.2014.2352152

1932-8184 © 2014 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

In this paper, we tackle the issue from a systematic perspective by searching for the strategy of resource (capacity) allocation in a power transmission network that is most favorable for resisting cascading failures, while keeping the total resource (capacity) limited (i.e., while minimizing the network cost). This serves as the primary objective of this paper. In more detail, the problem is formulated within a large-scale, nonlinear, and combinatorial multiobjective optimization framework and is solved by a fast and elitist genetic algorithm, namely, NSGA-II [22].

The search by the NSGA-II also requires 1) the construction of a model to describe the cascading-failure process in the network of interest and 2) the repeated evaluation of the model for every possible capacity allocation pattern proposed by the algorithm during the search. With respect to the model, two approaches are typically considered in the analysis of power transmission systems: complex network theory models, such as the Motter–Lai (ML) model [8], [9], and artificial power flow models, such as the ORNL–Pserc–Alaska (OPA) model [10], [11], [39]. These approaches provide different tradeoffs between the (relatively low) computational cost associated to the model evaluation (allowing applications to large-scale power grids) and the (high) level of detail in the system description (including physical characteristics and power flows constraints), respectively.

The OPA model seeks to faithfully describe the dispatching dynamics of the power flows during the evolution of the failure propagation following the initial disturbances, by explicitly incorporating the standard dc power flow equations and minimizing generation cost and load shedding [10]. Embracing this more physical description and solving the constrained linear optimization functions associated to the model result in a significant increase in the computational burden, rendering practical application extremely difficult for realistic networks with large numbers of elements [23]. For these reasons, topological models based on complex network theory (e.g., the ML model) have emerged in recent years [8], [9], [13], [14], [18], [24]–[26]. In particular, the ML model is a relatively simple and abstract model relying on the resemblance of complex networks to electrical infrastructure systems (in terms of graph theory). It has the advantage of modeling cascading dynamics with few parameters, so that its application to realistic large-scale networks is feasible and certainly more readily than OPA [16]. However, ML abstracts the power flow laws and constraints of the electrical system. Inevitably, then, it cannot provide direct physical measures of blackout size but rather abstract measures such as efficiency loss. This has posed questions on whether it is adequate in practice, due to its abstract nature, although it has been recognized to offer a new and interesting perspective on the study of cascading failures on power grids [23].

It is worth mentioning that studies tackling the problem of comparison between network-centric approaches and power flow approaches are few in literature. Some studies [23], [25], [27] have provided qualitative comparisons between complex network theory models and power flow models, identifying similarities and differences and evaluating advantages and disadvantages. Most recently, Correa and Yusta have concluded on the appropriateness of graph theory techniques for the assessment of electric network vulnerability by comparison to physical power flow models [28]. By extensive comparative simulation, Cupac *et al.* have shown that a network-centric model (CLM) exhibits ensemble properties that are consistent with the more realistic OPA fast-scale model [29]. Along these lines, our study takes the comparison a step forward by analyzing the optimization results, enabling to find more interesting insights.

In this paper, we embrace both the ML and OPA cascading failure models and embed them within NSGA-II for optimally solving the problem of capacity resource allocation. With respect to that, the second objective of this paper is to study the possibility of using a simplified network-centric model (instead of a detailed power flow model) within an optimization framework, without affecting the quality of the optimal solutions found. For illustration, we apply the method to the 400-kV French power transmission network, under the objectives of maximizing network resilience to cascading failures and minimizing investment costs. Finally, we systematically compare the results obtained by using the two cascading failure models of different complexity.

The remainder of this paper is organized as follows. In Section II, we introduce the ML and OPA cascading failure models in detail. We then formulate the multiobjective optimization problem taking investment costs and failure resilience into account in Section III. In Section IV, we briefly introduce the procedure of the NSGA-II algorithm. Section V illustrates the French 400-kV power transmission network case study and the analysis and comparison of the results. Discussion and conclusion are given in Section VI.

II. Models of Cascading Failure Considered in This Work

Modeling the dynamic evolution of system-wide cascading-failure processes poses a number of challenges due to the diversity of mechanisms, which can trigger the initial failure and influence the subsequent propagation of breakdowns in the power system [27]. Various cascading-failure models have been proposed; these can be divided into two main categories: those based on complex network theory analysis and those using power flow analysis, often including optimal economic power dispatch after each failure in the propagation, e.g., by linear optimal power flow [29].

Complex network theory models, including the ML model adopted in this work and described in Section II-A, abstract the representation of a power grid as a graph and then study the connectivity characteristics, the propagation mechanisms through the graph connections, and their relationships. These types of models have proved to provide a good understanding of the specific grid dynamics of cascading failures [30]. However, in these models, the assumptions only abstract the real loading of the components and the flow distribution through the connections. For this reason, it is necessary to ascertain the meaningfulness of the results for real electrical infrastructures.

Power flow models, on the contrary, are based on realistic power flow equations to describe the flow dispatching dynamics and failure evolution after the initial disturbances in the power

grid. The OPA model, which is the most commonly used of this type of models, is introduced in Section II-B and is based on the dc power flow approximation [31].

A. ML Model

The original ML model has been proposed by Motter and Lai [8], with extensions to differentiate generators and loads [16]. Here, the extended ML model in terms of transmission line failures is utilized. The power transmission network is represented as an undirected graph Q with a set of N vertices representing N_G generators and N_D loads representing distribution substations, interconnected by a set of M edges representing transmission lines. The structure of the network is identified by an $N \times N$ interaction matrix W, whose element w_{ij} is 0 if nodes i and j are not directly connected; otherwise, it is assigned a value of 1, for an unweighted network, or another numerical value, for a weighted network (as in the case of the work in this paper).

The ML model assumes that at each time step, one unit of the relevant quantity (e.g., electrical flow for power grids) is exchanged between every pair of generator and distributor nodes and transmitted along the shortest path connecting them. Then, the flow at one link is computed as the number of shortest paths passing through it. More precisely, the flow F_l^{ML} of link l is quantified by the link betweenness, calculated as the fraction of the generator–distributor shortest paths passing through that link, i.e.,

$$F_l^{\mathrm{ML}} = \frac{1}{N_G N_D} \sum_{i \in V_G, j \in V_D} \frac{n_{ij}(l)}{n_{ij}}, l \in E \tag{1}$$

where $E(\|E\| = M)$ is the set of all the links in the network; $V_G(\|V_G\| = N_G)$, and $V_D(\|V_D\| = N_D)$ are the sets of generators and distributors, respectively; n_{ij} is the number of shortest paths between generator nodes and distributor nodes; and $n_{ij}(l)$ is the number of generator–distributor shortest paths passing though link l.

In the *original* ML model [8], a homogeneous capacity–load relationship is assumed: The capacity of link l is assumed to be proportional to its initial flow $F_l^{\mathrm{ML}}(0)$ with a network tolerance parameter α, i.e.,

$$C_l^{\mathrm{ML}} = (1+\alpha) F_l^{\mathrm{ML}}(0), l \in E. \tag{2}$$

The concept of tolerance parameter α $(\alpha \geq 0)$ can be understood as an operating margin allowing safe operation of the component under potential load increment.[1] The occurrence of a cascading failure is initiated by removal of a link, which, in general, changes the distribution of shortest paths. Then, the flow at a particular link can change, and if it increases and exceeds its capacity, the corresponding link fails. Any failure leads to a new redistribution of loads, and as a result, subsequent failures can occur.

[1]In this paper, the link capacities are variables to be optimized (see Section III); thus, assumption (2) is obviously not introduced in the problem formulation of the present work.

Using this cascading-failure model, the damage of network Q can be characterized by the fraction of network efficiency lost in the cascading failure, i.e.,

$$V_{\mathrm{ML}} = \frac{E(Q) - \overline{E(Q)}}{E(Q)} \tag{3}$$

where $V_{\mathrm{ML}} \in [0,1]$ and $\overline{E(Q)}$ represents the residual network structure after the cascading failure. $E(Q)$ measures the network efficiency based on the node pair shortest-path distance between generators and distributors. For its computation, all pairs of nodes $i \in V_G$, and $j \in V_D$ are weighted by the inverse of their distance, i.e.,

$$E(Q) = \frac{1}{N_G N_D} \sum_{i \in V_G} \sum_{j \in V_D} \frac{1}{d(i,j)} \tag{4}$$

where $d(i,j)$ is the number of edges for an unweighted network or the sum of edge weights for a weighted network in the shortest path from i to j (like in the present case).

The geodesic network damage V_{ML} measures the functionality of a network when subjected to a contingency due to cascading-link disruption with regard to its steady state (base case). As V_{ML} increases, the impact on the network due to cascading failure also increases, as some components become disrupted. V_{ML} has proved to be a well-defined index capable of providing results consistent with those of physical-model indexes [28].

The detailed simulation of the ML cascading-failure model proceeds as follows.

1) A random link is chosen as failed and, thus, is removed from the network.
2) Recur to (1) and Floyd's shortest-path algorithm to calculate the flow of each working link in the network.
3) Test each link for failure: For each link $l \in E$ of the network, if $F_l^{\mathrm{ML}} > C_l^{\mathrm{ML}}$, then link l is regarded as failed and, thus, is removed from the network.
4) If any working link fails, return back to step 2. Otherwise, terminate the simulation and evaluate the network damage by (3).

Complex network theory models, such as the ML that we use within our optimization framework in Section III, have no direct physical relation to the mechanisms of realistic power grids, but they have the key advantage that by utilizing techniques from graph theory, they can be applied to analyze large-scale networks. For this reason, this modeling approach is seeing increasing applications for modeling cascading-failure processes in power grids.

B. OPA Model

The OPA model has been proposed by researchers at the Oak Ridge National Laboratory (ORNL), Power System Engineering Research Center of Wisconsin University (PSerc), and Alaska University (Alaska) [10], [11]. The OPA model is built upon the self-organized criticality theory; contains two different time-scale dynamics, i.e., fast power flow dispatching dynamics and slow power grid growth dynamics; and describes

the complexity and criticality of power systems. It is a novel and powerful tool for analyzing power systems. Our analysis focuses on the fast power flow dynamics, in order to ensure comparability with the ML model shortest-path assumption.

The cascading-failure model is based on the standard dc power flow equation, i.e.,

$$F^{\mathrm{OPA}} = A \cdot P \tag{5}$$

where F^{OPA} is a vector whose M components are the power flows through the lines, i.e., $F_l^{\mathrm{OPA}}(l \in E)$, P is a vector whose $N-1$ components are the power injection of each node; P_i (N is the total number of nodes in the network), with the exception of the reference generator, P_0; and A is a constant matrix that depends on the network structure and impedances (see [10] for details about the computation of A). The reference generator power is not included in vector P to avoid singularity of A as a consequence of the overall power balance.

The generator power dispatch is solved using standard linear programming methods. Using the input power demand, the power flow (5) is solved with the condition of minimizing the following cost function:

$$f = \sum_{i \in V_G} P_i(t) + K \sum_{j \in V_D} P_j(t). \tag{6}$$

This definition gives preference to generation shift while assigning a high cost (set $K = 100$) to load shedding, and it is assumed that all generators operate at the same cost and that all loads are served with equal priority. The minimization is done with the following constraints.

1) Generator power injections are generally positive and limited by installed capacity limits: $0 \le P_i \le P_i^{\max}, i \in V_G$.
2) Loads always have negative power injections: $P_j^{\mathrm{dem}} \le P_j \le 0, j \in V_D$.
3) The flow through links is limited by link capacities: $|F_i^{\mathrm{OPA}}| \le C_i^{\mathrm{OPA}}$.
4) Total power generation and consumption remain balanced: $\sum_{i \in V_G \cup V_D} P_i = 0$.

Notice that in order to simplify the power flow problem, making it linear, a number of assumptions have been made in the standard formulation of dc power flow, one of which is that the transmission line resistance is assumed to be negligible: $\mathrm{R} \ll \mathrm{X}$, i.e., lines are assumed without loss [31]. This means that the loss of power transmission is neglected in the original OPA cascading-failure model [10]. However, the objective of cost minimization (6) is only applied to guide the generator power redispatch after the occurrence of a transmission line failure, for which changes in generation or load shedding are usually considered, as the change in transmission loss among different redispatch strategies should probably not be large and considered by the network operator [10].

After solving the linear optimization by using the simplex method as implemented in the work of Flannery *et al.* [33], we examine which lines are overloaded. A line is considered to be overloaded if the power flow through it is within 1% of the limit capacity C_l^{OPA}. Each overloaded line may outage with probability p_1 (p_1 is set as 1 in the case study to ensure its comparability with ML). If an overloaded line experiences an outage, its power flow limit C_l^{OPA} is divided by a very large number k_1 to ensure that, practically, no power may flow through the line. Moreover, to avoid a matrix singularity from the line outage, the impedance values of failed lines are multiplied by a large number k_2, resulting in changes of network matrix A.

Load shedding is utilized to quantify the damage of the cascading failure. For an individual node, load shedding is defined as the absolute value of the difference between its power injection and demand, i.e.,

$$\mathrm{LS}_j = \left| P_j^{\mathrm{dem}} - P_j \right|, \quad j \in V_D. \tag{7}$$

Subsequently, total load shedding for the system is

$$\mathrm{LS} = \sum_{j \in V_D} \mathrm{LS}_j. \tag{8}$$

Finally, system load shedding is normalized by its total demand and used as a measure of damage to the system resulting from a cascading failure, i.e.,

$$V_{\mathrm{OPA}} = \frac{\mathrm{LS}}{D} = \frac{\sum\limits_{j \in V_D} \mathrm{LS}_j}{\sum\limits_{j \in V_D} P_j^{\mathrm{dem}}}. \tag{9}$$

The fact that simulation results from the OPA model are consistent with historical blackout data for real power systems has justified its effectiveness [11]. However, the applications of OPA have generally been limited to networks with a relatively small number of nodes compared with real power grids [23], due to the computational efforts involved.

III. Formulation of the Multiobjective Optimization Problem

Here, we generally frame the problem of searching the most favorable pattern of link capacities in a realistic power transmission network, so as to optimize its resilience against cascading failures. By associating a cost to (the capacity of) each link of the network, the optimization process also seeks to minimize the total cost. With the aim of comparing network-centric and power flow approaches, both the ML and OPA models introduced in Section II are used to evaluate the vulnerability of the pattern of link capacities proposed during the optimization search.

Specifically, we define the variables to be optimized as the capacities of the links in the network, $C_l, l \in E$ (i.e., C_l^{ML} for the ML model and C_l^{OPA} for the OPA model). Thus, the homogeneous capacity allocation strategy as expressed in (2) is no longer adopted in the optimization. Instead, any nonnegative vector $C \in \boldsymbol{R}_+^M$ could represent a potential solution. It is noted that the searching space $\boldsymbol{R}_+^M$ is intractably large in reality, where a power transmission network usually has hundreds or thousands of links.

We then assume that the cost associated with each link capacity is linearly proportional to the value of the capacity, with coefficient φ (we simply set φ as 1 in our case study).

The total investment cost related to a capacity allocation pattern $C \in \boldsymbol{R}_+^M$ in the power transmission network can then be defined as

$$Cost(C) = \sum_{l \in E} \varphi C_l. \tag{10}$$

The network damage resulting from a cascading failure in the presence of a given capacity pattern can be obtained by running the ML (or the OPA) simulation in correspondence of the capacity pattern and then using (3) [or (9) for OPA]. The cascade is initiated by the failure of a single link in each model. The single link is randomly selected from the set of links E in the network with equal probability. Then, the algorithms for cascading simulation proposed in Section II are applied. The cascade simulations run over several iterations until they either converge or exceed the maximum number of steps (we use a maximum of 20 iterations for both ML and OPA). Finally, the network vulnerability for a given capacity allocation pattern is obtained as the average network damage $\overline{V_{\mathrm{ML}}}$ (or $\overline{V_{\mathrm{OPA}}}$ for OPA), over various random triggers (we use 30 triggers for both ML and OPA).

Through the quantification of the capacity allocation cost and cascading-failure vulnerability, the capacity allocation problem is formulated as a multiobjective optimization, i.e.,

$$\begin{cases} \min\limits_{C \in \boldsymbol{R}_+^M} Cost(C) & (11) \\ \min\limits_{C \in \boldsymbol{R}_+^M} \overline{V}(C). & (12) \end{cases}$$

Objective function (11) is the sum of the link capacity costs; function (12) expresses the cascade vulnerability objective, where $\overline{V}(C)$ is $\overline{V_{\mathrm{ML}}}$ when the ML model is used or $\overline{V_{\mathrm{OPA}}}$ when OPA is used. Observe that under this definition, the most cascade-resilient network might be the network with infinite capacity, which obviously would conflict with the objective of minimizing cost.

IV. MOEAs for Optimal Capacity Allocation

Multiobjective evolutionary algorithms (MOEAs) have proven to be general, robust, and powerful search tools that are desirable for tackling problems involving 1) multiple conflicting objectives and 2) intractably large and highly complex search spaces [34]. In extreme synthesis, the main properties of evolutionary algorithms (EAs) are that the search for the optima is conducted 1) using a (possibly) large population of multiple solution points or candidates; 2) using operations inspired by the evolution of species, such as breeding and genetic mutation; 3) using probabilistic operations; and 4) using information on the objective or search functions and not on its derivatives. The main advantages are 1) fast convergence to near global optima, 2) superior global searching capability in complicated search spaces, and 3) applicability even when gradient information is not readily achievable. MOEAs rely on the following concepts [35].

1) Pareto front: The locus that is formed by a set of solutions that are equally good when compared with other solutions of that set is called Pareto front.
2) Nondomination: Nondominated or Pareto-optimal solutions are those solutions in the set that do not dominate each other, i.e., neither of them is better than the other in all the objective function evaluations. The solutions on each Pareto front are Pareto-optimal with respect to each other.

In this paper, we use a fast and elitist genetic algorithm, namely, NSGA-II [22], to solve multiobjective optimization problems (11) and (12). NSGA-II has been proved to be an efficient algorithm to find Pareto-optimal solutions [36]; for further details about this algorithm and relevant surveys on multiobjective evolutionary optimization, the reader is referred to [22], [34]–[36]. The complete procedure for our capacity allocation optimization problem is detailed as follows:

1) read power transmission network data (line, bus, adjacency matrix, etc.) and fix the MOEA parameters (population size, maximum generation, etc.);
2) randomly initialize a (parent) population of possible solutions (individuals) and evaluate the fitness of each individual with respect to the two objective functions (11) and (12); sort the parent population according to the nondomination criterion [35];
3) select the parents that are more fit for reproduction by using a binary tournament selection [22]; the procedure is such that fitter individuals are selected with higher probability;
4) generate an offspring population by crossover and mutation operators and evaluate the fitness of each individual in the offspring population with respect to the two objective functions (11) and (12);
5) combine the parent and offspring populations to generate a new "trial" aggregate population and perform nondominated sorting on the "trial" population;
6) generate a new parent population by selecting the best solutions in the sorted "trial" population, until a desired population size is reached;
7) if the stop condition is met, then terminate the iteration; otherwise, go to step 3.

The nondominated solutions of the last population constitute the Pareto-optimal front of the optimization problem at hand.

V. Case Study and Results Analysis

A. Case Study and Parameter Setting

In this paper, the 400-kV French power transmission network (FPTN400; see Fig. 1) is taken for exemplification of the proposed approach. The network is built from the data on the 400-kV transmission lines of the RTE website [37]. It has 171 nodes (substations) and 220 edges (transmission lines). We distinguish the generators, which are the source of power, from the other distribution substations, which receive power and transmit it to other substations or distribute it in local distribution grids. By obtaining the power plant list from EDF website [38] and relating them with the ID of the buses in the transmission network, we have 26 generators and 145 distributors. Only the nuclear power plants, hydroelectric plants, and thermal power plants whose installed capacities are larger than 1000 MW are considered. Although simplifications have been made, the network model still has sufficient details to illustrate the validity of the method on a realistic-size electrical infrastructure.

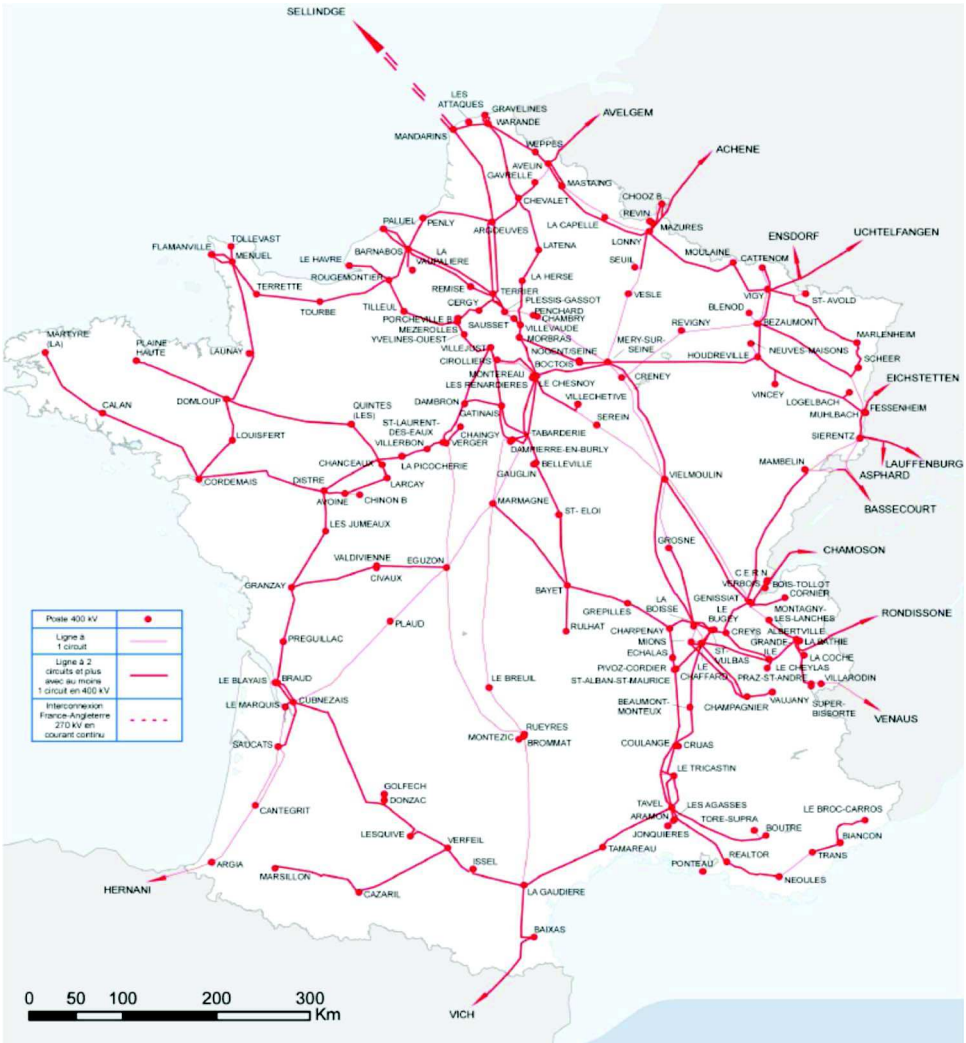


Fig. 1. 400-kV French power transmission network (FPTN400) [37].

TABLE I
PARAMETERS OF THE NSGA-II ALGORITHM

Parameters	Values
Population size	80
Maximum generation	1500
Crossover probability	0.9
Mutation probability	0.1
Crossover operator	20
Mutation operator	20

For optimal allocation of link capacity in the network, the NSGA-II algorithm introduced in Section IV is applied with regard to the objectives of minimizing cascade vulnerability and investment cost, expressed by functions (11) and (12), respectively. Both the ML and OPA models are used to evaluate the cascade vulnerability of the proposed network. The parameter values used in the NSGA-II algorithm are reported in Table I. In this paper, we do not attempt to find the best optimal setting for each of the NSGA-II parameters, and they have been set by trial and error guided by the aim of reaching convergence. For the interested reader, extensive studies exist particularly focusing on the task of tuning GA parameters [40]–[42].

B. Comparison Between the ML and OPA Models

1) Model Adjustments and Settings: The comparison between the optimization results of the ML and OPA models is not straightforward due to the differences of the two models in the way of representing system flow, in the iterative algorithms they rely on, and in the way of measuring the damage produced by the cascading failure. Accordingly, some assumptions and adjustments to the models are necessary to ensure their comparability.

Flow initialization: In the ML model, initial link flow is directly calculated by (1). Regarding the OPA model, the calculation of initial link power flow by (5) necessitates data about power demand and generator capacity. Prior studies set these data by evolving the network using combined fast–slow dynamics until the network reaches a steady state [10], [11]. In order to ensure comparability with ML and taking into account that we limit the scope of our comparison to fast dynamics, we use a simpler initialization strategy that does not require the consideration of network upgrades over time.

Although the ML model does not represent demand and generation capacity quantitatively, it assumes that every distributor is connected to every generator, whereby there is only one

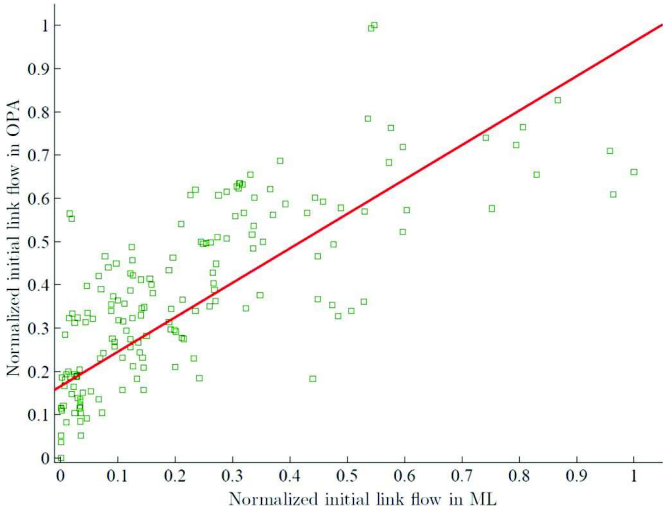


Fig. 2. Scatterplot of the normalized initial link flows in the ML and OPA models, with reference to the 400-kV French power transmission network. The initial link flow in ML is highly correlated to that in OPA ($r_{\mathrm{ML,OPA}} = 0.77$). The best fit line is also shown.

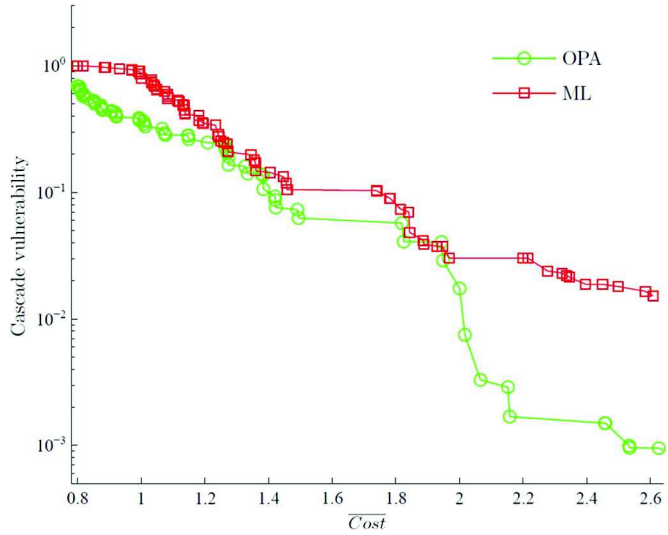


Fig. 3. Phase transitions in the Pareto-optimal fronts showing cascade vulnerability (i.e., average efficiency loss for ML and average load shedding for OPA) with respect to normalized investment cost.

shortest path from any distributor to every generator. This implies that every distributor attempts to extract an equal amount of power from every generator [29]. Thus, to facilitate comparability with the ML model, we use the following assumptions in OPA: 1) All the loads have equal constant power demand; and 2) the total generation capacity is set to be equal to the total demand and equally divided among the generators.

In Fig. 2, we plot the relationship between the initial flow of each link determined using the ML model and that determined using the OPA model in the FPTN400. Each green square in the figure corresponds to one of the links in the network. The x-axis is the value of initial flow of the link in ML, and its y-axis is the value of its initial flow in the OPA approach. It can be seen that the initial link flow in ML is highly correlated with the initial link flow in OPA, computed by means of the proposed initialization method (the correlation coefficient $r_{\mathrm{ML,OPA}}$ is equal to 0.77). That is to say, links with high initial flow in ML tend to have high initial flow in OPA, and vice versa. This shows that our initialization strategy is consistent for ML and OPA.

Cost normalization: Since the ML and OPA models rely on different variables and algorithms (see Section II), the numerical values of each link flow and capacity determined within the two approaches are obviously not identical. Therefore, in order to facilitate the comparison of the optimization results from the two approaches, the cost of each capacity (allocation pattern) proposed by the optimization algorithm is normalized by the corresponding total initial network flow,[2] and indicated as $\overline{Cost}$ in both the ML and OPA models.

Comparison method: As previously mentioned, it is evident that the ML and OPA models provide different results at the local scale [29]; however, we evaluate to what extent the two approaches are consistent at the global system level.

[2]By this definition, the normalized cost has precisely the same physical meaning with the network tolerance parameter α.

In particular, we compare the two approaches by performing the following analyses.

1) We verify whether the Pareto fronts based on the ML and OPA models exhibit similar characteristics in terms of phase transitions of cascade vulnerability with respect to normalized investment cost.
2) We investigate whether the Pareto-optimal solutions showing the same level of investment cost also present similar capacity allocation patterns.
3) We examine whether the link capacity patterns along the two optimal frontiers exhibit similar characteristics for decreasing network vulnerability (i.e., for increasing network resilience).

2) Comparison Results: We first investigate the shape of the Pareto fronts obtained using the ML and OPA models in the capacity allocation optimization: In particular, we analyze the variation of cascade vulnerability as a function of normalized investment cost. Notice that a proper comparison of the Pareto fronts obtained with the ML and OPA models is only possible with the adjustments proposed in the previous section. Fig. 3 shows that ML and OPA Pareto fronts exhibit similar phase transitions (although their absolute values are different, which is not unexpected considering the fact that they apply different modeling parameters and cascade vulnerability measures): Both curves present a sharp decrease in network vulnerability in the same $\overline{Cost}$ region (i.e., $1.0 \leq \overline{Cost} \leq 1.5$), where a small increase in the cost gives a large gain in terms of cascade resilience. Moreover, regions of plateau exist for certain cost values in both models (i.e., for $1.5 \leq \overline{Cost} \leq 1.75$ and $2.0 \leq \overline{Cost} \leq 2.2$ in ML, and for $1.5 \leq \overline{Cost} \leq 1.8$ and $2.15 \leq \overline{Cost} \leq 2.45$ in OPA), in which increasing investment cost does not improve network resilience. Finally, both curves show a relatively stable regime for large $\overline{Cost}$ values (i.e., $\overline{Cost} \geq 2.2$), where network resilience is already high, and its relative improvement is negligible even for a significant increase in the network cost (for example, referring to the ML model, increasing $\overline{Cost}$ from 1.97 to 2.61, i.e., of 32.5%, we

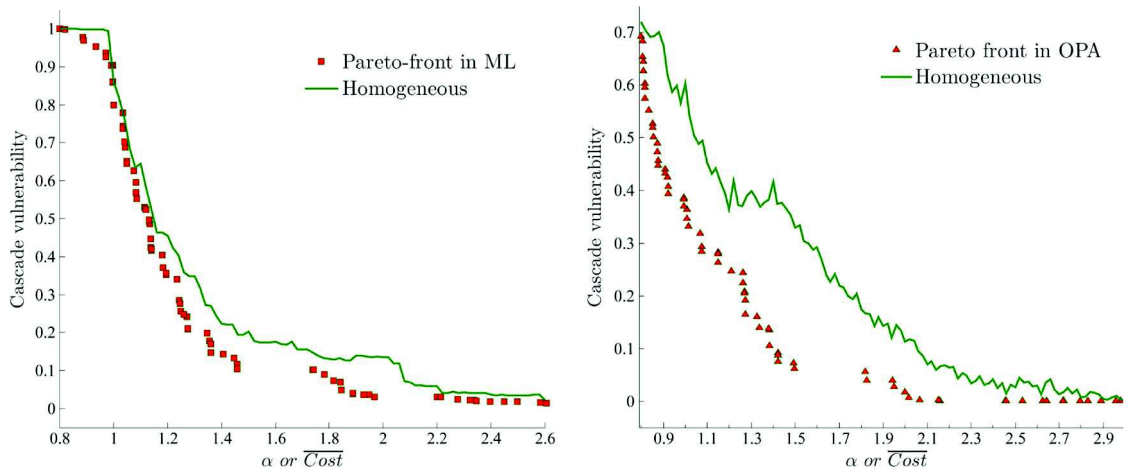


Fig. 4. (Left panel) ML and (right panel) OPA Pareto fronts (squares and triangles) obtained in the multiobjective optimization framework in Section III, together with (solid line) the results obtained by employing a homogeneous capacity allocation strategy.

reduce the network vulnerability of only 1.5%). One could refer to the Pareto fronts of ML (squares in left panel) and OPA (triangles in right panel) in Fig. 4, where this relative stable regime is shown more clearly on a linear y-axis scale.

In Fig. 4, we compare the Pareto fronts obtained by the ML and OPA models within the multiobjective optimization framework in Section III with the results obtained by assuming a classical homogeneous capacity allocation strategy (see Section II-A). The capacity in the homogeneous capacity allocation is assumed to be linearly proportional to the initial flow by means of the network tolerance parameter α, as indicated in (2); thus, the normalized cost of a given capacity allocation pattern is precisely equal to parameter α by construction. It can be seen that in both cases, the multiobjective optimization approach based on ML and OPA produces superior solutions as the corresponding Pareto fronts are closer to the coordinate axes. The linear (homogeneous) capacity–load relationship evidently appears not optimal for obtaining a cost-efficient and cascade-resilient network.

We then compare the link capacity patterns of those solutions along the two Pareto fronts that present approximately the same values of $\overline{Cost}$. In particular, three representative values of normalized cost (i.e., $\overline{Cost} = 1.07,\ 1.27,$ and 1.81) along the Pareto fronts are chosen, and the relationship between the link capacities of the corresponding optimal solutions obtained by the ML and OPA models is visualized using the scatterplots in Fig. 5(a)–(c), respectively. It is evident that the link capacities of the optimal solutions based on the ML and OPA models are highly correlated (with correlation coefficient $r_{\mathrm{ML,OPA}} = 0.73,\ 0.69,$ and 0.76, respectively). That is, links with low capacity in the ML model are likely to have low capacity also in the OPA model, and links with high capacity in ML also have high capacity in OPA.

Finally, it is interesting to analyze how the pattern of link capacities changes when lower network cascade vulnerability (higher network resilience) is demanded, i.e., which type of capacity allocation pattern is the most favorable in resisting cascading failure. We tackle this problem by investigating the "expected" network link capacity pattern as a function of cascade vulnerability, i.e., the configuration of capacity pattern "averaged" over all possible solutions of the Pareto front lying within a given "regime" (i.e., interval) of cascade vulnerability of interest. Parameter β^s (namely, β^s_{ML} for ML and β^s_{OPA} for OPA) is used to represent the "regime" of vulnerability, where s indicates the size of the corresponding interval. It is noted that smaller β^s represents higher network resilience.

Fig. 6 reports the results of averaged link capacity patterns for three different levels of cascade vulnerability, i.e., $0.6 \leq \beta^{0.1} \leq 0.7$, $0.3 \leq \beta^{0.1} \leq 0.4$, and $0 \leq \beta^{0.1} \leq 0.1$ in the case of a homogeneous allocation strategy (circles) and of the optimization-based approach in our study (squares). The left panel (a)–(c) refers to ML, whereas the right panel (d)–(f) relates to OPA. It is found that the optimal link capacity patterns exhibit consistent characteristics between ML and OPA models. For example, in both cases, the optimal link capacity patterns are similar to their corresponding homogeneous allocations only in less-resilient networks, i.e., when $0.6 \leq \beta^{0.1} \leq 0.7$, where the objective of minimizing investment cost is much more biased [see Fig. 6(a) and (d)]. When we increase the importance of minimizing the network vulnerability (e.g., for $0.3 \leq \beta^{0.1} \leq 0.4$ and $0 \leq \beta^{0.1} \leq 0.1$), the optimal link capacities show a nonlinear relationship with respect to their initial flows, as shown in Fig. 6(b), (c), (e), and (f). Specifically, the heavily loaded links tend to decrease their capacities, and the lightly loaded links tend to increase their capacities. That is to say, the unoccupied portion of capacity tends to decrease in links with larger loads, and the unoccupied portion of capacity tends to increase in the less-loaded links. Furthermore, the more importance is given to the minimization of network cascade vulnerability, the more pronounced the nonlinear behavior is, as shown in Fig. 6(c) and (f). Our findings are consistent with the empirical observations and results from the traffic fluctuation model [17], [19].

VI. Discussion and Conclusion

In this paper, we have tackled the problem of searching for the most favorable pattern of link capacity allocation for a CI network with the objective of resisting cascading failures with limited investment costs. The problem has been formulated within a multiobjective optimization framework and has been

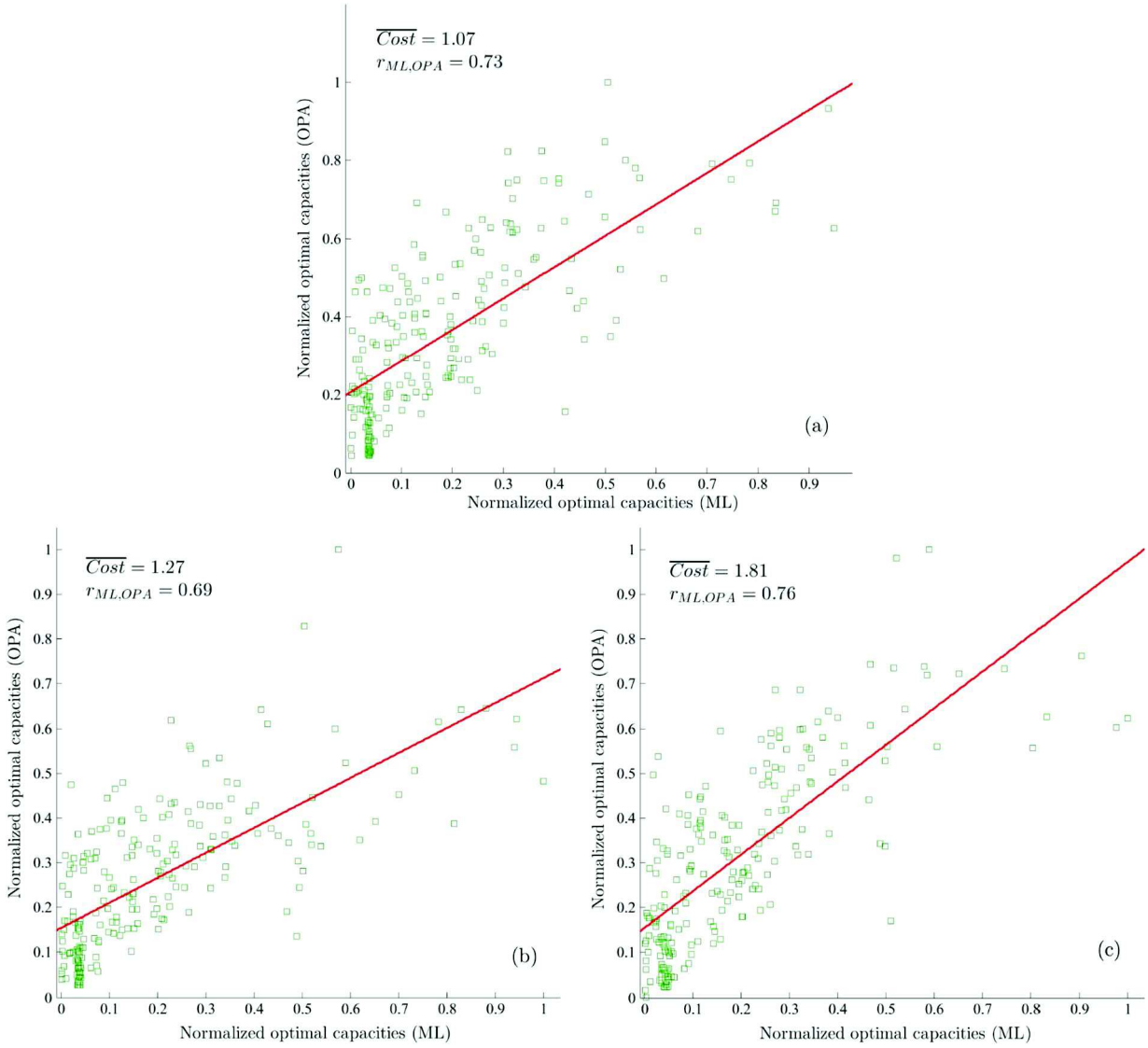


Fig. 5. Scatterplot of the (normalized) link capacities of three representative ML and OPA Pareto solutions showing the same normalized cost. The link capacities of the Pareto solutions with the same level of cost show highly correlated allocation patterns. (a) ML solution (1.07, 0.63) versus OPA solution (1.07, 0.30): $r_{\mathrm{ML,OPA}} = 0.73$. (b) ML solution (1.27, 0.24) versus OPA solution (1.27, 0.21): $r_{\mathrm{ML,OPA}} = 0.69$. (c) ML solution (1.81, 0.074) versus OPA solution (1.81, 0.057): $r_{\mathrm{ML,OPA}} = 0.76$. The line of best fit is also plotted, for visual guidance.

solved by an evolutionary algorithm, namely, the NSGA-II. The optimization has been carried out using two different approaches to cascade failure modeling: a computationally cheap complex network model, namely, the ML model, and a more detailed power flow model, namely, the OPA model. The approaches have been compared in a case study involving the 400-kV French power transmission network (FPTN400). Although simplifications have been applied, the network model still has sufficient detail to illustrate the validity of the method on a realistic electrical infrastructure.

The objective of this paper is twofold: 1) to tackle the issue of capacity–load relationship from a systematic perspective, by introducing the optimization of link capacity allocation; and 2) to study the possibility of using a simplified network-centric model (instead of a detailed power flow model) within the optimization framework, without affecting the quality of the optimal solutions found, by embedding both the ML and OPA models into the optimization and comparing their results.

Primarily, our multiobjective optimization results show that both the ML and OPA models produce improved Pareto solutions with respect to those obtained by assuming a classical homogeneous allocation strategy. In addition, the optimal link capacity allocations show a nonlinear capacity–load relation: The unoccupied portion of capacity tends to decrease in links with larger loads, whereas the unoccupied portion of capacity tends to increase in the lightly loaded links. This is in sharp contrast to the linear capacity–load relation hypothesized in previous works of literature [8], [9], [12]–[14], [18]. This nonlinear behavior is probably a consequence of the following observation: Since larger loads in heavily loaded components tend to result from a large number of flow events, the relative size of the fluctuations in these components tends to be small when other lightly loaded components fail during a cascading failure; considering that the unoccupied capacity is the operating margin that allows safe operation for the component under potential load increment (mainly determined by the perturbations caused

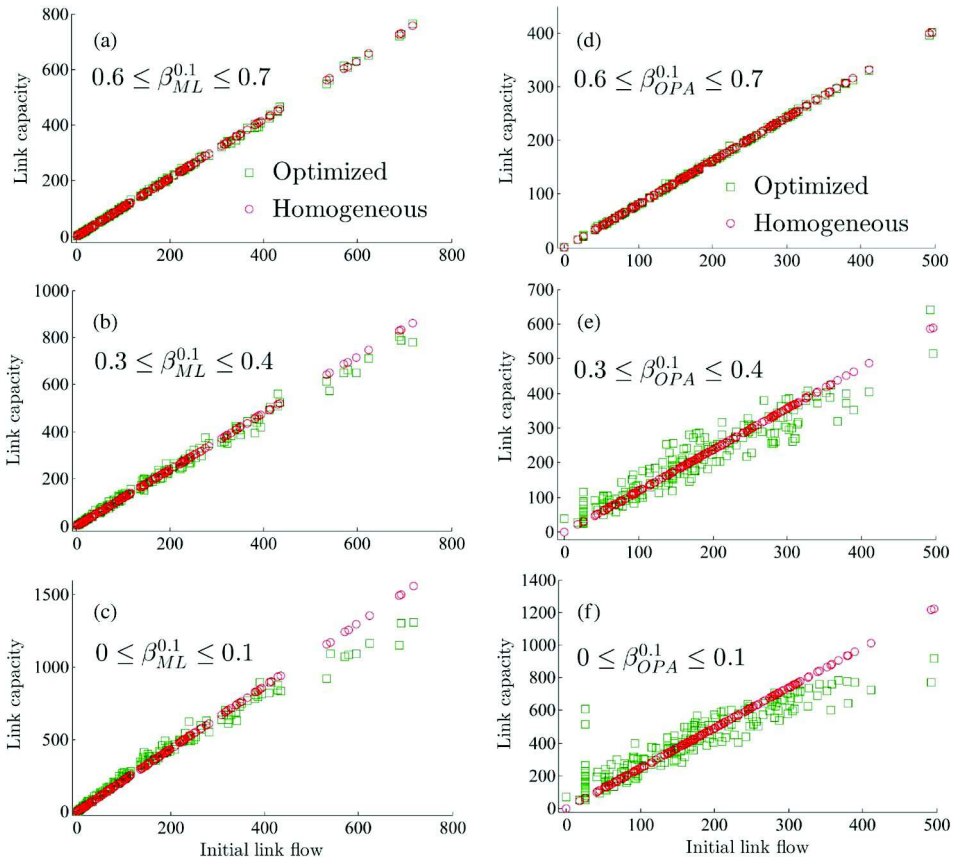


Fig. 6. "Averaged" optimal link capacity patterns for three different levels of cascade vulnerability ($0.6 \leq \beta^{0.1} \leq 0.7$, $0.3 \leq \beta^{0.1} \leq 0.4$, and $0 \leq \beta^{0.1} \leq 0.1$) in ML left panel (a)–(c)] and OPA [right panel (d)–(f)]. The scatterplot shows the relationship between the link capacities and the initial link flows in a homogeneous allocation strategy, where the capacity of a link is assumed to be proportional to its initial flow (circles) and after in the optimization-based approach in Section III (squares).

by the failure of other components of the network), this explains why in the optimal solutions the unoccupied capacity tends to be smaller for links with larger loads.

Additionally, the analysis of the behavior of the link capacity patterns of the Pareto-optimal solutions as a function of the vulnerability level has shown that the results provided by ML and OPA are consistent: The more importance is given to the objective of network cascade vulnerability, the more pronounced is the nonlinear capacity–load relation for both models. Moreover, the Pareto fronts produced by ML and OPA exhibit similar phase transitions. Both curves exhibit a sharp decrease in network vulnerability when $1.0 \leq \overline{Cost} \leq 1.5$, a plateau for certain cost values (i.e., for $1.5 \leq \overline{Cost} \leq 1.75$ and $2.0 \leq \overline{Cost} \leq 2.2$ in ML, and for $1.5 \leq \overline{Cost} \leq 1.8$ and $2.15 \leq \overline{Cost} \leq 2.45$ in OPA) and a relatively stable regime when $\overline{Cost} \geq 2.2$. Furthermore, the link capacities of the Pareto-optimal solutions produced by the ML and OPA models show a highly correlated allocation pattern, which means that links with low capacity in ML tend to have low capacity in OPA, and links with high capacity in ML also tend to have high capacity in OPA. This consistency is not insignificant since it demonstrates that one resilience-improved pattern of capacity allocation optimized by the ML model is also of higher resilience if measured by the more realistic OPA model.

The results from this comparative study provide an important contribution regarding the usefulness of a topological model (ML) in the optimization of a cascade-resilient electrical network. Although ML is a relatively simple and abstract model (that does not account for the power flow laws and constraints of the electrical system), it is able to provide results that are consistent with a detailed and more realistic power flow model (OPA), when applied to the problem of network optimization against cascading failure. Most importantly, with respect to OPA, it has the advantages of simplicity and scalability: The average time needed to carry out a single cascade failure simulation is 3.9 and 20.8 s for ML and OPA, respectively, on a double 2.4-GHz Intel CPU and 4-GB RAM computer. This provides impetus for the use of network-centric models to the study of cascading failure in large power network systems.

Future works may consider comparing our optimization results with real data, i.e., the empirical capacity–load characteristics, for extracting further insights about how realistic infrastructure systems evolve. Moreover, it is noted that the optimization based on the OPA model leads to solutions of reduced vulnerability compared with its ML counterpart (see Fig. 4), and the modeling reason behind it is worthy of further study. Furthermore, Newton–Raphson-based power flow approaches [43] could be applied for the comparison with the ML model, since they give a more detailed depiction of the cascading-failure process, although the price to be paid is that they are computationally expensive. Finally, it would be interesting to apply our method to other networks, e.g. the standard IEEE Power Systems Test Cases and the like.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

REFERENCES

[1] "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," Apr. 2004, Tech. Rep.

[2] "Final report system disturbance on 4 nov. 2006," 2007, Tech. Rep.

[3] J. J. Romero, "Blackouts illuminate India's power problems," *IEEE Spectr.*, vol. 49, no. 10, pp. 11–12, Oct. 2012.

[4] S. Battiston *et al.*, "Credit chains and bankruptcy propagation in production networks," *J. Econom. Dyn. Control*, vol. 31, no. 6, pp. 2061–2084, Jun. 2007.

[5] M. E. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Phys. Rev. E*, vol. 66, no. 3, pp. 035101-1–035101-4, Sep. 2002.

[6] K. Zhao, A. Kumar, T. P. Harrison, and J. Yen, "Analyzing the resilience of complex supply network topologies against random and targeted disruptions," *IEEE Syst. J.*, vol. 5, no. 1, pp. 28–39, Mar. 2011.

[7] D. Kempe, J. Kleinberg, and E. Tardos, "Maximizing the spread of influence through a social network," in *Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining*, 2003, pp. 137–146.

[8] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, no. 6, pp. 065102-1–065102-4, Dec. 2002.

[9] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, pp. 045104-1–045104-4, Apr. 2004.

[10] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An initial model for complex dynamics in electric power system blackouts," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2001, pp. 710–718.

[11] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 9, pp. 1733–1740, Sep. 2004.

[12] A. E. Motter, "Cascade control and defense in complex networks," *Phys. Rev. Lett.*, vol. 93, no. 9, pp. 098701-1–098701-4, Aug. 2004.

[13] Y. Li, G. Sansavini, and E. Zio, "Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks," *Reliab. Eng. Syst. Safety*, vol. 111, pp. 195–205, Mar. 2013.

[14] Y.-P. Fang, N. Pedroni, and E. Zio, "Optimal production facility allocation for failure resilient critical infrastructures," in *Proc. 22nd ESREL Annu. Conf.*, Sep. 2013, pp. 2605–2612.

[15] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Phys. Rev. E*, vol. 70, no. 3, pp. 035101-1–035101-4, Sep. 2004.

[16] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north American power grid," *Eur. Phys. J. B, Condensed Matter Complex Syst.*, vol. 46, no. 1, pp. 101–107, Jul. 2005.

[17] D.-H. Kim and A. E. Motter, "Fluctuation-driven capacity distribution in complex networks," *New J. Phys.*, vol. 10, no. 5, pp. 053022-1–053022-19, 2008.

[18] E. Zio and G. Sansavini, "Modeling interdependent network systems for identifying cascade-safe operating margins," *IEEE Trans. Reliab.*, vol. 60, no. 1, pp. 94–101, Mar. 2011.

[19] D.-H. Kim and A. E. Motter, "Resource allocation pattern in infrastructure networks," *J. Phys. A, Math. Theoret.*, vol. 41, no. 22, pp. 224 019-1–224 019-8, 2008.

[20] B. Wang and B. J. Kim, "A high-robustness and low-cost model for cascading failures," *Europhys. Lett.*, vol. 78, no. 4, pp. 48001-1–48001-5, 2007.

[21] P. Li, B.-H. Wang, H. Sun, P. Gao, and T. Zhou, "A limited resource model of fault-tolerant capability against cascading failure of complex network," *Eur. Phys. J. B*, vol. 62, no. 1, pp. 101–104, Mar. 2008.

[22] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *Evolutionary Computation, IEEE Trans.*, vol. 6, no. 2, pp. 182–197, Apr. 2002.

[23] K. Sun and Z.-X. Han, "Analysis and comparison on several kinds of models of cascading failure in power system," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Exhib., Asia Pac.*, 2005, pp. 1–7.

[24] B. Y. Calida, A. V. Gheorghe, R. Unal, and D. Vamanu, "Dealing with next generation infrastructures academic programmes complexity induced resiliency assessment," *Int. J. Crit. Infrastruct.*, vol. 6, no. 4, pp. 347–362, 2010.

[25] S. LaRocca, J. Johansson, H. Hassel, and S. Guikema, "Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems," arXiv preprint, arXiv: 1306.6696, 2013.

[26] P. Zhang *et al.*, "The robustness of interdependent transportation networks under targeted attack," *Europhys. Lett.*, vol. 103, no. 6, p. 68005, 2013.

[27] R. Baldick *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures," in *Proc. IEEE Power Energy Soc. Gen. Meet.-Convers. Del. Elect. Energy 21st Century*, 2008, pp. 1–8.

[28] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Elect. Power Syst. Res.*, vol. 101, pp. 71–79, Aug. 2013.

[29] V. Cupac, J. T. Lizier, and M. Prokopenko, "Comparing dynamics of cascading failures between network-centric and power flow models," *Int. J. Elect. Power Energy Syst.*, vol. 49, pp. 369–379, Jul. 2013.

[30] A. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Anal.*, vol. 26, no. 4, pp. 955–969, Aug. 2006.

[31] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans, "Usefulness of dc power flow for active power flow analysis," in *Proc. IEEE Power Eng. Soc. Gen. Meet.*, 2005, pp. 454–459.

[32] R. W. Floyd, "Algorithm 97: Shortest path," *Commun. ACM*, vol. 5, no. 6, p. 345, Jun. 1962.

[33] B. P. Flannery, W. H. Press, S. A. Teukolsky, and W. Vetterling, *Numerical Recipes in C*. New York, NY, USA: Press Syndicate Univ. Cambridge, 1992.

[34] E. Zitzler, M. Laumanns, and S. BlEuler, "A tutorial on evolutionary multiobjective optimization," in *Metaheuristics for Multiobjective Optimisation*. Berlin, Germany: Springer-Verlag, 2004, pp. 3–37.

[35] K. Deb, *Multi-Objective Optimization Using Evolutionary Algorithms*, vol. 2012. Chichester, U.K.: Wiley, 2001.

[36] A. Konak, D. W. Coit, and A. E. Smith, "Multi-objective optimization using genetic algorithms: A tutorial," *Reliab. Eng. Syst. Safety*, vol. 91, no. 9, pp. 992–1007, Sep. 2006.

[37] *Le Réseau de Transport d'Electricité 400 kv*, RTE, Paris, France, Nov. 2013. [Online]. Available: www.rte-france.com/uploads/media/CS4_2013.pdf

[38] EDF, "En direct de nos centrales," 2013. [Online]. Available: http://france.edf.com/france-45634.html/Avril

[39] S. Mei, F. He, X. Zhang, S. Wu, and G. Wang, "An improved OPA model and blackout risk assessment," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 814–823, May 2009.

[40] A. E. Eiben, Z. Michalewicz, M. Schoenauer, and J. E. Smith, "Parameter control in evolutionary algorithms," in *In Parameter Setting In Evolutionary Algorithms*. Berlin, Germany: Springer-Verlag, 2007, pp. 19–46.

[41] K. De Jong, "Parameter setting in EAs: A 30 year perspective," in *In Parameter Setting in Evolutionary Algorithms*. Berlin, Germany: Springer-Verlag, 2007, pp. 1–18.

[42] M. E. Samples, M. J. Byom, and J. M. Daida, "Parameter sweeps for exploring parameter spaces of genetic and evolutionary algorithms," in *In Parameter Setting in Evolutionary Algorithms*. Berlin, Germany: Springer-Verlag, 2007, pp. 161–184.

[43] H. Wang and J. S. Thorp, "Optimal locations for protection system enhancement: A simulation of cascading outages," *IEEE Trans. Power Del.*, vol. 16, no. 4, pp. 528–533, Oct. 2001.

Yi-Ping Fang received the B.S. degree in electronic and information engineering and the M.S. degree in information and communication engineering from Beihang University, Beijing, China, in 2009 and 2012, respectively. He is currently working toward the Ph.D. degree in industrial engineering within the Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy of the Électricité de France at the École Centrale Paris, Châtenay-Malabry, France.

His research interest is in the vulnerability and risk analysis of complex networked engineering systems.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Nicola Pedroni received the B.S. degree in energetic engineering, the M.Sc. degree in nuclear engineering, and the Ph.D. degree in radiation science and technology from the Politecnico di Milano, Milan, Italy, in 2003, 2005, and 2010, respectively. During his Ph.D. study, he visited the Department of Nuclear Science and Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA (2008–2009).

He is currently an Assistant Professor with the Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy of the Électricité de France with a joint appointment at the École Centrale Paris, Châtenay-Malabry, France, and the École Supérieure D'Électricité (SUPELEC), Gif-Sur-Yvette, France. He was an Assistant Professor in nuclear power plants with the Politecnico di Milano, Milan, Italy. He is a coauthor of about 20 papers on international journals and four chapters in international books. His research focuses on the study of computational methods for the risk analysis of safety critical systems, e.g., Monte Carlo methods for reliability estimation; theories for uncertainty representation; soft computing techniques for regression modeling; and algorithms for solving optimization problems.

Enrico Zio (M'06–SM'09) received the B.S. degree in nuclear engineering from the Politecnico di Milano, Milan, Italy, in 1991; the M.Sc. degree in mechanical engineering from the University of California, Los Angeles, CA, USA, in 1995; the Ph.D. degree in nuclear engineering from the Politecnico di Milano in 1995; and the Ph.D. degree in nuclear engineering from Massachusetts Institute of Technology, Cambridge, MA, USA, in 1998.

He is currently the Director of the Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy of the Électricité de France at the École Centrale Paris, Châtenay-Malabry, France, and the École Supérieure D'Électricité (SUPELEC), Gif-Sur-Yvette, France. He is also a Full Professor, a President and Rector's delegate of the Alumni Association, and the past Director of the Graduate School, Politecnico di Milano, Milan, Italy. He is an Adjunct Professor with the University of Stavanger, Stavanger, Norway. He is the author or coauthor of five international books and more than 170 papers on international journals. His research focuses on the characterization and modeling of the failure/repair/maintenance behavior of components, complex systems, and critical infrastructures for the study of their reliability, availability, maintainability, prognostics, safety, vulnerability, and security, mostly using a computational approach based on advanced Monte Carlo simulation methods, soft computing techniques, and optimization heuristics.

Prof. Zio is the Chairman of the European Safety and Reliability Association, a member of the Scientific Committee of the Accidental Risks Department of the French National Institute for Industrial Environment and Risks, and a member of the Korean Nuclear Society and China Prognostics and Health Management Society. He was the Chairman of the Italian Chapter of the IEEE Reliability Society. He has functioned as the Scientific Chairman of three international conferences and as an Associate General Chairman of two others. He is serving as an Associate Editor of the IEEE TRANSACTIONS ON RELIABILITY and as an Editorial Board Member in various international scientific journals, among which *Reliability Engineering and System Safety*; the *Journal of Risk and Reliability*; the *International Journal of Performability Engineering, Environment, Systems and Engineering*; and the *International Journal of Computational Intelligence Systems*.

Nuclear Engineering and Design 241 (2011) 310–327

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

How to effectively compute the reliability of a thermal–hydraulic nuclear passive system

E. Zio [a,b,*], N. Pedroni [b,1]

[a] Ecole Centrale Paris-Supelec, Grande Vois de Vigne - 92295 Chatenay-Malabry Cedex, France
[b] Energy Department, Politecnico di Milano, Via Ponzio, 34/3 – 20133 Milan, Italy

ARTICLE INFO

Article history:
Received 15 June 2010
Received in revised form
14 September 2010
Accepted 19 October 2010

ABSTRACT

The computation of the reliability of a thermal–hydraulic (T–H) passive system of a nuclear power plant can be obtained by (i) Monte Carlo (MC) sampling the uncertainties of the system model and parameters, (ii) computing, for each sample, the system response by a mechanistic T–H code and (iii) comparing the system response with pre-established safety thresholds, which define the success or failure of the safety function. The computational effort involved can be prohibitive because of the large number of (typically long) T–H code simulations that must be performed (one for each sample) for the statistical estimation of the probability of success or failure. The objective of this work is to provide operative guidelines to effectively handle the computation of the reliability of a nuclear passive system. Two directions of computation efficiency are considered: from one side, efficient Monte Carlo Simulation (MCS) techniques are indicated as a means to performing robust estimations with a limited number of samples: in particular, the Subset Simulation (SS) and Line Sampling (LS) methods are identified as most valuable; from the other side, fast-running, surrogate regression models (also called response surfaces or meta-models) are indicated as a valid replacement of the long-running T–H model codes: in particular, the use of bootstrapped Artificial Neural Networks (ANNs) is shown to have interesting potentials, including for uncertainty propagation. The recommendations drawn are supported by the results obtained in an illustrative application of literature.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Nuclear safety has expanded its considerations to severe accidents and increased its requirements for guaranteeing effective safety functions. This explains the interest in passive systems (Ahn et al., 2010; Kim et al., 2010), which all innovative reactor concepts make use of, to a large extent in combination with active systems (Mackay et al., 2008; Mathews et al., 2008, 2009).

According to the International Atomic Energy Agency (IAEA) definitions, a passive component does not need external input (especially energy) to operate (IAEA, 1991). Then, the term "passive" identifies a system which is composed entirely of passive components and structures, or a system, which uses active components in a very limited way to initiate subsequent passive operation. The currently accepted categorization of passive systems, developed by the IAEA, is summarized in Table 1 (IAEA, 1991).

Passive systems are expected to contribute significantly to nuclear safety by combining peculiar characteristics of simplicity, reduction of human interaction and reduction or avoidance of external electrical power and signals input (Nayak et al., 2008a,b, 2009). On the other hand, the assessment of the effectiveness of passive systems must include considerations on their reliability; these have to be drawn in the face of lack of data on some underlying phenomena, scarce or null operating experience of these systems over the wide range of conditions encountered during operation and less guaranteed performance as compared to active safety systems (Pagani et al., 2005; Burgazzi, 2007a).

Indeed, although passive systems are credited a higher reliability with respect to active ones, because of the reduced unavailability due to hardware failure and human error, the uncertainties involved in the actual *operation* of passive systems in the field and their *modeling* are usually larger than in active systems. Two different sources of uncertainties are usually considered in passive system analysis: randomness due to intrinsic variability in the behavior of the system (aleatory uncertainty) and imprecision due to lack of data on some underlying phenomena (e.g., natural circulation) and to scarce or null operating experience over the wide range of conditions encountered during operation (Apostolakis, 1990; Helton and Oberkampf, 2004).

* Corresponding author at: Energy Department, Politecnico di Milano, Via Ponzio, 34/3 – 20133 Milan, Italy. Tel.: +39 02 2399 6340; fax: +39 02 2399 6309.
E-mail addresses: enrico.zio@ecp.fr, enrico.zio@supelec.fr, enrico.zio@polimi.it (E. Zio).
[1] Tel.: +39 02 2399 6340; fax: +39 02 2399 6309.

0029-5493/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.nucengdes.2010.10.029

Table 1
Categorization of passive systems (IAEA, 1991).

Category	Description
A	Physical barriers and static structures (e.g., concrete buildings)
B	Moving working fluid (e.g., cooling by free convection)
C	Moving mechanical parts (e.g., check valves)
D	External signals and stored energy (e.g., scram systems)

As a consequence of these uncertainties, in practice there is a nonzero probability that the physical phenomena involved in the passive system operation lead to failure of performing the intended safety function even if (i) safety margins are present and (ii) no hardware failures occur. In fact, deviations in the natural forces and in the conditions of the underlying physical principles from the expected ones can impair the function of the system itself: this event is referred to in the literature as *functional failure* (Burgazzi, 2003). The quantification of the probability of this occurrence is an issue of concern both for the "nominal" passive systems (e.g., the ESBWR operating in nominal conditions) (Juhn et al., 2000; Rohde et al., 2008) and the "emergency" passive systems (e.g., accumulators, isolation condensers, etc.) (Chung et al., 2008). In the following, the discussion will focus on the latter type of systems.

The occurrence of functional failures is especially critical in Type B passive systems, i.e., those involving moving working fluids and referred to as thermal–hydraulic (T–H) passive systems (Table 1). The reason lies behind the small driving forces engaging passive operation and the complex and delicate T–H phenomena determining the system performance. For performing their accident prevention and/or mitigation functions, these passive systems rely exclusively on natural forces, e.g., gravity or natural convection, not generated by external power sources. Because the magnitude of the natural forces which drive operation is relatively small, counter-forces (e.g., friction) cannot be ignored because of comparable magnitude. This leads to uncertainty in the actual T–H system performance which must be evaluated by a specific, systematic and rigorous methodology.[2]

In recent years, several methodologies have been proposed in the literature to quantify the probability that nuclear passive systems fail to perform their functions (Burgazzi, 2007b; Zio and Pedroni, 2009a). A number of methods adopt the system reliability analysis framework. In Aybar and Aldemir (1999), a dynamic methodology based on the cell-to-cell mapping technique has been used for the reliability analysis of an inherently safe Boiling Water Reactor (BWR). In Burgazzi (2007a), the failure probability is evaluated as the probability of occurrence of different independent failure modes, a priori identified as leading to the violation of the boundary conditions and/or physical mechanisms needed for successful passive system operation. In Burgazzi (2002), modeling of the passive system is simplified in terms of the modeling of the unreliabilities of the hardware components of the system: this is done by identifying the hardware components failures that degrade the natural mechanisms which the passive system relies upon and associating the corresponding components unreliabilities. This concept is also at the basis of the Assessment of Passive System ReliAbility (APSRA) approach which has been applied to the reliability analysis of the natural circulation-based Main Heat Transport (MHT) system of an Indian Heavy Water Reactor (HWR) (Nayak et al., 2008a,b, 2009).

An alternative approach is founded on the introduction of the concept of *functional failures*, within the reliability physics framework of load-capacity exceedance (Burgazzi, 2003, 2007a,c, 2008, 2009): a passive system fails to perform its function due to deviations from its expected behavior which lead the load imposed on the system to overcome its capacity. In Woo and Lee (2009a,b, 2010) and Han and Yang (2010), this concept is at the basis of the estimation of the functional failure probability of passive decay heat removal systems of Very High Temperature Reactors (VHTRs). It also provides the basis for the methodologies known as Reliability Evaluation of PAssive Safety (REPAS) systems (D'Auria et al., 2002; Jafari et al., 2003; Zio et al., 2003) and Reliability Methods for Passive Safety (RMPS) functions (Marquès et al., 2005), developed and employed for the analysis of passive Residual Heat Removal Systems (RHRSs) of Light Water Reactors (LWRs). It has also been used to evaluate the failure probabilities of decay heat removal systems in Gas-cooled Fast Reactors (GFRs) (Pagani et al., 2005; Bassi and Marquès, 2008; Mackay et al., 2008; Patalano et al., 2008; Zio and Pedroni, 2009b,c, 2010; Pedroni et al., 2010; Zio et al., 2010), sodium-cooled Fast Breeder Reactors (FBRs) (Mathews et al., 2008, 2009; Arul et al., 2009, 2010) and the lead-cooled, fast spectrum Flexible Conversion Ratio Reactor (FCRR) (Fong et al., 2009). In all these analyses, the passive system is modeled by a detailed, mechanistic T–H system code and the probability of not performing the required function is estimated based on a Monte Carlo (MC) sample of code runs which propagate the *epistemic* (state-of-knowledge) uncertainties in the model describing the system and the numerical values of its parameters. Because of the existence of these uncertainties, it is possible that even if no hardware failure occurs, the system may not be able to accomplish its mission.[3]

The functional failure-based approach provides in principle the most realistic assessment of the T–H passive system, thanks to the flexibility of Monte Carlo Simulation (MCS) which does not suffer from any T–H model complexity and, therefore, does not force to resort to simplifying approximations: for this reason, the functional failure-based approach will be taken here as reference. On the other hand, such approach requires considerable and often prohibitive computational efforts. The reason is twofold. First, a large number of Monte Carlo-sampled T–H model evaluations must generally be carried out for an accurate uncertainty propagation and functional failure probability estimation. Since the number of simulations required to obtain a given accuracy depends on the magnitude of the failure probability to be estimated, with the computational burden increasing with decreasing functional failure probability (Schueller, 2007, 2009), this poses a significant challenge for the typically quite small (e.g., less than 10^{-4}) probabilities of functional failure of T–H passive safety systems. Second, long calculations (several hours) are typically necessary for each run of the detailed, mechanistic T–H code (one code run is required for each sample of values drawn from the uncertainty distributions) (Fong et al., 2009; Pourgol-Mohamad et al., 2010).[4]

Finally, notice that for the same reasons a high computational burden is associated also to the sensitivity analysis process, i.e., the identification of the model parameters that contribute the most

[2] Notice that in the following, the discussion will focus on Type B passive systems, i.e., those involving moving working fluids and referred to as T–H passive systems; thus, the locution "passive system" will implicitly mean "T–H passive system" in the remainder of the paper.

[3] It is worth mentioning also the work performed by Lee and co-workers who took up the problem of passive system functional reliability assessment focusing on the idea of *identifying* the limit state function of the system (essentially referring to the generic structural reliability paradigm of load-capacity exceedance described above) as a *prelude* to the quantification of the functional reliability itself (Aumeier, 1994; Aumeier and Lee, 1993, 1994; Aumeier et al., 1995, 2006; Lee et al., 1993, 1994, 1995). However, since the focus of the present paper is on the *efficient computation* of the passive system functional reliability (*given* the limit state function of the system and proper input probability distributions representing the uncertainties in the system model and parameters), no further details are given here for brevity; the interested reader is thus referred to the cited references.

[4] For example, the computer code RELAP5-3D, which is used to describe the thermal–hydraulic behavior of nuclear systems, may take up to 20 h per run in some applications.

to the uncertainty in the performance of the passive system and consequently to its functional failure (Saltelli et al., 2008; Marrel et al., 2009).

Thus, efficient simulation techniques must be sought to perform robust functional failure probability estimation, uncertainty propagation and sensitivity analysis while reducing as much as possible the number of T–H code simulations and the associated computational time.

The objective of the present paper is to show how the computational issues associated to the functional reliability assessment of nuclear passive systems can be effectively handled. Two conceptual directions of computation efficiency are considered: efficient Monte Carlo Simulation techniques for performing robust estimations based on a limited number of samples drawn (i.e., T–H code simulations); fast-running, surrogate regression models (also called response surfaces or meta-models) in replacement of the long-running T–H model codes.

Within this conceptual framework, *different* computational methods are recommended for efficiently tackling the *different* phases of the functional reliability assessment of nuclear passive systems: in particular, an optimized Line Sampling (LS) method (Zio and Pedroni, 2010) is recommended for functional failure probability estimation, whereas the use of Subset Simulation (SS) (Au and Beck, 2001, 2003b) and bootstrapped Artificial Neural Networks (ANNs) (Efron and Thibshirani, 1993; Zio, 2006) is suggested for uncertainty propagation and sensitivity analysis.

These recommendations are arrived at on the basis of (i) a critical review of the methods available in the literature on the subject and (ii) the experience of the authors in nuclear passive systems functional reliability assessments (Zio and Pedroni, 2009a,b,c, 2010; Pedroni et al., 2010; Zio et al., 2010).

The remainder of the paper is organized as follows. In Section 2, the main sources and types of uncertainties involved in the operation and modeling of nuclear passive systems are recalled. In Section 3, the reliability analysis of nuclear passive systems is framed in terms of the concept of functional failure. In Section 4, the two conceptual directions considered for reducing the computational burden associated to the reliability assessment of nuclear passive systems (i.e., advanced MCS and empirical regression modeling) are presented and critically analyzed on the basis of a literature review. In Section 5, techniques are recommended to effectively tackle the computational burden associated to the different phases of the reliability assessment; results of the application of the proposed techniques to a case study of literature are also shown. Finally, guidelines and recommendations are summarized in the concluding section.

2. Sources and types of uncertainties in the operation and modeling of nuclear passive systems

Uncertainties in the operation and modeling of nuclear passive systems must be accounted for in their reliability evaluations within a Probabilistic Risk Assessment (PRA) framework (Burgazzi, 2004, 2007a,b,c; Pagani et al., 2005).

To effectively represent and model these uncertainties, it is useful to distinguish two kinds: "aleatory" and "epistemic" (Apostolakis, 1990; Helton and Oberkampf, 2004; USNRC, 2009). The former refers to phenomena occurring in a random way: probabilistic modeling offers a sound and efficient way to describe such occurrences. The latter captures the analyst's confidence in the PRA model by quantifying the degree of belief of the analysts on how well it represents the actual system; it is also referred to as *state-of-knowledge* or *subjective* uncertainty and can be reduced by gathering information and data to improve the knowledge on the system behavior.

Table 2
Categories of uncertainties associated to nuclear passive systems reliability assessment.

Categories of uncertainties		
ALEATORY	Occurrence of accident scenarios Failure time of mechanical components Variation of geometrical dimensions Variation of material properties	
EPISTEMIC	T–H analysis	Model (correlations) Parameters
	System failure analysis	Failure criteria Failure modes (critical parameters)

As might be expected, the uncertainties affecting the operation of nuclear passive systems (Table 2) are both of aleatory kind, because of the randomness in the occurrence of some phenomena, and of epistemic nature, because of the limited knowledge on some phenomena and processes and the paucity of the relative operational and experimental data available (Burgazzi, 2007a).

Aleatory uncertainties concern, for instance, the occurrence of an accident scenario, the time to failure of a component or the variation of the actual geometrical dimensions (due to differences between the as-built system and its design upon which the analysis is based) and material properties (affecting the failure modes, e.g., concerning undetected leakages and heat losses) (NUREG-1150, 1990; Helton, 1998; USNRC, 2002; Burgazzi, 2007a,b,c). Two examples of classical probabilistic models used to describe this kind of uncertainties in PRAs are the Poisson model for events randomly occurring in time (e.g., random variations of the operating state of a valve) and the binomial model for events occurring "as the immediate consequence of a challenge" (e.g., failures on demand) (NUREG-CR-6850, 2005). The effects of these uncertainties are then propagated onto the risk measure, e.g., by Monte Carlo simulation based on Importance Sampling or Stratified Sampling (Hofer et al., 2002; Cacuci and Ionescu-Bujor, 2004; Krzykacz-Hausmann, 2006). The contribution of aleatory uncertainty to nuclear passive systems failure is quite clear: for example, natural circulation could be altered by a random disturbance in the system geometry or by a random variation of the operating state of a component (Pagani et al., 2005).

In the present paper, the representation and propagation of aleatory uncertainties are not considered, the focus being on epistemic uncertainty (Pagani et al., 2005; Bassi and Marquès, 2008; Mackay et al., 2008; Mathews et al., 2008; Patalano et al., 2008; Arul et al., 2009, 2010).

Epistemic uncertainty is associated to the lack of knowledge about the properties and conditions of the phenomena (i.e., natural circulation) underlying the behavior of the passive systems. This uncertainty manifests itself in the model representation of the system behavior, in terms of both (*model*) uncertainty in the hypotheses assumed and (*parameter*) uncertainty in the values of the parameters of the model (Cacuci and Ionescu-Bujor, 2004; Helton et al., 2006; Patalano et al., 2008).

Model uncertainty arises because mathematical models are simplified representations of real systems and, therefore, their results may be affected by error or bias. Model uncertainty also includes the fact that the model could be too simplified and therefore would neglect some important phenomena affecting the final result. This latter type of uncertainty is sometimes identified independently from model uncertainty and is known as *completeness* uncertainty (USNRC, 2009).

Model uncertainty may for example involve the correlations adopted to describe the T–H phenomena, which are subject to errors of approximation. Such uncertainties may for example be captured by a multiplicative model (Zio and Apostolakis, 1996;

Patalano et al., 2008):

$$z = c(\boldsymbol{x})\varepsilon, \quad (1)$$

where z is the real value of the quantity to be predicted (e.g., heat transfer coefficients, friction factors, Nusselt numbers or thermal conductivity coefficients), $c(\cdot)$ is the mathematical model of the correlation (i.e., the result of the correlation as computed by the T–H code), $\boldsymbol{x}$ is the vector of correlating variables and ε is the associated multiplicative error factor: as a result, the uncertainty in the quantity z to be predicted is translated into an uncertainty in the multiplicative error factor ε. This error is commonly classified as representing *model* uncertainty.

Furthermore, uncertainty affects the values of the *parameters* used to describe the system (e.g., power level, pressure, cooler wall temperature, material conductivity, ...), e.g., owing to errors in their measurement or insufficient data and information. For example, according to industry practice and experience, an error of 2% is usually considered in the determination of the power level in a reactor, due to uncertainties in the measurements. As a consequence, the power level is usually known only to a certain level of precision, i.e., epistemic uncertainty is associated with it.

Both model and parameter uncertainties associated to the current state of knowledge of the system can be represented by subjective probability distributions within a Bayesian approach to PRA (Apostolakis, 1990, 1995, 1999). In current PRAs, the effect of these uncertainties is often propagated on the risk measure by Latin Hypercube Sampling (LHS) (Helton and Davis, 2003).

Epistemic uncertainties affect also the identification of the *failure criterion* to be adopted for the system under analysis: for instance, reactor parameters (e.g., the maximal cladding temperature) as well as passive system variables (e.g., the thermal power exchanged in a cooler) could be equally adopted as indicators of the safety performance of the passive system; furthermore, the failure thresholds may be established as point-targets (e.g., a specific quantity of liquid must be delivered within a fixed time) or time-varying targets or even integral targets over a defined mission time (e.g., the system must reject at least a given value of thermal power during the entire system intervention) (Jafari et al., 2003; Marquès et al., 2005).

Finally, state-of-knowledge uncertainty affects the identification of the possible *failure modes* and related *causes* and *consequences*, such as leaks (e.g., from pipes and pools), deposit thickness on components surfaces (e.g., pipes or heat exchangers), presence of non-condensable gases, stresses, blockages and material defects (Burgazzi, 2007a). The identification of all the relevant modes/causes of failure in terms of *critical parameters* for the passive system performance/stability and the assessment of the relative uncertainty may be attempted by commonly used hazard identification procedures, like HAZard and OPerability (HAZOP) analysis and Failure Mode and Effect Analysis (FMEA) (Burgazzi, 2004, 2006).

The contribution of epistemic uncertainties to the definition of the reliability/failure probability of nuclear passive systems can be qualitatively explained as follows. If the analyst is not fully confident on the validity of the correlations adopted to estimate, e.g., the design value of the heat transfer coefficient in the core during natural convection (e.g., due to the paucity of experimental data available in support of the use of a particular correlation), he/she admits that in a *real* accident scenario the *actual* value of the heat transfer coefficient in the core might deviate from the nominal/design one (i.e., different from the value computed by a deterministic correlation). If this variation (accepted as plausible by the analyst) were to take place during an accident scenario, it may cause the passive system to fail performing its safety function; based on the current state of knowledge of the heat transfer phenomenon in the core under the expected conditions, the likelihood of the heat transfer coefficient variation is to be quantified for *estimating* the reliability/failure probability. A future improvement in the state of knowledge, e.g., due to the collection of data and information useful to improve the characterization of the heat transfer phenomenon, would lead to a change in the epistemic uncertainty distribution describing the likelihood of the various values of heat transfer coefficient and eventually to a more accurate *estimate* of the system reliability/failure probability (Pagani et al., 2005; Bassi and Marquès, 2008; Mackay et al., 2008; Mathews et al., 2008, 2009; Patalano et al., 2008; Arul et al., 2009, 2010; Fong et al., 2009).

In the present paper, *only* epistemic uncertainties are considered in the estimation of the reliability/failure probability of nuclear passive systems (Pagani et al., 2005; Bassi and Marquès, 2008; Mackay et al., 2008; Mathews et al., 2008; Patalano et al., 2008; Arul et al., 2009,2010).

3. Functional failure analysis of nuclear passive systems

The essential steps for the conceptual development of the functional failure analysis of nuclear passive systems are briefly reported below (Marquès et al., 2005):

1. Detailed modeling of the system response by means of a deterministic, best-estimate (typically long-running) T–H code.
2. Identification of the vector $\boldsymbol{x} = \{x_1, x_2, \ldots, x_j, \ldots, x_{n_i}\}$ of parameters/variables, models and correlations (i.e., the inputs to the T–H code) which contribute to the uncertainty in the vector $\boldsymbol{y} = \{y_1, y_2, \ldots, y_l, \ldots, y_{n_o}\}$ of the outputs of the best-estimate T–H calculations (Section 2).
3. Propagation of the uncertainties associated to the identified relevant parameters, models and correlations $\boldsymbol{x}$ (step 2. above) through the deterministic, long-running T–H code in order to provide a complete representation (in terms of Probability Density Functions – PDFs, Cumulative Distribution Functions – CDFs and so on) of the *uncertainty* associated to the vector $\boldsymbol{y}$ of the outputs (step 2. above) of the deterministic, best-estimate T–H code.
4. Estimation of the *functional failure probability* of the passive system conditional on the current state of knowledge about the phenomena involved (step 2. above) (Pagani et al., 2005; Bassi and Marquès, 2008; Mackay et al., 2008; Mathews et al., 2008, 2009; Patalano et al., 2008; Arul et al., 2009, 2010; Fong et al., 2009; Zio and Pedroni, 2009a,b,c, 2010; Pedroni et al., 2010; Zio et al., 2010). Formally, let $Y(\boldsymbol{x})$ be a single-valued scalar variable indicator of the performance of the passive system (e.g., the fuel peak cladding temperature) and α_Y a threshold value defining the corresponding failure criterion (e.g., a limit value imposed by regulating authorities).[5] For illustrating purposes, let us assume that the passive system operates as long as $Y(\boldsymbol{x}) < \alpha_Y$; equivalently, introducing a variable called Performance Function (PF) as $g_x(\boldsymbol{x}) = Y(\boldsymbol{x}) - \alpha_Y$, failure occurs if $g_x(\boldsymbol{x}) > 0$. The probability $P(F)$ of system functional failure can then be expressed by the multidimensional integral:

$$P(F) = \iint \ldots \int I_F(\boldsymbol{x}) q(\boldsymbol{x}) d\boldsymbol{x} \quad (2)$$

where $q(\cdot)$ is the joint Probability Density Function (PDF) representing the uncertainty in the parameters $\boldsymbol{x}$, F is the failure

[5] Note that the choice of a *single-valued* performance function does not reduce the generality of the approach, because any multidimensional vector of physical quantities (i.e., the vector $\boldsymbol{y}$ of the outputs of the T–H code in this case) can be conveniently re-expressed as a scalar parameter by resorting to suitable min–max transformations: see Au and Beck (2001, 2003b) and Zio and Pedroni (2009b,c, 2010) for details.

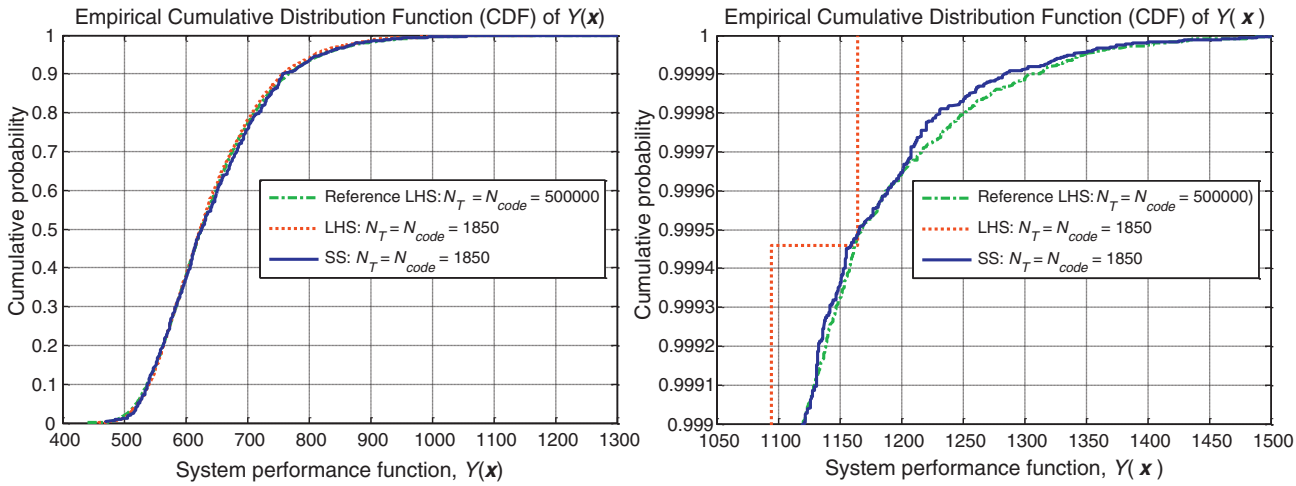


Fig. 1. Empirical CDF of the performance function $Y(\boldsymbol{x})$ of the passive system in Pagani et al. (2005). Solid lines: SS with $N_T = 1850$ samples; dashed lines: LHS with $N_T = 1850$ samples; dot-dashed lines: reference LHS with $N_T = 500{,}000$ samples.

region (where $g_x(\cdot) > 0$) and $I_F(\cdot)$ is an indicator function such that $I_F(\boldsymbol{x}) = 1$, if $\boldsymbol{x} \in F$ and $I_F(\boldsymbol{x}) = 0$, otherwise. The MCS procedure for estimating the functional failure probability entails that a *large* number N_T of samples of the values of the system parameters $\boldsymbol{x}$ be drawn from the corresponding probability distributions and used to evaluate $Y(\boldsymbol{x})$ by running the T–H code. An estimate $\hat{P}(F)^{N_T}$ of the probability of failure $P(F)$ can then be computed by dividing the number of times that $Y(\boldsymbol{x}) > \alpha_Y$ by the total number of samples N_T.

5. Perform a sensitivity study to determine the contribution of the individual uncertain parameters (i.e., the inputs to the T–H code) $\{x_j: j = 1, 2, \ldots, n_i\}$ to the uncertainty in the outputs of the T–H code $\{y_l: l = 1, 2, \ldots, n_o\}$ (and in the performance function $Y(\boldsymbol{x})$ of the passive system) and consequently to the functional failure probability of the T–H passive system. As is true for uncertainty propagation (step 4. above), sensitivity analysis relies on *multiple* (e.g., many thousands) evaluations of the code for different combinations of system inputs.

In this work, we propose to tackle the computational burden posed by the uncertainty propagation, failure probability estimation and sensitivity analysis of steps 3.–5. above in two effective ways (Section 4): from one side, efficient Monte Carlo Simulation techniques can be employed to perform robust estimations with a limited number of input samples (Section 4.1); from the other side, fast-running, surrogate regression models (also called response surfaces or meta-models) can be used to replace the long-running T–H model code (Section 4.2).

4. Handling the computational issues associated to the functional reliability assessment of nuclear passive systems

In this section, the two approaches considered for dealing with the computational issue associated to the functional reliability assessment of nuclear passive systems are summarized: in Section 4.1, various Monte Carlo Simulation techniques are synthetically described; in Section 4.2, empirical regression modeling is presented as a means to build fast-running, surrogate models for replacing the long-running T–H model codes. Both approaches are critically reviewed on the basis of the available literature.

4.1. Advanced Monte Carlo Simulation methods

As previously stated, the computational issues described in the previous Section 3 can be tackled from one side by resorting to efficient simulation techniques that perform robust estimations with

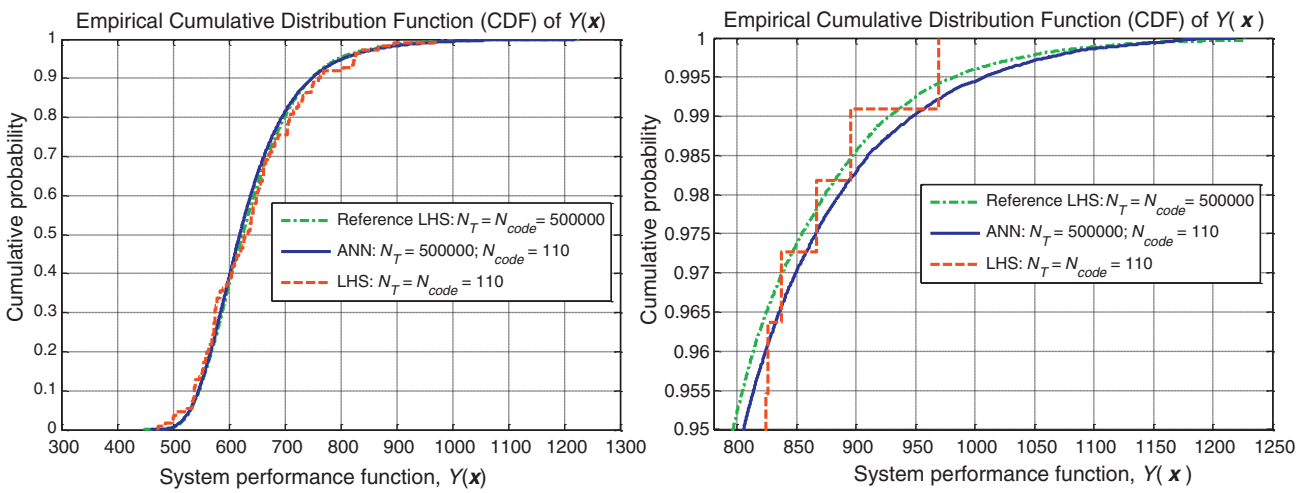


Fig. 2. Empirical CDF of the performance function $Y(\boldsymbol{x})$ of the passive system in Pagani et al. (2005). Solid lines: $N_T = 500{,}000$ estimations from $B = 1000$ bootstrapped ANNs built on $N_{code} = N_{train} + N_{val} + N_{test} = 80 + 20 + 10 = 110$ input/output examples (i.e., T–H code runs); dashed lines: LHS with $N_T = N_{code} = 110$ samples (i.e., T–H code runs); dot-dashed lines: reference LHS with $N_T = N_{code} = 500{,}000$ samples (i.e., T–H code runs).

a limited number of input samples, thus with an associated low computational time.

One such technique is the Importance Sampling (IS) method (Kalos and Whitlock, 1986; Au and Beck, 2003a; Au, 2004; Schueller et al., 2004). This technique amounts to replacing the original PDF of the uncertain variables with an Importance Sampling Density (ISD) chosen so as to generate samples that lead to failure more frequently (Au and Beck, 2003a). IS has the capability of considerably reducing the variance of the estimates compared with standard MCS, provided that the ISD is chosen similar to the theoretical optimal one. In practice, substantial insights on the system behavior and extensive modeling work may be required to identify a "good" ISD, e.g., by setting up complex kernel density estimators (Au and Beck, 2003a), by identifying the design point of the problem (Au, 2004) or simply by tuning the parameters of the ISD based on expert judgment and trial-and-error (Pagani et al., 2005). Overall, this increases the effort associated to the simulation; furthermore, there is always the risk that an inappropriate choice of the ISD may lead to worse estimates compared to standard MCS (Schueller et al., 2004).

Another technique is Stratified Sampling. This technique requires dividing the sample space into several non-overlapping subregions (referred to as "strata") and calculating the probability of each subregion; the (stratified) sample is then obtained by randomly sampling a predefined number of outcomes from *each* stratum (Helton and Davis, 2003; Cacuci and Ionescu-Bujor, 2004). By so doing, the full coverage of the sample space is ensured while maintaining the probabilistic character of random sampling. A major issue related to the implementation of Stratified Sampling lies in defining the strata and calculating the associated probabilities, which may require considerable a priori knowledge. As a remark, notice that the widely used event tree techniques in nuclear reactor PRA can be seen as defining and implementing Stratified Sampling of accident events and scenarios (Cacuci and Ionescu-Bujor, 2004).

A popular compromise between plain random sampling (i.e., standard MCS) and Importance/Stratified Sampling is offered by LHS, which is commonly used in PRA (Morris, 2000) for efficiently generating random samples (MacKay et al., 1979; Helton and Davis, 2003; Helton et al., 2005; Sallaberry et al., 2008). The effectiveness of LHS, and hence its popularity, derives from the fact that it provides a dense *stratification* over the range of each uncertain variable, with a relatively small sample size, while preserving the desirable probabilistic features of simple random sampling; moreover, there is no necessity to determine strata and strata probabilities like in Stratified Sampling (Helton and Davis, 2003). For these reasons LHS is frequently adopted for efficiently propagating *epistemic* uncertainties in PRA problems (NUREG-1150, 1990; Helton, 1998; Hofer et al., 2002; Krzykacz-Hausmann, 2006; Helton and Sallaberry, 2009).

On the other hand, LHS is very efficient for estimating mean values and standard deviations in complex reliability problems (Olsson et al., 2003), but only slightly more efficient than standard MCS for estimating small failure probabilities (Pebesma and Heuvelink, 1999), like those expected for passive safety systems.

Recently, SS (Au and Beck, 2001, 2003b) and LS (Koutsourelakis et al., 2004; Pradlwarter et al., 2005) have been proposed as advanced Monte Carlo Simulation methods for efficiently tackling the multidimensional problems of structural reliability. These methods have proved efficient also in the estimation of the functional failure probability of T–H passive systems (Zio and Pedroni, 2009b,c, 2010). Indeed, structural reliability problems are also formulated within a functional failure framework of analysis, in which the systems fail whenever the load applied (i.e., the stress) exceeds their capacity (i.e., the resistance) (Schueller and Pradlwarter, 2007). This makes the two methods suitable for application to the functional reliability analysis of nuclear passive systems, where the failure is specified in terms of one or more safety variables (e.g., temperatures, pressures, flow rates, . . .) crossing the safety thresholds specified by the regulating authorities (Bassi and Marquès, 2008; Mackay et al., 2008; Mathews et al., 2008; Patalano et al., 2008).

More specifically, in the SS approach, the functional failure probability is expressed as a product of conditional probabilities of some chosen intermediate and thus more frequent events. The problem of evaluating the small probabilities of functional failures is thus tackled by performing a sequence of simulations of more frequent events in their conditional probability spaces; the necessary conditional samples are generated through successive Markov Chain Monte Carlo (MCMC) simulations (Metropolis et al., 1953), in a way to gradually populate the intermediate conditional regions until the final functional failure region is reached.

In the LS method, *lines*, instead of random *points*, are used to probe the failure domain of the high-dimensional problem under analysis (Pradlwarter et al., 2005). An "important direction" is optimally determined to point towards the failure domain of interest and a number of conditional, one-dimensional problems are solved along such direction, in place of the high-dimensional problem (Pradlwarter et al., 2005). The approach has been shown to perform better than standard MCS in a wide range of reliability applications (Koutsourelakis et al., 2004; Schueller et al., 2004; Pradlwarter et al., 2005, 2007; Schueller and Pradlwarter, 2007; Lu et al., 2008; Valdebenito et al., 2010; Zio and Pedroni, 2009c, 2010). Furthermore, if the boundaries of the failure domain of interest are not too rough (i.e., almost linear) and the "important direction" is almost perpendicular to them, the variance of the failure probability estimator could be ideally reduced to zero (Koutsourelakis et al., 2004).[6]

In the present paper, particular focus is devoted to SS and LS: for this reason, synthetic descriptions of these techniques and an illustrative application to the functional failure analysis of a T–H passive system are reported in Section 5.

4.2. Empirical regression modeling

Another way to tackle the computational issues associated to the reliability analysis of nuclear passive systems is that of resorting to fast-running, surrogate regression models, also called response surfaces or meta-models, to approximate the input/output function implemented in the long-running system model code, and then substitute it in the passive system reliability analysis (Storlie and Helton, 2008).

The construction of such regression models entails running the system model code a predetermined, *reduced* number of times (e.g., 50–100) for specified values of the uncertain input variables and collecting the corresponding values of the output of interest; then, statistical techniques are employed for calibrating/adapting the internal *parameters/coefficients* of the response surface of the regression model in order to fit the input/output data generated in the previous step.

Putting it in a formal framework, let us consider a generic metamodel to be built for performing the task of nonlinear regression, i.e., estimating the nonlinear relationship between a vector of input

[6] Apart from efficient MC techniques, there exist methods based on nonparametric order statistics (Wilks, 1942) that propagate uncertainties through mechanistic T–H codes with reduced computational burden, especially if only one- or two-sided confidence intervals are needed for particular statistics (e.g., the 95th percentile) of the outputs of the code. For example, the so-called *coverage* (Guba et al., 2003; Makai and Pal, 2006) and *bracketing* (Nutt and Wallis, 2004) approaches can be used to identify the number of sample code runs required to obtain a given *confidence* level on the estimates of prescribed statistics of the code outputs.

variables $\boldsymbol{x} = \{x_1, x_2, \ldots, x_j, \ldots, x_{n_i}\}$ and a vector of output targets $\boldsymbol{y} = \{y_1, y_2, \ldots, y_l, \ldots, y_{n_o}\}$, on the basis of a *finite* (and possibly *small*) set of input/output data examples (i.e., patterns), $D_{train} = \{(\boldsymbol{x}_p, \boldsymbol{y}_p), p = 1, 2, \ldots, N_{train}\}$ (Zio, 2006). It can be assumed that the target vector $\boldsymbol{y}$ is related to the input vector $\boldsymbol{x}$ by an unknown nonlinear deterministic function $\boldsymbol{\mu_y}(\boldsymbol{x})$ corrupted by a noise vector $\boldsymbol{\varepsilon}(\boldsymbol{x})$, i.e.,

$$\boldsymbol{y}(\boldsymbol{x}) = \boldsymbol{\mu}_y(\boldsymbol{x}) + \boldsymbol{\varepsilon}(\boldsymbol{x}) \tag{3}$$

As introduced in Section 3, in the present case of T–H passive system functional failure probability assessment the vector $\boldsymbol{x}$ contains the relevant uncertain system parameters/variables, the nonlinear deterministic function $\boldsymbol{\mu}_y(\boldsymbol{x})$ represents the complex, long-running T–H mechanistic model code (e.g., RELAP5-3D), the vector $\boldsymbol{y}(\boldsymbol{x})$ contains the output variables of interest for the analysis and the noise $\boldsymbol{\varepsilon}(\boldsymbol{x})$ represents the errors introduced by the numerical methods employed to calculate $\boldsymbol{\mu}_y(\boldsymbol{x})$ (Storlie et al., 2009); for simplicity, in the following we assume $\boldsymbol{\varepsilon}(\boldsymbol{x}) = 0$ (Secchi et al., 2008). Thus, the objective of the regression task is to estimate $\boldsymbol{\mu}_y(\boldsymbol{x})$ in (3) by means of a regression function $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{w}^*)$ depending on a set of parameters $\boldsymbol{w}^*$ to be properly determined on the basis of the available data set D_{train}. The algorithm used to calibrate the set of parameters $\boldsymbol{w}^*$ is obviously dependent on the nature of the regression model adopted, but in general it aims at minimizing the mean (absolute or quadratic) error between the output targets of the original T–H code, $\boldsymbol{y}_p = \boldsymbol{\mu_y}(\boldsymbol{x}_p)$, $p = 1, 2, \ldots, N_{train}$, and the output vectors of the regression model, $\hat{\boldsymbol{y}}_p = \boldsymbol{f}(\boldsymbol{x}_p, \boldsymbol{w}^*)$, $p = 1, 2, \ldots, N_{train}$; for example, the Root Mean Squared Error (RMSE) is commonly adopted to this purpose (Zio, 2006).

Several examples can be found in the open literature concerning the application of surrogate meta-models in reliability problems. In Bucher and Most (2008), Gavin and Yau (2008) and Liel et al. (2009), polynomial Response Surfaces (RSs) are employed to evaluate the failure probability of structural systems; in Arul et al. (2009, 2010), Fong et al. (2009) and Mathews et al. (2009), *linear* and *quadratic* polynomial RSs are employed for performing the reliability analysis of T–H passive systems in advanced nuclear reactors; in Deng (2006), Hurtado (2007), Cardoso et al. (2008) and Cheng et al. (2008), learning statistical models such as ANNs, Radial Basis Functions (RBFs) and Support Vector Machines (SVMs) are trained to provide *local* approximations of the failure domain in structural reliability problems; in Volkova et al. (2008) and Marrel et al. (2009), Gaussian meta-models are built to calculate global sensitivity indices for a complex hydrogeological model simulating radionuclide transport in groundwater.

However, when using the approximation of the system output provided by an empirical regression model, an additional source of *model* uncertainty is introduced which needs to be evaluated, particularly in safety critical applications like those related to nuclear power plant technology. In this paper we propose to resort to *bootstrapped* regression models (Efron and Thibshirani, 1993), i.e., ensembles of regression models, constructed on different data sets bootstrapped from the original one (Zio, 2006; Storlie et al., 2009). In fact, the ensemble framework of regression modeling allows quantifying the model uncertainty associated to the estimates provided by the regression models in terms of *confidence intervals*.

The bootstrap method is a distribution-free inference method which requires no prior knowledge about the distribution function of the underlying population (Efron and Thibshirani, 1993). The basic idea is to generate samples from the observed data by sampling with replacement from the original data set (Efron and Thibshirani, 1993): each of these bootstrapped data sets is used to build a bootstrapped regression model which is used to calculate the reliability quantity of interest (e.g., the passive system failure probability in this case). From the theory and practice of ensembles of empirical models, it can be shown that the estimates given by bootstrapped regression models is in general more accurate than the estimate of the best regression model in the bootstrap ensemble of regression models (Zio, 2006; Cadini et al., 2008).

Some examples of the application of the bootstrap method for the evaluation of the uncertainties associated to the output of regression models in safety-related problems can be found in the literature: in Zio (2006), bootstrapped ANNs are trained to predict nuclear transients processes; in Cadini et al. (2008) and Secchi et al. (2008), the model uncertainty, quantified in terms of a *standard deviation*, is used to "correct" the ANN output in order to provide conservative estimates for important safety parameters in nuclear reactors (i.e., percentiles of the pellet cladding temperature); finally, in Storlie et al. (2009), the bootstrap procedure is combined with different regression techniques, e.g., Multivariate Adaptive Regression Spline (MARS), Random Forest (RF) and Gradient Boosting Regression (GBR), to calculate confidence intervals for global sensitivity indices of the computationally demanding model of a nuclear waste repository.

In the present paper, particular emphasis is given to bootstrapped ANN regression models: for this reason, a synthetic description of this technique and an illustrative application to the functional failure analysis of a T–H passive system is reported in Section 5.

5. Recommendations for reducing the computational burden associated to the functional reliability analysis of nuclear passive systems

In this section (i) the different phases of the functional reliability analysis of nuclear passive systems are considered: in particular, the estimation of the functional failure probability (Section 5.1), the uncertainty propagation (Section 5.2) and sensitivity analysis (Section 5.3) phases; (ii) on the basis of the literature review and the considerations made in the previous Section 4, techniques are recommended to efficiently tackle the computational burden associated to *each* of these analyses; (iii) guidelines on the recommended techniques are provided, with illustrative applications to the functional reliability analysis of a nuclear passive system of literature (Pagani et al., 2005).

5.1. Functional failure probability estimation

If the analyst is only interested in an accurate and precise estimation of the (typically small) functional failure probability of the T–H passive system (modeled by a *long-running*, *nonlinear* and *non-monotonous* T–H code), then the use of the Line Sampling technique is strongly suggested.

In extreme synthesis, the computational steps of the algorithm are (Pradlwarter et al., 2005, 2007):

1. From the original multidimensional joint probability density function $q(\cdot): \Re^n \to [0, \infty)$, sample N_T vectors $\{\boldsymbol{x}^k : k = 1, 2, \ldots, N_T\}$, with $\boldsymbol{x}^k = \left\{x_1^k, x_2^k, \ldots, x_j^k, \ldots, x_n^k\right\}$.
2. Transform the N_T sample vectors $\{\boldsymbol{x}^k : k = 1, 2, \ldots, N_T\}$ defined in the original (i.e., physical) space into N_T samples $\{\boldsymbol{\theta}^k : k = 1, 2, \ldots, N_T\}$ defined in the so-called "standard normal space", where each random variable is represented by an independent central unit Gaussian distribution; also the PFs $g_x(\cdot)$ defined in the physical space have to be transformed into $g_\theta(\cdot)$ in the standard normal space (Huang and Du, 2006).
3. In the standard normal space, determine a *unit* vector $\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \ldots, \alpha_j, \ldots, \alpha_n\}^T$ (hereafter also called "important unit vector" or "important direction") pointing towards the failure domain F of interest.
4. Reduce the problem of computing the high-dimensional failure probability integral (2) to a number of conditional one-

dimensional problems, solved along the "important direction" $\boldsymbol{\alpha}$ in the standard normal space: in particular, estimate N_T conditional "one-dimensional" failure probabilities $\{\hat{P}(F)^{1D,k} : k = 1, 2, \ldots, N_T\}$, corresponding to each one of the standard normal samples $\{\boldsymbol{\theta}^k : k = 1, 2, \ldots, N_T\}$ obtained in step 2. Notice that $2 \cdot N_T$ or $3 \cdot N_T$ system performance analyses (i.e., runs of the T–H model code) have to be carried out to calculate *each* of the N_T conditional one-dimensional failure probability estimates $\{\hat{P}(F)^{1D,k} : k = 1, 2, \ldots, N_T\}$ (see Pradlwarter et al., 2005, 2007 for details).

5. Compute the unbiased estimator $\hat{P}(F)^{N_T}$ for the failure probability $P(F)$ and its variance $\sigma^2\left[\hat{P}(F)^{N_T}\right]$ as:

$$\hat{P}(F)^{N_T} = \left(\frac{1}{N_T}\right)\sum_{k=1}^{N_T}\hat{P}(F)^{1D,k}, \tag{4}$$

$$\sigma^2\left[\hat{P}(F)^{N_T}\right] = \left(\frac{1}{N_T}\right)(N_T - 1)\sum_{k=1}^{N_T}\left(\hat{P}(F)^{1D,k} - \hat{P}(F)^{N_T}\right)^2. \tag{5}$$

The LS method here outlined can significantly reduce the variance (5) of the estimator (4) of the failure probability integral (2) (Koutsourelakis et al., 2004); however, its efficiency depends on the determination of the important direction $\boldsymbol{\alpha}$ (step 3. above).

With respect to this issue, four methods have been proposed in the open literature to estimate the important direction $\boldsymbol{\alpha}$ for LS. In Koutsourelakis et al. (2004), the important unit vector $\boldsymbol{\alpha}$ is computed as the normalized "center of mass" of the failure domain F of interest; in Koutsourelakis et al. (2004) and Valdebenito et al. (2010), the important unit vector $\boldsymbol{\alpha}$ is taken as pointing in the direction of the "design point" in the standard normal space; in Pradlwarter et al. (2005), the direction of $\boldsymbol{\alpha}$ is identified as the normalized gradient of the performance function $g_\theta(\cdot)$ in the standard normal space; finally, in a previous paper by the authors (Zio and Pedroni, 2010), the important direction $\boldsymbol{\alpha}$ is taken as the one minimizing the variance (5) of the failure probability estimator (4). This latter method produces more accurate and precise failure probability estimates than those provided by the other three techniques of literature and, for this reason, its adoption is recommended for the estimation of the small failure probabilities of T–H passive systems.

In more details, in Zio and Pedroni (2010) the *optimal* important direction $\boldsymbol{\alpha}^{opt}$ for Line Sampling is defined as the one minimizing the variance $\sigma^2\left[\hat{P}(F)^{N_T}\right]$ (5) of the LS failure probability estimator $\hat{P}(F)^{N_T}$ (4). Notice that $\boldsymbol{\alpha}^{opt}$ can be expressed as the normalized version of a proper vector $\boldsymbol{\theta}^{opt}$ in the standard normal space, i.e., $\boldsymbol{\alpha}^{opt} = \boldsymbol{\theta}^{opt}/||\boldsymbol{\theta}^{opt}||_2$. Thus, in order to search for a physically meaningful important unit vector $\boldsymbol{\alpha}^{opt}$ (i.e., a vector that optimally points towards the failure domain F of interest), $\boldsymbol{\theta}^{opt}$ should belong to the failure domain F of interest, i.e., $\boldsymbol{\theta}^{opt} \in F$ or, equivalently, $g_\theta(\boldsymbol{\theta}^{opt}) > 0$.

In mathematical terms, the optimal LS important direction $\boldsymbol{\alpha}^{opt}$ is obtained by solving the following nonlinear constrained minimization problem:

$$\text{Find } \boldsymbol{\alpha}^{opt} = \boldsymbol{\theta}^{opt}/||\boldsymbol{\theta}^{opt}||_2 : \sigma^2\left[\hat{P}(F)^{N_T}\right] = \min_{\boldsymbol{\alpha}=\boldsymbol{\theta}/||\boldsymbol{\theta}||_2}\left\{\sigma^2\left[\hat{P}(F)^{N_T}\right]\right\} \tag{6}$$
$$\text{subject to } \boldsymbol{\theta} \in F (\text{i.e., } g_\theta(\boldsymbol{\theta}) > 0).$$

The conceptual steps of the procedure for solving (6) are (Zio and Pedroni, 2010):

1. An optimization algorithm proposes a candidate solution $\boldsymbol{\alpha} = \boldsymbol{\theta}/||\boldsymbol{\theta}||_2$ to (6): for example, probabilistic search algorithms like Genetic Algorithms (GAs) (Konak et al., 2006; Marseguerra et al., 2006) are particularly suitable for multivariate nonlinear problems like those involving nuclear passive safety systems (Zio and Pedroni, 2010).
2. The LS failure probability estimator $\hat{P}(F)^{N_T}$ (4) and the associated variance $\sigma^2\left[\hat{P}(F)^{N_T}\right]$ (5) are calculated using the unit vector $\boldsymbol{\alpha} = \boldsymbol{\theta}/||\boldsymbol{\theta}||_2$ proposed as important direction in step 1. above.
3. The variance $\sigma^2\left[\hat{P}(F)^{N_T}\right]$ obtained in step 2. above is the objective function to be *minimized*.
4. The feasibility of the proposed solution $\boldsymbol{\alpha} = \boldsymbol{\theta}/||\boldsymbol{\theta}||_2$ is checked by evaluating the system PF $g_\theta(\cdot)$ (i.e., by running the system model code) in correspondence of $\boldsymbol{\theta}$: if the proposed solution $\boldsymbol{\alpha} = \boldsymbol{\theta}/||\boldsymbol{\theta}||_2$ is not feasible (i.e., if $\boldsymbol{\theta} \notin F$ or, equivalently, $g_\theta(\boldsymbol{\theta}) \le 0$), it is *penalized* by *increasing* the value of the corresponding objective function $\sigma^2\left[\hat{P}(F)^{NT}\right]$.
5. Steps 1.–4. are repeated until a predefined stopping criterion is met and the optimization algorithm identifies the *optimal* unit vector $\boldsymbol{\alpha}^{opt} = \boldsymbol{\theta}^{opt}/||\boldsymbol{\theta}^{opt}||_2$.

Notice that (i) the optimization search requires the iterative evaluation of hundreds or thousands of possible solutions $\boldsymbol{\alpha} = \boldsymbol{\theta}/||\boldsymbol{\theta}||_2$ to (6) and (ii) $2 \cdot N_T$ or $3 \cdot N_T$ system performance analyses (i.e., runs of the system model code) have to be carried out to calculate the objective function $\sigma^2\left[\hat{P}(F)^{N_T}\right]$ for *each* proposed solution (steps 2. and 3. above); as a consequence, the computational effort associated to this technique would be absolutely prohibitive with a system model code requiring hours or even minutes to run a single simulation. Hence, for practical applicability, one has to resort to a regression model as a fast-running approximator of the original system model code for performing the calculations in steps 2. and 4. above, to make the computational cost acceptable.

The regression model suggested is the classical three-layered feed-forward ANN (Bishop, 1995). In order to improve the *accuracy* in the approximation of the system PF $g_\theta(\cdot)$ (needed for an accurate estimation of the LS important direction $\boldsymbol{\alpha}$), the employed ANN models can be trained by a properly devised *sequential*, *two-step* algorithm based on error back-propagation, as proposed in Zio and Pedroni (2010). In extreme synthesis, a *first-step* ANN regression model is built using a set of input/output data examples. The resulting ANN model is used (instead of the original, long-running system model code) to provide an *approximation* to the *design point* of the problem: this is meant to provide an approximate, rough indication of the real location of the failure domain F of interest. Subsequently, a new data set is randomly generated *centered* on the approximate design point previously identified: a *second-step* ANN model is then constructed on these newly generated data set. This should result in an ANN regression model which is more accurate in proximity of the failure domain F of interest, thus providing reliable estimates of the system PF $g_\theta(\cdot)$ for the identification of the LS important direction $\boldsymbol{\alpha}$ (Zio and Pedroni, 2010).

For completeness, we report some of the results obtained in a previous work by the authors (Zio and Pedroni, 2010), in which the optimized LS method described above is applied for the estimation of the *small* functional failure probability $P(F)$ of the passive decay heat removal system of a Gas-cooled Fast Reactor (GFR) of literature (Pagani et al., 2005) (notice that in this example $P(F) = 3.541 \times 10^{-4}$). A detailed description of the system is not reported here for brevity: the interested reader is referred to Pagani et al. (2005) for details.

Further, the benefits coming from the use of the proposed method is shown by means of a comparison between the estimation *accuracies* and *precisions* of the following simulation methods: (i) standard MCS; (ii) LHS (Helton and Davis, 2003); (iii) standard IS (Au and Beck, 2003a; Au, 2004); (iv) a combination of standard IS and LHS (hereafter referred to as IS + LHS) (Olsson et al., 2003); (v) SS (Au and Beck, 2001, 2003b); (vi) optimized LS (Zio and Pedroni, 2010); (vii) a combination of optimized LS and LHS (hereafter referred to as LS + LHS) (Zio and Pedroni, 2010). Part of the results used in the comparison are derived from the manipulation of results previously obtained by the authors (Zio and Pedroni, 2009b,c, 2010).

Table 3
Values of the performance indicators $\bar{\varepsilon}$ (8), $\bar{w}_{CI}$ (10) and FOM (11) obtained with $N_T = 1850$ samples by methods (i)–(vii) in the estimation of the functional failure probability $P(F)$ of the passive system in Pagani et al. (2005).

Functional failure probability ("True" value, $P(F) = 3.541 \times 10^{-4}$)					
Method	$N_{c,P(F)}$	$N_{c,add}$	Performance indicators ($N_T = 1850$; $S = 2000$)		
			$\bar{\varepsilon}$ (%)	$\bar{w}_{CI}$ (%)	*FOM*
Standard MCS (i)	$N_T = 1850$	0	101.681	305.874	1.081×10^3
LHS (ii)	$N_T = 1850$	0	96.652	305.870	1.222×10^3
IS (iii)	$N_T = 1850$	110	3.803	18.601	6.159×10^5
IS + LHS (iv)	$N_T = 1850$	110	3.564	17.970	7.121×10^5
SS (v)	$N_T = 1850$	0	35.760	183.180	6.414×10^3
LS (vi)	$3 \cdot N_T = 5550$	110	0.517	2.322	1.329×10^7
LS + LHS (vii)	$3 \cdot N_T = 5550$	110	0.268	1.102	8.295×10^7

In order to properly represent the randomness of the probabilistic simulation methods (i)–(vii) adopted and provide a statistically meaningful comparison between their performances in the estimation of the system failure probability $P(F)$, $S = 2000$ independent runs of each method have been carried out. In each simulation $s = 1, 2, \ldots, S$, the percentage relative absolute error ε_s between the true (reference) value of the system failure probability $P(F)$ and the corresponding estimate $\hat{P}(F)_s^{N_T}$ obtained with N_T samples is computed as follows:

$$\varepsilon_s = \frac{|P(F) - \hat{P}(F)_s^{N_T}|}{P(F)} \times 100, s = 1, 2, \ldots, S \tag{7}$$

The accuracies of the simulation methods of interest in the estimation of $P(F)$ are then compared in terms of the mean percentage relative absolute error $\bar{\varepsilon}$ over $S = 2000$ runs:

$$\bar{\varepsilon} = \left(\frac{1}{S}\right) \sum_{s=1}^{S} \varepsilon_s \tag{8}$$

The quantity (8) provides a measure of the percentage relative absolute error in the estimation of the failure probability $P(F)$ made *on average in a single run* by the simulation method with N_T samples; obviously, the lower $\bar{\varepsilon}$, the higher the *accuracy* of the method.

The failure probability estimates $\hat{P}(F)_s^{N_T}$, $s = 1, 2, \ldots, S$, are then used to build a *bootstrapped* 95% Confidence Interval (CI) for the failure probability estimator $\hat{P}(F)^{N_T}$, i.e.,

$$\left\lfloor L_{CI,\hat{P}(F)^{N_T}}, U_{CI,\hat{P}(F)^{N_T}} \right\rfloor \tag{9}$$

where $U_{CI,\hat{P}(F)^{N_T}}$ and $L_{CI,\hat{P}(F)^{N_T}}$ are the 2.5th and 97.5th percentiles, respectively, of the *bootstrapped empirical distribution* of the failure probability estimator $\hat{P}(F)^{N_T}$. The percentage relative *width* $\bar{w}_{CI}$ of the bootstrapped 95% CI of the LS failure probability estimator $\hat{P}(F)^{N_T}$ is then computed as

$$\bar{w}_{CI} = \frac{U_{CI,\hat{P}(F)^{N_T}} - L_{CI,\hat{P}(F)^{N_T}}}{P(F)} \times 100 \tag{10}$$

Obviously, the lower $\bar{w}_{CI}$, the higher the *precision* of the method.

Finally, in addition to the accuracy and precision of the failure probability estimator, also the computational time associated to the simulation method has to be taken into account. To this aim, the FOM can be used:

$$\text{FOM} = \frac{1}{\sigma^2(\hat{P}(F)^{N_T})t_{comp}} \approx \frac{1}{\hat{\sigma}^2(\hat{P}(F)^{N_T})t_{comp}} \tag{11}$$

where t_{comp} is the computational time required by the simulation method and $\sigma^2 \left\lfloor \hat{P}(F)^{N_T} \right\rfloor$ is defined in (5). Since $\sigma^2(\hat{P}(F)^{N_T}) \propto N_T$ and approximately $t_{comp} \propto N_T$, the FOM is independent of N_T. Obviously, the higher the FOM, the higher the computational efficiency of the method.

Table 3 reports the values of the performance indicators $\bar{\varepsilon}$ (8), $\bar{w}_{CI}$ (10) and FOM (11) obtained with $N_T = 1850$ samples by the simulation methods (i)–(vii) (notice that since N_T is the same for all the simulation methods, performance indicators $\bar{\varepsilon}$ (8) and $\bar{w}_{CI}$ (10) can be compared fairly). The number of T–H code runs required by each method is also reported: actually, when a single run of the system model code lasts several hours (which is often the case for passive safety systems) the total number of simulations is the *critical* parameter which determines the overall computational cost (i.e., t_{comp}) associated to the method. In particular, $N_{c,P(F)}$ is the number of code runs used by the algorithm *only* to *estimate* the failure probability $P(F)$; instead, $N_{c,add}$ is the number of *additional* code runs required to *set up* the method: for example, for IS and IS + LHS, $N_{c,add}$ code runs are used to build the ISD by identification of the "design point" of the problem (Au, 2004); instead, for LS and LS + LHS, $N_{c,add}$ code runs are used to identify the important direction $\boldsymbol{\alpha}$ by minimization of the variance of the LS failure probability estimator (Zio and Pedroni, 2010).

It can be seen that the optimized Line Sampling methods (i.e., both LS and LS + LHS) provide more accurate and precise failure probability estimates than the other methods: actually, the mean percentage errors $\bar{\varepsilon}$ are about 13–380 times lower than those of the other methods, whereas the percentage 95% CI widths $\bar{w}_{CI}$ are about 16–278 times lower than those of the other methods. Finally, although the computational cost associated to the optimized Line Sampling methods is higher than that of the other methods (because the total number of T–H code runs is more than 3 times larger), the overall computational efficiency of the method is significantly higher: actually, the FOM is about 2–4 *orders of magnitude* larger than that of the other methods.

The previous example has served to demonstrate that the optimized LS methods indeed provide more accurate and precise failure probability estimates than the other simulation methods considered. However, this must be achieved with a *small* number of samples (and, thus, of T–H model evaluations: say, few tens or hundreds depending on the application), because in practice the T–H computer codes require several hours to run a single simulation (Fong et al., 2009). Thus, we consider here a practical situation where the number $N_{c,P(F)}$ of T–H code runs allowed for estimating the *small* failure probability $P(F) = 3.541 \times 10^{-4}$ is set to few tens (e.g., 30 in this case). The results are summarized in Table 4.

It can be seen that even in this case the optimized Line Sampling methods (i.e., both LS and LS + LHS) provide more accurate and precise failure probability estimates than the other methods: actually, the mean percentage errors $\bar{\varepsilon}$ are about 6–44 times lower than those of the other methods, whereas the percentage 95% CI widths $\bar{w}_{CI}$ are about 6–163 times lower than those of the other methods. Finally, the global efficiency of the method is significantly higher: actually, the FOM is about 1–3 *orders of magnitude* larger than that of the other methods.

These results confirm the recommendation of adopting this method.

Table 4
Values of the performance indicators $\bar{\varepsilon}$ (8), $\bar{w}_{CI}$ (10) and FOM (11) obtained with $N_{c,P(F)}=30$ T–H code runs by methods (i)–(vii) in the estimation of the functional failure probability $P(F)$ of the passive system in Pagani et al. (2005).

Functional failure probability ("True" value, $P(F)=3.541\times10^{-4}$)					
Method	N_T	$N_{c,add}$	Performance indicators ($N_{c,P(F)}=30$; $S=2000$)		
			$\bar{\varepsilon}$ (%)	$\bar{w}_{CI}$ (%)	*FOM*
Standard MCS (i)	$N_{c,P(F)}=30$	0	206.150	3.943×10^3	911.541
LHS (ii)	$N_{c,P(F)}=30$	0	183.080	3.492×10^3	1.162×10^3
IS (iii)	$N_{c,P(F)}=30$	110	29.049	139.280	1.474×10^5
IS + LHS (iv)	$N_{c,P(F)}=30$	110	27.182	134.170	1.679×10^5
SS (v)	/	0	/	/	/
LS (vi)	$N_{c,P(F)}/3=10$	110	7.016	36.278	2.338×10^6
LS + LHS (vii)	$N_{c,P(F)}/3=10$	110	4.684	24.154	5.029×10^6

5.2. Uncertainty analysis

The objective of the uncertainty analysis is to propagate the uncertainty associated to the input parameters $\boldsymbol{x}=\{x_1,x_2,\ldots,x_j,\ldots,x_{ni}\}$ through the deterministic, long-running T–H code in order to quantify the uncertainty associated to the output variables $\boldsymbol{y}=\{y_1,y_2,\ldots,y_l,\ldots,x_{no}\}$ of interest and to the performance function $Y(\boldsymbol{x})$ of the passive system (e.g., computing PDFs, CDFs and percentiles).

In all fairness, notice that the strongly recommended LS technique allows *only* the (efficient) calculation of the failure probability of the passive system, but it does not allow a *complete* uncertainty propagation: actually, no PDFs, CDFs or percentiles of the T–H code outputs of interest can be identified in a single simulation run. Thus, if the analyst is interested in propagating the uncertainty onto the output, two options are recommended:

1. in the (unlikely) case that the T–H model is sufficiently simple and requires *seconds or minutes* to run, the use of the SS algorithm may represent the optimal choice (Section 5.2.1);
2. in those (more realistic) cases where the T–H model requires many hours, or days, to perform a single evaluation, the use of fast-running surrogate regression models (e.g., bootstrapped ANNs, in this work) instead of the long-running original T–H code seems mandatory (Section 5.2.2).

These recommendations are further explained and motivated below.

5.2.1. Uncertainty propagation using Subset Simulation

The idea underlying the SS method is to convert the simulation of an event (e.g., the rare failure event) into a sequence of simulations of intermediate conditional events corresponding to subsets (or subregions) of the uncertain input parameter space (for example, if a passive decay heat removal system in a nuclear reactor is assumed to fail when the fuel peak cladding temperature exceeds 725 °C, then plausible intermediate conditional events could be represented by the peak cladding temperature exceeding 350, 500 and 650 °C, respectively). During simulation, the conditional samples (lying in the intermediate subsets or subregions) are generated by means of properly designed Markov chains; by so doing, the conditional samples gradually populate the successive intermediate subsets (or subregions) up to the target (failure) region (Au and Beck, 2001, 2003b).

In synthesis, the SS algorithm proceeds as follows. First, N vectors $\{\boldsymbol{x}_0^k: k=1,2,\ldots,N\}$ are sampled by standard MCS, i.e., from the original probability density function $q(\cdot)$. The corresponding values of the response variable $\{Y(\boldsymbol{x}_0^k): k=1,2,\ldots,N\}$ are then computed and the first threshold value y_1 (identifying the first intermediate conditional event) is chosen as the $(1-p_0)N$th value in the increasing list of values $\{Y(\boldsymbol{x}_0^k): k=1,2,\ldots,N\}$. With this choice of y_1, there are now p_0N samples among $\{\boldsymbol{x}_0^k: k=1,2,\ldots,N\}$ whose response $Y(\boldsymbol{x})$ lies in the intermediate subregion $F_1=\{\boldsymbol{x}: Y(\boldsymbol{x})>y_1\}$. Starting from each one of these samples, MCMC simulation is used to generate $(1-p_0)N$ additional conditional samples in the intermediate subregion $F_1=\{\boldsymbol{x}: Y(\boldsymbol{x})>y_1\}$, so that there are a total of N conditional samples $\{\boldsymbol{x}_1^k: k=1,2,\ldots,N\}\in F_1$. Then, the intermediate threshold value y_2 is chosen as the $(1-p_0)N$th value in the ascending list of $\{Y(\boldsymbol{x}_1^k): k=1,2,\ldots,N\}$ to define $F_2=\{\boldsymbol{x}: Y(\boldsymbol{x})>y_2\}$. The p_0N samples lying in F_2 function as 'seeds' for sampling $(1-p_0)N$ additional conditional samples lying in F_2, making up a total of N conditional samples $\{\boldsymbol{x}_2^k: k=1,2,\ldots,N\}\in F_2$. This procedure is repeated until the samples lying in the intermediate subregion $F_{m-1}=\{\boldsymbol{x}: Y(\boldsymbol{x})>y_{m-1}\}$ are generated to yield $y_m>y$ as the $(1-p_0)N$th value in the ascending list of $\{Y(\boldsymbol{x}_{m-1}^k): k=1,2,\ldots,N\}$ (Au and Beck, 2001, 2003b; Au, 2005; Au et al., 2007).

The superior efficiency of SS with respect to standard MCS in the uncertainty propagation task has been widely demonstrated in the open literature: the interested reader may refer to Au and Beck (2001, 2003b) for mathematical details, to Ching et al. (2005), Katafygiotis and Cheung (2005,2007), Au (2007), Au et al. (2007) and Pradlwarter et al. (2007) for illustrative applications to high-dimensional (i.e., $n\geq100$) structural reliability problems and to Zio and Pedroni (2009b) for an application to the functional failure analysis of a T–H passive system.

For completeness, we report some of the results previously obtained by the authors (Zio and Pedroni, 2009b) in the use of the SS method to propagate the uncertainties through the T–H model of the passive decay heat removal system of a GFR analyzed in the previous Section 5.1 (Pagani et al., 2005). Nine uncertain input parameters $\{x_j: j=1,2,\ldots,9\}$ are taken into account and two safety variables $\{y_l: l=1,2\}$ (i.e., the hot- and average-channel temperatures of the naturally circulating coolant leaving the core) are considered as outputs of interest of the T–H system model code. The output variables $\{y_l: l=1,2\}$ are then used to generate a single-valued system performance indicator (or critical response variable) $Y(\boldsymbol{x})$ for the evaluation of passive system failure; further details can be found in Pagani et al. (2005) and Zio and Pedroni (2009b).

The performance of SS is compared to that of LHS: notice that LHS has been chosen as benchmark method due to its popularity and wide use in PRA (Helton and Davis, 2003; Sallaberry et al., 2008; Helton and Sallaberry, 2009). Following the approach presented in Au et al. (2007) and subsequently used in Zio and Pedroni (2009b), Fig. 1, left shows the empirical Cumulative Distribution Function (CDF) of the performance function $Y(\boldsymbol{x})$ of the passive decay heat removal system considered; in addition, Fig. 1, right focuses on the portion of CDF where the cumulative probability ranges between 0.999 and 1. The results produced by SS with a total of $N_T=1850$ samples (i.e., T–H code runs) are shown in solid lines, whereas those produced by LHS with the same number of samples/T–H code runs (i.e., $N_T=1850$) are shown in dashed lines. The dot-dashed

lines correspond to the results obtained by LHS with $N_T = 500{,}000$ samples/T–H code runs: this number of samples is largely sufficient for efficiently estimating the CDF even where the cumulative probability ranges between 0.999 and 1: thus, the corresponding results are taken as benchmarks.

Notice that the results from SS are satisfactorily close to the reference solution in all the probability ranges considered. On the contrary, LHS with 1850 samples is not able to produce accurate results for values of the cumulative probability very close to 1 (Fig. 1, right). This is due to the fact that with 1850 samples there are on average only $1850(1-0.999) = 1850 \times 0.001 \sim 2$ samples in Fig. 1, right. In contrast, SS (due to successive conditional MCMC simulations) generates 1850 and 500 conditional samples in Fig. 1, left and right, respectively, giving enough information for an efficient estimation of the CDF.

Then, the 99.9th percentile of the performance function $Y(\boldsymbol{x})$ of the passive system is estimated by SS with 1850 samples (obtaining 1120.1 °C) and LHS with 1850 (obtaining 1095.3 °C) and 500,000 samples (obtaining 1118.9 °C). It can be seen that the estimate of the 99.9th percentile produced by SS with 1850 samples is very *accurate* and close to the reference one, i.e., the one computed by LHS with 500,000 samples: however, this result is obtained with a computational effort which is $500{,}000/1850 \approx 270$ times lower; on the contrary, the percentile identified by LHS with 1850 samples is much lower than the reference one.

Finally, to assess quantitatively the statistical properties and the *precision* of the 99.9th percentile estimates produced by SS with 1850 samples and LHS with 1850 samples, $S = 100$ independent runs have been carried out for each simulation method and the empirical 95% Confidence Intervals (CIs) of the 99.9th percentile estimates thereby obtained have been computed: the obtained CIs are [1068.9, 1183.0] and [1012.4, 1242.1] for SS and LHS, respectively. It can be seen that the width of the 95% CI produced by SS is about 2 times lower than that of LHS: thus, conversely, the precision of the estimate is 2 times higher.

As a final remark, it is worth noting that for SS (differently from LS) there does not seem to exist any indication that it is possible to reduce the number of samples (i.e., the number of T–H model code evaluations) to below a few hundreds. Actually, referring to the computational flow of SS described above, at least $N = 100$ samples have to be generated in *each* subset F_i, $i = 1, 2, \ldots, m$, to produce reliable estimates in the uncertainty propagation phase: thus, if high quantiles (e.g., the 99.9th or 99.99th percentiles) have to be estimated (which is often the case for passive safety systems), then an amount of about $N \times m = 100 \times 3 = 300$ or $N \times m = 100 \times 4 = 400$ samples have to be generated, respectively. As a consequence, if the T–H model requires many hours, or days, to perform a single evaluation, SS is not suitable.

5.2.2. Uncertainty propagation using bootstrapped Artificial Neural Networks

In those cases where the T–H model requires many hours, or days, to perform a single evaluation, the use of fast-running surrogate regression models instead of the long-running original T–H code becomes somewhat mandatory: because calculations with the surrogate model can be performed quickly, the problem of long simulation times is circumvented.

Here, the use of ANNs is recommended for this task. In extreme synthesis, ANNs are computing devices inspired by the function of the nerve cells in the brain (Bishop, 1995). They are composed of many parallel computing units (called *neurons* or *nodes*) arranged in different *layers* and interconnected by weighed connections (called *synapses*). Each of these computing units performs a few simple operations and communicates the results to its neighbouring units. From a mathematical viewpoint, ANNs consist of a set of nonlinear (e.g., sigmoidal) basis functions with adaptable parameters $\boldsymbol{w}^*$ that are adjusted by a process of *training* (on many different input/output data examples), i.e., an iterative process of regression error minimization (Rumelhart et al., 1986). ANNs have been demonstrated to be universal approximants of *continuous* nonlinear functions (under mild mathematical conditions) (Cybenko, 1989), i.e., in principle, an ANN model with a properly selected architecture can be a consistent estimator of any continuous nonlinear function, e.g., any nonlinear T–H code simulating the system of interest. Further details about ANN regression models are not reported here for brevity; the interested reader may refer to the cited references and the copious literature in the field. The particular type of ANN considered in this paper is the classical three-layered feed-forward ANN trained by the error back-propagation algorithm.

Notice that the recommendation of using ANN regression models is mainly based on (i) theoretical considerations about the (mathematically) demonstrated capability of ANN regression models of being *universal* approximants of continuous nonlinear functions (e.g., any nonlinear T–H code simulating the system of interest) (Cybenko, 1989) and (ii) the experience of the authors' in the use of ANN regression models for propagating the uncertainties through T–H model codes simulating passive safety systems (Pedroni et al., 2010; Zio et al., 2010): for example, in Pedroni et al. (2010), both the accuracy and precision of ANN regression models in estimating the percentiles of the temperature of the naturally circulating coolant in a passive decay heat removal system have been compared and shown to be superior to those of simple quadratic Response Surface (RS) regression models. Since no further comparisons with other types of regression models have been performed by the authors yet, no additional proofs of the superiority of ANNs with respect to other regression models can be provided at present, in general terms.

To evaluate the additional source of *model* uncertainty introduced by the ANN empirical regression model the use of an ensemble of ANN regression models, constructed on different data sets bootstrapped from the original one is recommended (Zio, 2006; Storlie et al., 2009). The bootstrap method is a distribution-free inference method which requires no prior knowledge about the distribution function of the underlying population (Efron and Thibshirani, 1993). The basic idea is to generate a sample from the observed data by sampling with replacement from the original data set (Efron and Thibshirani, 1993): each of these bootstrapped data sets is used to build a bootstrapped regression model which is used to calculate the quantity of interest (e.g., in this case of uncertainty propagation, the quantity of interest may be represented by the vector $\boldsymbol{y}$ of the outputs of the T–H model code, by the performance function of the passive system $Y(\boldsymbol{x})$ and by their percentiles). In this context, the bootstrap algorithm is used to quantify, in terms of *confidence intervals*, the model uncertainty associated to the estimates provided by the ANN regression models. Recall also that from the theory and practice of ensemble empirical models, it can be shown that the estimates given by bootstrapped ANN regression models are in general more accurate than the estimate of the best ANN regression model in the bootstrap ensemble of ANN regression models (Zio, 2006; Cadini et al., 2008).

In synthesis, the following steps must be undertaken to perform uncertainty propagation by means of bootstrapped ANNs (Zio, 2006; Storlie et al., 2009):

1. Generate a data set D_{train} of training input/output data examples by sampling a (possibly *reduced*) number N_{train} of independent input parameters values $\boldsymbol{x}_p$, $p = 1, 2, \ldots, N_{train}$, and calculating the corresponding set of N_{train} output vectors $\boldsymbol{y}_p = \boldsymbol{\mu}_{\boldsymbol{y}}(\boldsymbol{x}_p)$ through the mechanistic T–H system code.

2. Generate a set D_{val} of validation input/output data examples (different from D_{train}) by sampling a (possibly *reduced*) number N_{val} of independent input parameters values $\boldsymbol{x}_p$, $p = 1, 2, \ldots, N_{val}$, and calculating the corresponding set of N_{val} output vectors $\boldsymbol{y}_p = \boldsymbol{\mu}_{\boldsymbol{y}}(\boldsymbol{x}_p)$ through the mechanistic T–H system code.
3. Build an ANN regression model $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{w}^*)$ using the training and validation data sets D_{train} and D_{val}; in particular, the training data set D_{train} is used to calibrate the internal parameters $\boldsymbol{w}^*$ of the regression model, whereas the validation data set D_{val} is used to monitor the accuracy of the ANN model during the training procedure in order to avoid *overfitting* of the training data according to the so-called *early stopping* method. In practice, the RMSE is computed on D_{val} at different iterative stages of the training procedure: at the beginning of training, this value decreases as does the RMSE computed on the training set D_{train}; later in the training, if the ANN regression model starts overfitting the data, the RMSE calculated on the validation set D_{val} starts increasing and training must be stopped (Bishop, 1995).
4. Measure the accuracy of the constructed regression model constructed in step 3. by computing proper numerical figures (e.g., the commonly adopted coefficient of determination R^2 and RMSE) for each output y_l, $l = 1, 2, \ldots, n_o$, on a *new* data set $D_{test} = \{(\boldsymbol{x}_p, \boldsymbol{y}_p), p = 1, 2, \ldots, N_{test}\}$ of size N_{test}, purposely generated for *testing* the regression model built (Marrel et al., 2009), and thus different from those used for training and validation.
5. Use the regression model $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{w}^*)$, in place of the original T–H model code, to provide a point estimate $\hat{Q}$ of the quantity Q of interest (e.g., in this case of uncertainty propagation, the quantity Q may be represented by the vector $\boldsymbol{y}$ of the outputs of the T–H model code, by the performance function of the passive system $Y(\boldsymbol{x})$ and by their percentiles).
6. Build an ensemble of B (e.g., $B = 500$–1000) regression models $\{\boldsymbol{f}_b(\boldsymbol{x}, \boldsymbol{w}_b^*), b = 1, 2, \ldots, B\}$ on the basis of bootstrap data sets $D_{train,b} = \{(\boldsymbol{x}_{p,b}, \boldsymbol{y}_{p,b}), p = 1, 2, \ldots, N_{train}\}$, $b = 1, 2, \ldots, B$, generated by performing random sampling *with replacement* from the original training data set $D_{train} = \{(\boldsymbol{x}_p, \boldsymbol{y}_p), p = 1, 2, \ldots, N_{train}\}$.
7. Use each of the bootstrapped regression models $\boldsymbol{f}_b(\boldsymbol{x}, \boldsymbol{w}_b^*)$, $b = 1, 2, \ldots, B$, to calculate an estimate $\hat{Q}_b$, $b = 1, 2, \ldots, B$, for the quantity Q of interest: by so doing, a bootstrap-based *empirical* probability distribution for the quantity Q is produced which is the basis for the construction of the corresponding confidence intervals.
8. Calculate the so-called Bootstrap Bias Corrected (BBC) point estimate $\hat{Q}_{BBC}$ for Q (see Baxt and White, 1995 for details) and the corresponding two-sided BBC-$100 \times (1-\alpha)$% CI (using the bootstrap-based *empirical* probability distribution for the quantity Q obtained in step 7. above).

The complete and detailed bootstrap algorithm is not reported here for brevity; some technical details can be found in Efron and Thibshirani (1993), Zio (2006), Cadini et al. (2008), Secchi et al. (2008), Storlie et al. (2009), Pedroni et al. (2010) and Zio et al. (2010).

For completeness, we report some of the results obtained in a previous work by the authors (Pedroni et al., 2010), in which bootstrapped ANNs are used to propagate the uncertainties through the T–H model of Section 5.1 (Pagani et al., 2005); again, the performance of bootstrapped ANNs is compared to that of LHS.

Fig. 2, left shows the empirical CDF of the performance function $Y(\boldsymbol{x})$ of the passive decay heat removal system considered; in addition, Fig. 2, right focuses on the portion of CDF where the cumulative probability ranges between 0.95 and 1. The results obtained with $N_T = 500{,}000$ estimations from $B = 1000$ by bootstrapped ANNs (built on $N_{code} = N_{train} + N_{val} + N_{test} = 80 + 20 + 10 = 110$ input/output examples, i.e., T–H code runs) are shown in solid lines, whereas those produced by LHS with the *same* number of T–H code runs (i.e., $N_T = N_{code} = 110$) are shown in dashed lines. Notice that the comparison between these two approaches is fair because the number N_{code} of runs of the original T–H system model code (and thus the associated *overall computational effort*) is the same (i.e., $N_{code} = 110$); however, for LHS the *few* system model code runs are *directly* used to produce the CDF of interest, whereas for bootstrapped ANNs they are used to build the regression models, which are in turn employed to produce the CDF estimate. The dot-dashed lines correspond to the results obtained by LHS with $N_T = N_{code} = 500{,}000$ samples (i.e., T–H code runs): this number of samples is largely sufficient for efficiently estimating the CDF even where the cumulative probability ranges between 0.95 and 1: thus, the corresponding results are taken as *benchmarks*.

The bootstrapped ANNs are shown to be quite *reliable* and *accurate*, as the CDF produced is satisfactorily close to the reference one (i.e., the one produced by LHS with $N_T = N_{code} = 500{,}000$ samples) in all the probability ranges considered. Also, the bootstrapped ANN results are obtained at a much lower computational effort: actually, the number N_{code} of T–H code runs (i.e., 110) is about 4500 times lower than that of the reference case (i.e., 500,000). The overall CPU time required by the use of bootstrapped ANNs (i.e., on average 2.22 h) is about 180 times lower than that required by the use of the original T–H model code (i.e., on average 409 h).

Further, it can be seen that the bootstrapped ANNs built on $N_{code} = N_{train} + N_{val} + N_{test} = 80 + 20 + 10 = 110$ input/output examples (i.e., T–H code runs) outperform LHS with the same number $N_{code} = 110$ of T–H code simulations: actually, LHS is not able to produce accurate results, in particular for values of the cumulative probability very close to 1 (Fig. 2, right).

The two approaches are further compared in the estimation of the 95th percentile of the performance function $Y(\boldsymbol{x})$ of the passive decay heat removal system. The BBC point estimate of the 95th percentile of the performance function $Y(\boldsymbol{x})$ obtained with $N_T = 500{,}000$ estimations from $B = 1000$ bootstrapped ANNs and with $N_T = 110$ and 500,000 estimations from LHS are 802.5 °C, 824.1 °C and 794.2 °C, respectively. It can be seen that the estimate produced by the bootstrapped ANNs is quite close to the *reference* one, i.e., the one obtained by LHS with 500,000 samples: the corresponding percentage Relative Absolute Error (RAE) is 1.04%; on the contrary, the percentile identified by LHS with $N_T = 110$ samples is considerably larger: the corresponding percentage RAE is 3.74%. It can be seen that the percentage RAE produced by the bootstrapped ANNs is 3.6 times lower than that of LHS with $N_T = 110$ samples: thus, conversely, the *accuracy* of the estimate is 3.6 times higher.

Finally, to assess quantitatively the statistical properties and the *precision* of the 95th percentile estimates produced by the methods considered, the 95% CI associated to the estimates are evaluated. In particular, $S = 1000$ independent runs of LHS with $N_T = N_{code} = 110$ samples are carried out and the *empirical* 95% CI of the 95th percentile estimate thereby obtained has been computed: it turns out to be [785.6, 868.2]; on the contrary, the BBC 95% CI is produced by $B = 1000$ bootstrapped ANN regression models constructed on $N_{code} = 110$ data examples according to steps 1.–8. above: it turns out to be [777.06, 818.92]. It can be seen that the width of the CI produced by bootstrapped ANNs is about 2 times lower than that of LHS: thus, conversely, the precision of the estimate is 2 times higher.

5.3. Sensitivity analysis

For safety-critical systems, like nuclear passive systems, the task of sensitivity analysis is fundamental for reliability/failure probability assessment and safety decision-making and assurance (Helton and Sallaberry, 2009). In particular, in the functional failure analysis of a T–H passive system, sensitivity analysis can be a useful tool for identifying the uncertain parameters (i.e., the uncertain inputs to the T–H code) that contribute most to the variability

of the model outputs (i.e., the coolant outlet temperatures): this information is important for the identification of those parameter and hypothesis uncertainties that are most relevant in determining system failure (Saltelli et al., 2008; Volkova et al., 2008; Marrel et al., 2009).

In general, the sensitivity analysis outcomes provide two important insights. On the one side, the analyst is able to identify those parameters/variables whose epistemic uncertainty plays a major role in determining the functional failure of the T–H passive system: consequently, his/her efforts can be focused on increasing the state-of-knowledge on these important parameters/variables and the related physical phenomena (for example, by the collection of experimental data one may achieve an improvement in the state-of-knowledge on the correlations used to model the heat transfer process in natural convection and a corresponding reduction in the uncertainty); on the opposite side, the analyst can identify those parameters/variables that are not important and may be excluded from the modeling and analysis.

The options recommended for performing sensitivity analysis are the same as those proposed for uncertainty analysis (Section 5.2), as explained below.

5.3.1. Sensitivity analysis using Subset Simulation

The Markov chain samples generated by SS can be used not only for estimating the conditional probabilities but also to infer the probable scenarios that will occur in the case of failure (Au, 2005). Intuitively, from the comparison of the probability density function $q(x_j|F)$ of the uncertain parameter $x_j, j = 1, 2, \ldots, n_i$, conditional to the occurrence of failure F, with the unconditional probability density function $q(x_j)$, an indication can be obtained on how important is the parameter x_j in affecting the system failure. Formally, for any given value of x_j the Bayes' theorem reads,

$$P(F|x_j) = \frac{q(x_j|F)}{q(x_j)} P(F), \quad j = 1, 2, \ldots, n_i \tag{12}$$

so that $P(F|x_j)$ is insensitive to x_j when $q(x_j|F) \sim q(x_j)$, i.e., when the conditional probability density function $q(x_j|F)$ is similar in shape to the PDF $q(x_j)$ (Au and Beck, 2003b; Au, 2005; Au et al., 2007). The effectiveness of this approach for sensitivity analysis has been demonstrated by a number of studies conducted in the field of structural reliability: for example, in Au and Beck (2003a,b) and Au (2005), the approach has been effectively used to address a 1500-dimensional problem concerning a steel frame subject to stochastic ground motion; in Au et al. (2007) the method has been applied to perform a compartment fire risk analysis where seven uncertain parameters were considered, whereas in Zio and Pedroni (2009b) it has been applied to perform the sensitivity analysis of the model of Section 5.1.

In this latter work, the sensitivity of the passive system performance to the $n_i = 9$ uncertain input parameters has been studied by examining the change of the sample distributions $q(x_j|F_i)$, $j = 1, 2, \ldots, n_i$, $i = 1, 2, \ldots, m$, at different conditional levels F_i, $i = 1, 2, \ldots, m$. The histograms of the conditional samples of two of the nine uncertain parameters (i.e., x_2, the pressure level established in the guard containment after the Loss of Coolant Accident (LOCA), and x_8, the friction factor in mixed convection) at different conditional levels for a single SS run are shown in Fig. 3, left. It can be seen that the performance of the passive system is strongly sensitive to the pressure level established in the guard containment after the LOCA, as indicated by the significant leftward shift of its empirical conditional distribution (histograms) from the unconditional one (solid lines). A slight sensitivity of the passive system performance is also observed with respect to the correlation errors in the friction factor (rightward shift) in mixed convection.

The information contained in the empirical conditional distributions $q(x_j|F_i)$, $j = 1, 2, \ldots, n_i$, $i = 1, 2, \ldots, m$, can then be used to *refine* the sensitivity information by obtaining the distribution of the system failure probability conditional on the values of the individual uncertain input parameters, i.e., $P(F|x_j)$, according to (12) (Fig. 3, right): this information is relevant because it quantifies how the failure probability $P(F)$ of the passive system would change if the value of the uncertain parameter x_j were set to a given value (e.g., if its epistemic uncertainty were reduced).

Note that SS presents the advantage over other standard techniques of sensitivity analysis, of being directly "embedded" in the computation of the failure probability: the SS algorithm produces the empirical conditional distributions of Fig. 3 *during the simulation* that is performed to compute the functional failure probability of the passive system. In other words, *while* estimating the functional failure probability of the system, sensitivity analysis results are produced that can be readily visualized for identification and ranking of the most important variables.

5.3.2. Sensitivity analysis using bootstrapped Artificial Neural Networks

Bootstrapped ANNs are used to replace the original T–H code in the *multiple* (e.g., many thousands) system performance evaluations (for different combinations of system inputs) required by sensitivity analysis; thus, in principle, bootstrapped ANNs could be used in the development of any of the sensitivity analysis methods available in the open literature.

Here we recommend the use of bootstrapped ANNs for computing first- and total-order Sobol sensitivity indices (Sobol, 1993) for the vector $\boldsymbol{y}$ of the outputs of the T–H code and for the passive system performance function $Y(\boldsymbol{x})$: see Zio et al. (2010) for a preliminary analysis of this kind.

By definition, the first-order Sobol sensitivity index S_j^l, $j = 1, 2, \ldots, n_i$, $l = 1, 2, \ldots, n_o$, quantifies the proportion of the variance of the output y_l, $l = 1, 2, \ldots, n_o$, that can be attributed to the variance of the uncertain input variable x_j *alone*, i.e., *without* taking into account *interactions* with other input variables; on the contrary, the total-order Sobol sensitivity index S_{Tj}^l, $j = 1, 2, \ldots, n_i$, $l = 1, 2, \ldots, n_o$, quantifies the proportion of the variance of the output y_l, $l = 1, 2, \ldots, n_o$, that can be attributed to the variance of the uncertain input variable x_j taking into account the *interactions* (of *all* the *orders*) with all the other input variables. A thorough description of these sensitivity measures goes beyond the scope of this work: mathematical details can be found in Saltelli (2002a,b) and Saltelli et al. (2008).

As pointed out in Saltelli (2002a), the sensitivity indices S_j^l and S_{Tj}^l have the advantage of being *global* because the effect of the *entire* distribution of the parameter whose uncertainty importance is evaluated, is considered; moreover, this sensitivity index is also "model free" because its computation is independent from assumptions about the model form, such as linearity, additivity and so on. The drawback of this approach relies in the computational burden associated to its calculation: actually, thousands or millions of system model evaluations are frequently required for the evaluation of Sobol indices through Monte Carlo-based techniques (Saltelli, 2002a; Saltelli et al., 2008).

For completeness, we complete the results obtained in a previous work by the authors (Zio et al., 2010) (in which bootstrapped ANNs were applied for computing first-order Sobol indices for one of the outputs of the model of Section 5.1) by computing first- and total-order Sobol indices S_j^Y and S_{Tj}^Y for the performance function $Y(\boldsymbol{x})$ of the model of the T–H passive system of Section 5.1. The algorithm proposed by Saltelli (2002a) has been implemented to obtain the "true" (i.e., reference) values of the first- and total-order Sobol

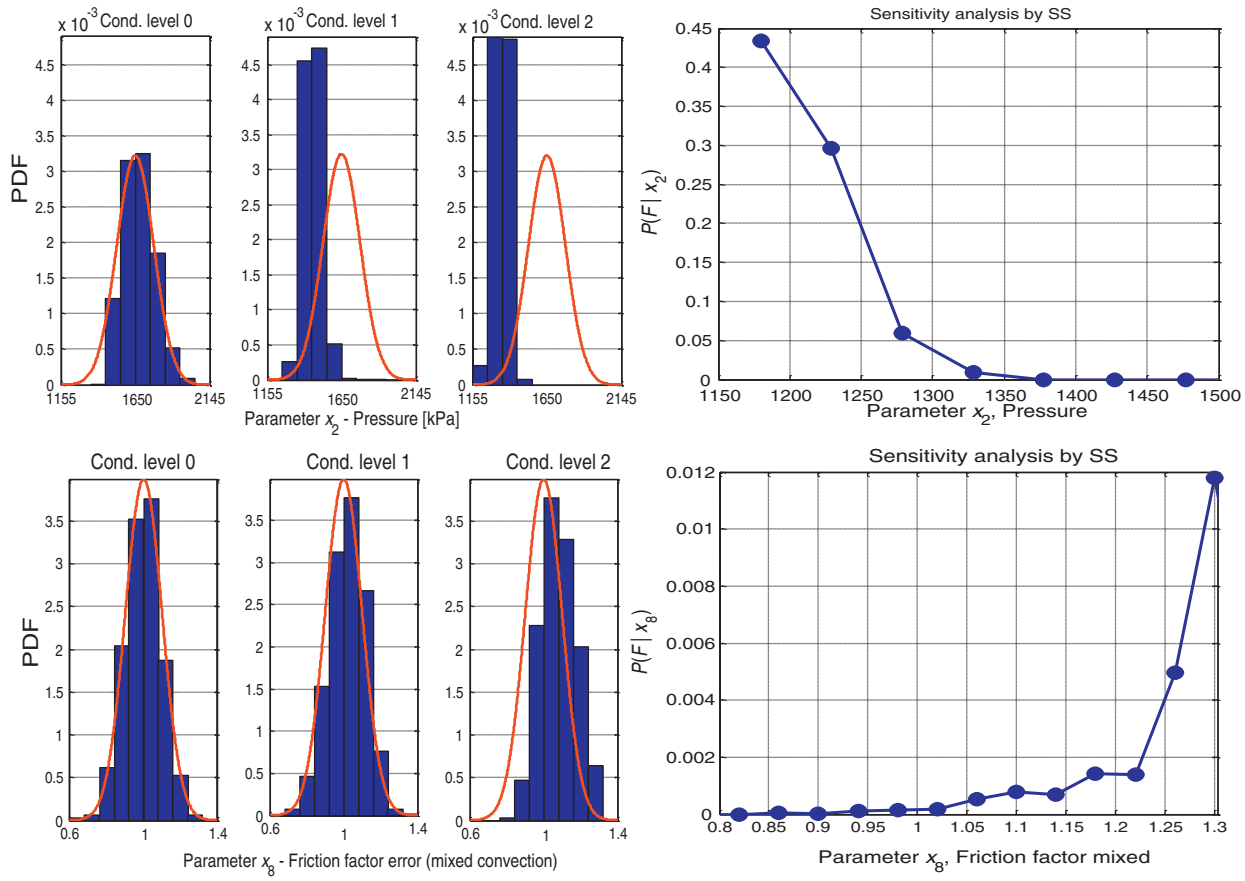


Fig. 3. Sensitivity analysis by SS. Left: empirical conditional distributions of uncertain input parameters x_2 and x_8 at different conditional levels (histograms) compared to their unconditional distributions (solid lines); right: distribution of the system failure probability conditional on the values of the individual uncertain input parameters x_2 and x_8, i.e., $P(F|x_2)$ and $P(F|x_8)$.

sensitivity indices S_j^Y and S_{Tj}^Y for the input variables x_j, $j = 1, 2, \ldots, 9$: these values obtained with $N_T = 110{,}000$ runs of the original T–H model code are reported for reference in Table 5 (in parentheses).

Table 5 reports also the BBC point estimates $\hat{S}_{j,BBC}^Y$ and $\hat{S}_{Tj,BBC}^Y$ for S_j^Y and S_{Tj}^Y, $j = 1, 2, \ldots, 9$, obtained with $N_T = 110{,}000$ estimations from $B = 1000$ bootstrapped ANN models built on $N_{code} = N_{train} + N_{val} + N_{test} = 80 + 20 + 10 = 110$ input/output examples, i.e., T–H code runs; the table also shows the corresponding BBC-95% CIs: the information conveyed by these intervals is important when few data are used to train the bootstrapped ANNs and the consequent confidence of the analyst on the Sobol index point estimates $\hat{S}_{j,BBC}^Y$ and $\hat{S}_{Tj,BBC}^Y$ is poor, like in the present case.

It can be seen that bootstrapped ANNs are quite *accurate* because the BBC point estimates produced are satisfactorily close to the reference values; moreover, ANNs are sufficiently *precise* since the BBC 95% CIs are quite *narrow* around the reference values.

Finally, notice that the computational cost associated to the use of bootstrapped ANNs is much lower than that required by the use of the original T–H code: actually, the computational times associated to both analyses have been of 2.12 h and 92 h, respectively, on a Pentium 4 CPU 3.00 GHz.

Table 5
Bootstrap Bias Corrected (BBC) point estimates $\hat{S}_{j,BBC}^Y$ and $\hat{S}_{Tj,BBC}^Y$, $j = 1, 2, \ldots, 9$, and BBC-95% Confidence Intervals (CIs) of the first- and total-order Sobol sensitivity indices S_j^Y and S_{Tj}^Y, $j = 1, 2, \ldots, 9$, calculated he performance function $Y(\boldsymbol{x})$ of the model of the T–H passive system in Pagani et al. (2005).

Parameters	Sensitivity analysis using bootstrapped ANNs			
	S_i^Y		S_{Ti}^Y	
	$\hat{S}_{j,BBC}^Y$ ("reference")	BBC-95% CI	$\hat{S}_{Tj,BBC}^Y$ ("reference")	BBC-95% CI
x_1	7.6774×10^{-3} (8.6372×10^{-3})	[4.751×10^{-4}, 8.971×10^{-3}]	0.0113 (0.0121)	[9.001×10^{-3}, 0.0195]
x_2	0.7879 (0.7928)	[0.7792, 0.8158]	0.8259 (0.8391)	[0.8188, 0.8553]
x_3	0.0496 (0.0516)	[0.0331, 0.0510]	0.0546 (0.0434)	[0.0391, 0.0570]
x_4	3.3248×10^{-6} (8.4218×10^{-6})	[$0.8.317 \times 10^{-5}$]	2.226×10^{-3} (3.0575×10^{-3})	[3.231×10^{-4}, 4.385×10^{-3}]
x_5	0.0651 (0.0522)	[0.0583, 0.0767]	0.0711 (0.0833)	[0.0655, 0.0809]
x_6	1.2317×10^{-4} (6.5814×10^{-5})	[$0.3.718 \times 10^{-4}$]	2.2169×10^{-3} (3.1948×10^{-3})	[3.179×10^{-4}, 4.862×10^{-3}]
x_7	2.4542×10^{-5} (6.0669×10^{-5})	[$0.4.239 \times 10^{-4}$]	2.2013×10^{-3} (3.0618×10^{-3})	[3.447×10^{-4}, 4.621×10^{-3}]
x_8	0.0527 (0.0522)	[0.0500, 0.0677]	0.0827 (0.0832)	[0.0718, 0.0955]
x_9	1.5848×10^{-6} (5.9493×10^{-6})	[$0.8.168 \times 10^{-5}$]	2.1968×10^{-3} (3.0531×10^{-3})	[3.455×10^{-4}, 4.333×10^{-3}]

6. Conclusions

The assessment of the reliability of T–H passive systems is a crucial issue to be resolved for their extensive use in future nuclear power plants. The reliance of T–H passive systems on inherent physical principles makes their reliability evaluation quite difficult to accomplish, if compared to classical system reliability analysis, due to the lack of data which makes current knowledge of passive system operation somewhat poor, thus introducing large *uncertainties* in the analysis. These uncertainties are both of aleatory and epistemic nature and are mainly due to poor understanding and imprecise modeling of the phenomena affecting the T–H performance of the system and of the relative physical correlations, environmental and boundary conditions used.

These issues may in principle be detrimental for the public acceptance of future reactor designs, which conversely are expected to offer an overall, guaranteed level of safety higher than the one of the currently operating nuclear fleet, especially thanks to the adoption of passive systems.

Thus, there is a strong need for the development and demonstration of consistent methodologies and approaches for T–H passive systems reliability assessment.

As a further step forward in this direction, in this paper the computational issues associated with assessing the reliability of T–H passive systems have been considered. The copious use of expert judgment and subjective assumptions during the assessment process leads to the need of propagating the associated uncertainties by simulating several times the system response under different working conditions: this can be done by Monte Carlo sampling the uncertainties in the system model and parameters, and simulating the corresponding passive system response with a mechanistic T–H computer code. However, this approach requires considerable computational efforts. The reason is twofold. First, a large number of Monte Carlo-sampled T–H model evaluations must generally be carried out for an accurate estimation of the functional failure probability. Since the number of simulations required to obtain a given accuracy depends on the magnitude of the failure probability to be estimated, with the computational burden increasing with decreasing functional failure probability, this poses a significant challenge for the typically quite small (e.g., less than 10^{-4}) probabilities of functional failure of T–H passive safety systems. Second, long calculations (several hours) are typically necessary for each run of the detailed, mechanistic T–H code (one code run is required for each sample of values drawn from the uncertainty distributions).

These computational issues can be tackled in two different ways. From one side, efficient Monte Carlo Simulation techniques can be employed to perform robust estimations with a limited number of input samples; from the other side, fast-running, surrogate regression models (also called response surfaces or meta-models) can be used to replace the long-running T–H model code.

Different approaches have been considered and compared with reference to a case study of literature involving the natural convection cooling in a GFR after a LOCA (Pagani et al., 2005).

On the basis of the results obtained in the present and previous works by the authors (Zio and Pedroni, 2009a,b,c, 2010; Pedroni et al., 2010; Zio et al., 2010), the following guidelines and recommendations can be drawn:

- If the interest is only in an accurate and precise estimation of the (typically small) functional failure probability of the T–H passive system (modeled by a *long-running*, *nonlinear* and *non-monotonous* T–H code), then the following approach is recommended (Section 5.1):
  a. build an Artificial Neural Network (ANN) regression model using a *sequential*, *two-step* training algorithm on a *reduced* number of examples (e.g., around one hundred) of the input/output nonlinear relationships underlying the original system model code;
  b. use the ANN model as a fast-running surrogate of the original system model code in the determination of the LS important direction; the technique recommended for this is that based on the *minimization* of the variance of the LS failure probability estimator by means of Genetic Algorithms: the motivation is that since it relies directly on the definition of the *optimal* LS important direction, it produces more accurate and precise failure probability estimates than those provided by the other techniques proposed in the literature;
  c. estimate the functional failure probability of the T–H passive system by means of Line Sampling with a *small* number of samples (e.g., few tens); the accuracy and precision of the estimates can be enhanced by combining Line Sampling with Latin Hypercube Sampling.

  It is worth remarking once more that the LS technique allows *only* the calculation of the failure probability of the passive system, whereas it does not allow a *complete* uncertainty propagation.
- If the analyst is interested also in the uncertainty propagation (i.e., determination of the PDFs, CDFs, percentiles of the T–H code outputs of interest and so on) and sensitivity analysis, two options are recommended:
  1. the SS method offers a feasible means because it generates a *large* amount of conditional (failure) samples by *sequential* MCMC simulations developed in different *subsets* of the uncertain input space. This allows producing the PDFs and CDFs of *all* the T–H code outputs of interest (e.g., peak cladding temperatures, pressures, mass flow rates and so on) in a *single* simulation run. Moreover, the conditional samples distributions in different *subsets* of the uncertain input space can be used to study the sensitivity of the passive system performance to the uncertain system input parameters: the informative measure of the importance of a given parameter in determining the failure of the system is the deviation of its conditional distribution from the unconditional one.

     On the other hand, differently from the LS method, there does not seem to exist any indication that it is possible to reduce the number of samples (i.e., the number of T–H model code evaluations) to below a few hundreds. Actually, at least one hundred samples have to be generated in *each* subset to produce reliable failure probability estimates: thus, if the failure probabilities to be estimated are 10^{-4} or 10^{-5} (which is often the case for passive safety systems), then an amount of 400 or 500 samples have to be generated, respectively. As a consequence, if the T–H model requires many hours, or days, to perform a single evaluation, SS is not suitable; on the other hand, if the T–H model is sufficiently simple and requires *seconds or minutes* to run, SS may represent the optimal choice.
  2. in those (realistic) cases where the T–H model requires many hours, or days, to perform a single evaluation, the use of fast-running surrogate regression models (e.g., ANNs, quadratic RSs, . . .) instead of the long-running original T–H code seems mandatory. The following procedure is recommended:
     a. run the T–H system model code a predetermined, *reduced* number of times (e.g., 50–100) for specified values of the uncertain input variables;
     b. collect the corresponding values of the output of interest;
     c. employ statistical techniques for calibrating/adapting the internal *parameters/coefficients* of the response surface of the regression model in order to fit the input/output data generated in the previous steps;
     d. use the empirical regression model built at step c. to estimate the quantities of interest: in this paper, the estimation of (i) the CDF of the passive system performance function, (ii)

its 95th and 99.9th percentiles and (iii) first- and total-order Sobol sensitivity indices has been illustrated;

e. use the bootstrap procedure to quantify, in terms of confidence intervals, the uncertainties associated to the estimates provided by the empirical regression models.

It is worth pointing out that the selection of a surrogate regression model suitable to replace the complex, nonlinear T–H code in the uncertainty propagation process is quite a difficult task: actually, such selection is heavily dependent on the particular application at hand, so that no *general* rules are available to this aim.

In the present paper, ANN regression models have been recommended on the basis of (i) theoretical considerations about the (mathematically) demonstrated capability of ANN regression models of being *universal* approximants of continuous nonlinear functions (e.g., any nonlinear T–H code simulating the system of interest) (Cybenko, 1989) and (ii) the experience of the authors in the use of ANN regression models for propagating the uncertainties through T–H model codes simulating passive safety systems (Pedroni et al., 2010; Zio et al., 2010). However, since no detailed and systematic comparisons with other types of regression models (except for quadratic response surfaces (Pedroni et al., 2010) have been performed by the authors yet, no additional proofs of the superiority of ANNs with respect to other regression models can be provided at present. Future research will be devoted to address this issue, although it is arguably optimistic to think that a general statement in this direction can be reached.

Finally, a general remark is in order to drive the reader towards a correct interpretation of the numerical results obtained and of the recommendations drawn in the present paper. Actually, one may interpret that the failure probabilities and sensitivity indices computed by means of the methodologies described and recommended throughout the paper are *the* failure probabilities and sensitivity indices associated to the "*real*" T–H passive system under analysis (i.e., those quantities that would characterize the behavior of the T–H passive system in its operation during a *real* accidental transient). However, in order for this to be true, the T–H code employed in the analyses would need to be flawless and comprehensive of *all* the relevant failure modes of the real T–H passive system, *all* aleatory uncertainties would need to be modeled perfectly, and *all* epistemic uncertainties would need to be well characterized. This is obviously not so and it seems in order to acknowledge that the computational methods described and recommended throughout the paper can "only" do as much, driving the T–H code with its limitations (even if very detailed and extremely demanding to run). In other words, the paper has addressed the quantification of passive system functional reliability "only" from the computational viewpoint, i.e., to the extent that the relevant failure modes are captured in the T–H model code being driven, and to the extent that the input uncertainty distributions are appropriate. Even after consistency checks are run and statistical confidence bounds are established on the results, issues may remain concerning the possibility of "extending" the results obtained in the analyses to the "*actual*" behavior of the "*real*" T–H passive system during an accidental transient, because of the model incomplete representation of reality.

References

Ahn, S.K., Kim, I.S., Oh, K.M., 2010. Deterministic and risk-informed approaches for safety analysis of advanced reactors: Part I. Deterministic approaches. Reliability Engineering and System Safety 95, 451–458.

Apostolakis, G.E., 1990. The concept of probability in safety assessment of technological systems. Science 250, 1359.

Apostolakis, G.E., 1994. A commentary on model uncertainty. In: Mosleh, A., Siu, N., Smidts, C., Lui, C. (Eds.), Proc. Workshop on Model Uncertainty: Its Characterization and Quantification. Center for Reliability Engineering, University of Maryland, College Park, Maryland, pp. 13–22, also published as NUREG/CP-0138, U.S. Nuclear Regulatory Commission, Washington, DC.

Apostolakis, G.E., 1999. The distinction between aleatory and epistemic uncertainties is important: an example from the inclusion of ageing effects into PSA. In: Proc. Int. Topl. Mtg. Probabilistic Safety Assessment (PSA '99), Washington, DC, August 22–26, 1999. American Nuclear Society, La Grange Park, Illinois, pp. 135–142.

Arul, A.J., Iyer, N.K., Velusamy, K., 2009. Adjoint operator approach to functional reliability analysis of passive fluid dynamical systems. Reliability Engineering and System Safety 94, 1917–1926.

Arul, A.J., Kannan Iyer, N., Velusamy, K., 2010. Efficient reliability estimate of passive thermal hydraulic safety system with automatic differentiation. Nuclear Engineering and Design, doi:10.1016/j.nucengdes.2010.05.012.

Au, S.K., 2004. Probabilistic failure analysis by importance sampling Markov chain simulation. Journal of Engineering Mechanics 130 (3), 303–311.

Au, S.K., 2005. Reliability-based design sensitivity by efficient simulation. Computers and Structures 83, 1048–1061.

Au, S.K., 2007. Augmented approximate solutions for consistent reliability analysis. Probabilistic Engineering Mechanics 22, 77–87.

Au, S.K., Beck, J.L., 2001. Estimation of small failure probabilities in high dimensions by subset simulation. Probabilistic Engineering Mechanics 16 (4), 263–277.

Au, S.K., Beck, J.L., 2003a. Importance sampling in high dimensions. Structural Safety 25 (2), 139–163.

Au, S.K., Beck, J.L., 2003b. Subset Simulation and its application to seismic risk based on dynamic analysis. Journal of Engineering Mechanics 129 (8), 1–17.

Au, S.K., Wang, Z.H., Lo, S.M., 2007. Compartment fire risk analysis by advanced Monte Carlo simulation. Engineering Structures 29 (9), 2381–2390.

Aumeier, S.E., 1994. Probabilistic techniques for multi-component system diagnostics and surveillance. Ph.D. dissertation, University of Michigan, Ann Arbor, MI (USA).

Aumeier, S.E., Lee, J.C., 1993. A Monte Carlo technique for system diagnostics, monitoring, and surveillance. Transactions of the American Nuclear Society 69, 235–236.

Aumeier, S.E., Lee, J.C., 1994. Probabilistic system diagnostics and surveillance. In: Proc. ARS'94 – Intl. Topical Meeting on Advanced Reactor Safety, Pittsburgh (PA), April 17–21, 1994.

Aumeier, S.E., Lee, J.C., Akcasu, A.Z., 1995. Probabilistic techniques using Monte Carlo Sampling for multi-component system diagnostics. In: Proc. International conference on mathematics and computations, reactor physics, and environmental analyses, Portland, OR (USA), 30 April–4 May, 1995.

Aumeier, S.E., Alpay, B., Lee, J.C., 2006. Probabilistic techniques for diagnosis of multiple component degradations. Nuclear Science and Engineering 153, 101–123.

Aybar, H.S., Aldemir, T., 1999. Dynamic probabilistic reliability and safety assessment: an application to IS-BWR. In: Proceedings of the Seventh International Conference on Nuclear Engineering, Tokio, Japan.

Bassi, C., Marquès, M., 2008. Reliability assessment of 2400 MWth gas-cooled fast reactor natural circulation decay heat removal in pressurized situations. Science and Technology of Nuclear Installations, Special Issue "Natural Circulation in Nuclear Reactor Systems", Hindawi Publishing Corporation, Paper 87376.

Baxt, W.G., White, H., 1995. Bootstrapping confidence intervals for clinic input variable effects in a network trained to identify the presence of acute myocardial infarction. Neural Computation 7, 624–638.

Bishop, C.M., 1995. Neural Networks for Pattern Recognition. Oxford University Press.

Bucher, C., Most, T., 2008. A comparison of approximate response function in structural reliability analysis. Probabilistic Engineering Mechanics 23, 154–163.

Burgazzi, L., 2002. Passive system reliability analysis: a study on the isolation condenser. Nuclear Technology 139 (July), 3–9.

Burgazzi, L., 2003. Reliability evaluation of passive systems through functional reliability assessment. Nuclear Technology 144, 145.

Burgazzi, L., 2004. Evaluation of uncertainties related to passive systems performance. Nuclear Engineering and Design 230, 93–106.

Burgazzi, L., 2006. Failure mode and effect analysis application for the safety and reliability analysis of a thermal–hydraulic passive system. Nuclear Technology 146, 150–158.

Burgazzi, L., 2007a. Addressing the uncertainties related to passive system reliability. Progress in Nuclear Energy 49, 93–102.

Burgazzi, L., 2007b. State of the art in reliability of thermal–hydraulic passive systems. Reliability Engineering and System Safety 92, 671–675.

Burgazzi, L., 2007c. Thermal–hydraulic passive system reliability-based design approach. Reliability Engineering and System Safety 92 (9), 1250–1257.

Burgazzi, L., 2008. About time-variant reliability analysis with reference to passive systems assessment. Reliability Engineering and System Safety 93 (11), 1682–1688.

Burgazzi, L., 2009. Evaluation of the dependencies related to passive system failure. Nuclear Engineering and Design 239 (12), 3048–3053.

Cacuci, D.G., Ionescu-Bujor, M., 2004. A comparative review of sensitivity and uncertainty analysis of large scale systems: II. Statistical methods. Nuclear Science and Engineering 147, 204–217.

Cadini, F., Zio, E., Kopustinskas, V., Urbonas, R., 2008. An empirical model based bootstrapped neural networks for computing the maximum fuel cladding temperature in a RBMK-1500 nuclear reactor accident. Nuclear Engineering and Design 238, 2165–2172.

Cardoso, J.B., De Almeida, J.R., Dias, J.M., Coelho, P.G., 2008. Structural reliability analysis using Monte Carlo simulation and neural networks. Advances in Engineering Software 39, 505–513.
Cheng, J., Li, Q.S., Xiao, R.C., 2008. A new artificial neural network-based response surface method for structural reliability analysis. Probabilistic Engineering Mechanics 23, 51–63.
Ching, J., Beck, J.L., Au, S.K., 2005. Hybrid subset simulation method for reliability estimation of dynamical systems subject to stochastic excitation. Probabilistic Engineering Mechanics 20, 199–214.
Chung, Y.J., Lee, S.W., Kim, S.H., Kim, K.K., 2008. Passive cooldown performance of a 65 MW integral reactor 238, 1681–1689.
Cybenko, G., 1989. Approximation by superpositions of a sigmoidal function. Mathematics of Control Signals Systems 2, 303–314.
D'Auria, F., Bianchi, F., Burgazzi, L., Ricotti, M.E., 2002. The REPAS study: reliability evaluation of passive safety systems. In: Proceedings of the 10th International Conference on Nuclear Engineering ICONE 10-22414, Arlington, VA, USA, April 14–18.
Deng, J., 2006. Structural reliability analysis for implicit performance function using radial basis functions. International Journal of Solids and Structures 43, 3255–3291.
Efron, B., Thibshirani, R.J., 1993. An Introduction to the Bootstrap. Monographs on Statistics and Applied Probability 57. Chapman and Hall, New York.
Fong, C.J., Apostolakis, G.E., Langewish, D.R., Hejzlar, P., Todreas, N.E., Driscoll, M.J., 2009. Reliability analysis of a passive cooling system using a response surface with an application to the flexible conversion ratio reactor. Nuclear Engineering and Design 239 (12), 2660–2671.
Gavin, H.P., Yau, S.C., 2008. High-order limit state functions in the response surface method for structural reliability analysis. Structural Safety 30, 162–179.
Guba, A., Makai, M., Pal, L., 2003. Statistical aspects of best estimate method-I. Reliability Engineering and System Safety 80, 217–232.
Han, S.J., Yang, J.E., 2010. A quantitative evaluation of reliability of passive systems within probabilistic safety assessment framework for VHTR. Annals of Nuclear Energy 37, 345–358.
Helton, J.C., 1998. Uncertainty and Sensitivity Analysis Results Obtained in the 1996 Performance Assessment for the Waste Isolation Power Plant, SAND98-0365. Sandia National Laboratories.
Helton, J., Oberkampf, W., 2004. Alternative representations of epistemic uncertainties. Reliability Engineering and System Safety 85 (Special Issue).
Helton, J.C., Davis, F.J., 2003. Latin hypercube sampling and the propagation of uncertainty in analyses of complex systems. Reliability Engineering and System Safety 81, 23–69.
Helton, J.C., Davis, F.J., Johnson, J.D., 2005. A comparison of uncertainty and sensitivity analysis results obtained with random and Latin hypercube sampling. Reliability Engineering and System Safety 89 (3), 305–330.
Helton, J.C., Johnson, J.D., Sallaberry, C.J., Storlie, C.B., 2006. Survey on sampling-based methods for uncertainty and sensitivity analysis. Reliability Engineering and System Safety 91, 1175–1209.
Helton, J.C., Sallaberry, C., 2009. Computational implementation of sampling-based approaches to the calculation of expected dose in performance assessments for the proposed high-level radioactive waste repository at Yucca Mountain, Nevada. Reliability Engineering and System Safety 94, 699–721.
Hofer, E., Kloos, M., Krzykacz-Hausmann, B., Peschke, J., Woltereck, M., 2002. An approximate epistemic uncertainty analysis approach in the presence of epistemic and aleatory uncertainties. Reliability Engineering and System Safety 77, 229–238.
Huang, B., Du, X., 2006. A robust design method using variable transformation and Gauss-Hermite integration. International Journal for Numerical Methods in Engineering 66, 1841–1858.
Hurtado, J.E., 2007. Filtered importance sampling with support vector margin: a powerful method for structural reliability analysis. Structural Safety 29, 2–15.
IAEA, 1991. Safety Related Terms for Advanced Nuclear Plant. IAEA TECDOC-626.
Jafari, J., D'Auria, F., Kazeminejad, H., Davilu, H., 2003. Reliability evaluation of a natural circulation system. Nuclear Engineering and Design 224, 79–104.
Juhn, P.E., Kupitz, J., Cleveland, J., Cho, B., Lyon, R.B., 2000. IAEA activities on passive safety systems and overview of international development. Nuclear Engineering and Design 201, 41–59.
Kalos, M.H., Whitlock, P.A., 1986. Monte Carlo Methods, vol. 1: basics. Wiley-Interscience, New York, NY, USA.
Katafygiotis, L., Cheung, S.H., 2005. A two-stage subset simulation-based approach for calculating the reliability of inelastic structural systems subjected to Gaussian random excitations. Computer Methods in Applied Mechanics and Engineering 194, 1581–1595.
Katafygiotis, L., Cheung, S.H., 2007. Application of spherical subset simulation method and auxiliary domain method on a benchmark reliability study. Structural Safety 29, 194–207.
Kim, I.S., Ahn, S.K., Oh, K.M., 2010. Deterministic and risk-informed approaches for safety analysis of advanced reactors: Part II. Risk-informed approaches. Reliability Engineering and System Safety 95, 459–468.
Konak, A., Coit, D.W., Smith, A.E., 2006. Multi-objective optimization using genetic algorithms: a tutorial. Reliability Engineering and System Safety 91 (9), 992–1007.
Koutsourelakis, P.S., Pradlwarter, H.J., Schueller, 2004. Reliability of structures in high dimensions: Part I. Algorithms and application. Probabilistic Engineering Mechanics 19, 409–417.
Krzykacz-Hausmann, B., 2006. An approximate sensitivity analysis of results from complex computer models in the presence of epistemic and aleatory uncertainties. Reliability Engineering and System Safety 91, 1210–1218.
Lee, J.C., Aumeier, S.E., Patton, B.W., Rank, P.J., 1993. Simulation-based diagnostics and control for nuclear power plants. DOE/ER-75712-1, Progress Report for the Period April 15, 1992–April 14, 1993.
Lee, J.C., Aumeier, S.E., Patton, B.W., Rank, P.J., 1994. Simulation-based diagnostics and control for nuclear power plants. DOE/ER-75712-2, Progress Report for the Period April 15, 1993–April 14, 1994.
Lee, J.C., Aumeier, S.E., Patton, B.W., Rank, P.J., 1995. Simulation-based diagnostics and control for nuclear power plants. DOE/ER-75712-3, Final Report for the Period April 15, 1992–April 14, 1995.
Liel, A.B., Haselton, C.B., Deierlein, G.G., Baker, J.W., 2009. Incorporating modeling uncertainties in the assessment of seismic collapse risk of buildings. Structural Safety 31 (2), 197–211.
Lu, Z., Song, S., Yue, Z., Wang, J., 2008. Reliability sensitivity method by Line Sampling. Structural Safety 30, 517–532.
MacKay, M.D., Beckman, R.J., Conover, W.J., 1979. A comparison of three methods for selecting values of input variables in the analysis of output from a computer code. Technometrics 21 (2), 239–245.
Mackay, F.J., Apostolakis, G.E., Hejzlar, P., 2008. Incorporating reliability analysis into the design of passive cooling systems with an application to a gas-cooled reactor. Nuclear Engineering and Design 238 (1), 217–228.
Makai, M., Pal, L., 2006. Best estimate method and safety analysis II. Reliability Engineering and System Safety 91, 222–232.
Marquès, M., Pignatel, J.F., Saignes, P., D'Auria, F., Burgazzi, L., Müller, C., Bolado-Lavin, R., Kirchsteiger, C., La Lumia, V., Ivanov, I., 2005. Methodology for the reliability evaluation of a passive system and its integration into a probabilistic safety assessment. Nuclear Engineering and Design 235, 2612–2631.
Marrel, A., Iooss, B., Laurent, B., Roustant, O., 2009. Calculations of Sobol indices for the Gaussian process metamodel. Reliability Engineering and System Safety 94, 742–751.
Marseguerra, M., Zio, E., Martorell, S., 2006. Basics of genetic algorithms optimization for RAMS applications. Reliability Engineering and System Safety 91 (9), 977–991.
Mathews, T.S., Ramakrishnan, M., Parthasarathy, U., John Arul, A., Senthil Kumar, C., 2008. Functional reliability analysis of safety grade decay heat removal system of Indian 500 MWe PFBR. Nuclear Engineering and Design 238 (9), 2369–2376.
Mathews, T.S., Arul, A.J., Parthasarathy, U., Kumar, C.S., Ramakrishnan, M., Subbaiah, K.V., 2009. Integration of functional reliability analysis with hardware reliability: An application to safety grade decay heat removal system of Indian 500 MWe PFBR. Annals of Nuclear Energy 36, 481–492.
Metropolis, N., Rosenbluth, A.W., Rosenbluth, M.N., Taller, A.H., 1953. Equations of state calculations by fast computing machines. Journal of Chemical Physics 21 (6), 1087–1092.
Morris, M.D., 2000. Three technometrics experimental design classics. Technometrics 42 (1), 26–27.
Nayak, A.K., Gartia, M.R., Antony, A., Vinod, G., Sinha, R.K., 2008a. Passive system reliability analysis using the APSRA methodology. Nuclear Engineering and Design 238, 1430–1440.
Nayak, A.K., Jain, V., Gartia, M.R., Srivastava, A., Prasad, H., Anthony, A., Gaikwad, A.J., Bhatia, S.K., Sinha, R.K., 2008b. Reliability assessment of passive isolation condenser system using APSRA methodology. Annals of Nuclear Energy 35, 2270–2279.
Nayak, A.K., Jain, V., Gartia, M.R., Prasad, H., Anthony, A., Bhatia, S.K., Sinha, R.K., 2009. Reliability assessment of passive isolation condenser system of AHWR using APSRA methodology. Reliability Engineering and System Safety 94, 1064–1075.
NUREG-1150, 1990. Severe Accident Risk: an Assessment for Five US Nuclear Power Plants. US Nuclear Regulatory Commission.
NUREG-CR-6850, 2005. EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology. US Nuclear Regulatory Commission.
Nutt, W.T., Wallis, G.B., 2004. Evaluations of nuclear safety from the outputs of computer codes in the presence of uncertainties. Reliability Engineering and System Safety 83, 57–77.
Olsson, A., Sabdberg, G., Dahlblom, O., 2003. On Latin hypercube sampling for structural reliability analysis. Structural Safety 25, 47–68.
Pagani, L., Apostolakis, G.E., Hejzlar, P., 2005. The impact of uncertainties on the performance of passive systems. Nuclear Technology 149, 129–140.
Patalano, G., Apostolakis, G.E., Hejzlar, P., 2008. Risk-informed design changes in a passive decay heat removal system. Nuclear Technology 163, 191–208.
Pebesma, E.J., Heuvelink, G.B.M., 1999. Latin hypercube sampling of Gaussian random fields. Technometrics 41 (4), 203–212.
Pedroni, N., Zio, E., Apostolakis, G.E., 2010. Comparison of bootstrapped Artificial Neural Networks and quadratic Response Surfaces for the estimation of the functional failure probability of a thermal–hydraulic passive system. Reliability Engineering and System Safety 95 (4), 386–395.
Pourgol-Mohamad, M., Mosleh, A., Modarres, M., 2010. Methodology for the use of experimental data to enhance model output uncertainty assessment in thermal hydraulics codes. Reliability Engineering and System Safety 95 (2), 77–86.
Pradlwarter, H.J., Pellissetti, M.F., Schenk, C.A., Schueller, G.I., Kreis, A., Fransen, S., Calvi, A., Klein, M., 2005. Realistic and efficient reliability estimation for aerospace structures. Computer Methods in Applied Mechanics and Engineering 194, 1597–1617.
Pradlwarter, H.J., Schueller, G.I., Koutsourelakis, P.S., Charmpis, D.C., 2007. Application of line sampling simulation method to reliability benchmark problems. Structural Safety 29, 208–221.

Rohde, M., Marcel, C.P., Manera, A., Van der Hagen, T.H.J.J., Shiralkar, B., 2008. Investigating the ESBWR stability with experimental and numerical tools: a comparative study. Nuclear Engineering and Design 240 (2), 275–384.
Rumelhart, D.E., Hinton, G.E., Williams, R.J., 1986. Learning internal representations by error back-propagation. In: Rumelhart, D.E., McClelland, J.L. (Eds.), Parallel Distributed Processing: Exploration in the Microstructure of Cognition, vol. 1. MIT Press, Cambridge (MA).
Sallaberry, C.J., Helton, J.C., Hora, S.C., 2008. Extension of Latin Hypercube samples with correlated variables. Reliability Engineering and System Safety 93 (7), 1047–1059.
Saltelli, A., 2002a. Making best use of model evaluations to compute sensitivity indices. Computer Physics Communications 145, 280–297.
Saltelli, A., 2002b. Sensitivity analysis for importance assessment. Risk Analysis 22 (3), 579–590.
Saltelli, A., Ratto, M., Andres, T., Campolongo, F., Cariboni, J., Gatelli, D., Saisana, M., Tarantola, S., 2008. Global Sensitivity Analysis. The Primer. John Wiley and Sons Ltd.
Schueller, G.I., 2007. On the treatment of uncertainties in structural mechanics and analysis. Computers and Structures 85, 235–243.
Schueller, G.I., 2009. Efficient Monte Carlo simulation procedures in structural uncertainty and reliability analysis—recent advances. Journal of Structural Engineering and Mechanics 32 (1), 1–20.
Schueller, G.I., Pradlwarter, H.J., 2007. Benchmark study on reliability estimation in higher dimensions of structural systems—an overview. Structural Safety 29 (3), 167–182.
Schueller, G.I., Pradlwarter, H.J., Koutsourelakis, P.S., 2004. A critical appraisal of reliability estimation procedures for high dimensions. Probabilistic Engineering Mechanics 19, 463–474.
Secchi, P., Zio, E., Di Maio, F., 2008. Quantifying uncertainties in the estimation of safety parameters by using bootstrapped artificial neural networks. Annals of Nuclear Energy 35, 2338–2350.
Sobol, I.M., 1993. Sensitivity analysis for nonlinear mathematical model. Mathematical Modeling & Computational Experiment 1, 407–414.
Storlie, C.B., Helton, J.C., 2008. Multiple predictor smoothing methods for sensitivity analysis: description of techniques. Reliability Engineering and System Safety 93, 28–54.
Storlie, C.B., Swiler, L.P., Helton, J.C., Sallaberry, C.J., 2009. Implementation and evaluation of nonparametric regression procedures for sensitivity analysis of computationally demanding models. Reliability Engineering and System Safety 94, 1735–1763.
USNRC, 2002. An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-specific Changes to the Licensing Basis. NUREG-1. 174 – Revision 1. US Nuclear Regulatory Commission, Washington, DC.
USNRC, 2009. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. NUREG-1855. US Nuclear Regulatory Commission, Washington, DC.
Valdebenito, M.A., Pradlwarter, H.J., Schueller, G.I., 2010. The role of the design point for calculating failure probabilities in view of dimensionality and structural nonlinearities. Structural Safety 32 (2), 101–111.
Volkova, E., Iooss, B., Van Dorpe, F., 2008. Global sensitivity analysis for a numerical model of radionuclide migration from the RRC "Kurchatov Institute" red-waste disposal site. Stochastic Environmental Research and Risk Assessment 22, 17–31.
Wilks, S.S., 1942. Statistical prediction with special reference to the problem of tolerance limits. Annals of Mathematical Statistics 13, 400–409.
Woo, T.H., Lee, U.C., 2009a. Dynamical reliability of the passive system in the very high temperature gas cooled reactor. Annals of Nuclear Energy 36, 1299–1306.
Woo, T.H., Lee, U.C., 2009b. Passive system reliability in the nuclear power plants (NPPs) using statistical modeling. Nuclear Engineering and Design 239 (12), 3014–3020.
Woo, T.H., Lee, U.C., 2010. The statistical analysis of the passive system reliability in the Nuclear Power Plants (NPPs). Progress in Nuclear Energy 52, 456–461.
Zio, E., 2006. A study of the bootstrap method for estimating the accuracy of artificial neural networks in predicting nuclear transient processes. IEEE Transactions on Nuclear Science 53 (3), 1460–1470.
Zio, E., Apostolakis, G.E., 1996. Two methods for the structured assessment of model uncertainty by experts in performance assessment in radioactive waste repositories. Reliability Engineering and System Safety 54 (2), 225–241.
Zio, E., Cantarella, M., Cammi, A., 2003. The analytic hierarchy process as a systematic approach to the identification of important parameters for the reliability assessment of passive systems. Nuclear Engineering and Design 226, 311–336.
Zio, E., Pedroni, N., 2009a. Building confidence in the reliability assessment of thermal–hydraulic passive systems. Reliability Engineering and System Safety 94 (2), 268–281.
Zio, E., Pedroni, N., 2009b. Estimation of the functional failure probability of a thermal–hydraulic passive systems by means of Subset Simulation. Nuclear Engineering and Design 239, 580–599.
Zio, E., Pedroni, N., 2009c. Functional failure analysis of a thermal–hydraulic passive system by means of Line Sampling. Reliability Engineering and System Safety 94 (11), 1764–1781.
Zio, E., Pedroni, N., 2010. An optimized Line Sampling method for the estimation of the failure probability of nuclear passive systems. Reliability Engineering and System Safety, doi:10.1016/j.ress.2010.06.007.
Zio, E., Apostolakis, G.E., Pedroni, N., 2010. Quantitative functional failure analysis of a thermal–hydraulic passive system by means of bootstrapped Artificial Neural Networks. Annals of Nuclear Energy 37 (5), 639–649.

 DOI: 10.1111/risa.12305

Assessing the Performance of a Classification-Based Vulnerability Analysis Model

Tai-ran Wang,[1,*] Vincent Mousseau,[2] Nicola Pedroni,[1] and Enrico Zio[1,3]

In this article, a classification model based on the majority rule sorting (MR-Sort) method is employed to evaluate the vulnerability of safety-critical systems with respect to malevolent intentional acts. The model is built on the basis of a (limited-size) set of data representing (*a priori* known) vulnerability classification examples. The empirical construction of the classification model introduces a source of uncertainty into the vulnerability analysis process: a quantitative assessment of the performance of the classification model (in terms of accuracy and confidence in the assignments) is thus in order. Three different approaches are here considered to this aim: (i) a model-retrieval-based approach, (ii) the bootstrap method, and (iii) the leave-one-out cross-validation technique. The analyses are presented with reference to an exemplificative case study involving the vulnerability assessment of nuclear power plants.

KEY WORDS: Classification model; confidence estimation; MR-Sort; nuclear power plants; vulnerability analysis

1. INTRODUCTION

The vulnerability of safety-critical systems and infrastructures (e.g., nuclear power plants) is of great concern, given the multiple and diverse hazards that they are exposed to (e.g., intentional, random, natural)[1] and the potential large-scale consequences. This has motivated an increased attention in analyses to guide designers, managers, and stakeholders in (i) the systematic identification of the sources of vulnerability, (ii) its qualitative and quantitative assessment,[2,3] and (iii) the selection of proper actions to reduce it. In this article, we are concerned only with *intentional* hazards (i.e., those related to malevolent acts) and we mainly address issue (ii) mentioned above (i.e., the quantitative evaluation of vulnerability).

With respect to that, due to the specific features (low frequency but important effects) of intentional hazards (characterized by significant *uncertainties* due to behaviors of different rationality) the analysis is difficult to perform by traditional risk assessment methods.[1,4,5] For this reason, in this work we propose to tackle the issue of evaluating vulnerability to malevolent intentional acts by an empirical classification modeling framework. In particular, we adopt a classification model based on the majority rule sorting (MR-Sort) method[6] to assign an alternative of interest (i.e., a safety-critical system) to a given (vulnerability) class (or category). The MR-Sort classification model contains a group of (adjustable) parameters that have to be calibrated by means of a set of *empirical* classification examples (also called training set), that is, a set of alternatives with the corresponding preassigned vulnerability classes.

[1]Chair on Systems Science and the Energy Challenge, European Foundation for New Energy-Electricité de France, Ecole Centrale Paris and Supélec, Chatenay Malabry Cedex, France.
[2]Laboratory of Industrial Engineering, Ecole Centrale Paris, Grande Voie des Vignes, F92-295, Chatenay Malabry Cedex, France.
[3]Politecnico di Milano, Energy Department, Nuclear Section, c/o Cesnef, via Ponzio 33/A, 20133, Milan, Italy.
*Address correspondence to Tai-ran Wang, Ecole Centrale Paris and Supélec, Grande Voie des Vignes, F92-295, Chatenay Malabry, Cedex, France; tairan.wang@ecp.fr.

 0272-4332/14/0100-0001$22.00/1 © 2014 Society for Risk Analysis

Due to the finite (typically small) size of the set of training classification examples usually available in the analysis of real complex safety-critical systems, the performance of the classification model is impaired. In particular, (i) the classification *accuracy* (resp., error), that is, the expected fraction of patterns correctly (resp., incorrectly) classified, is typically reduced (resp., increased); (ii) the classification process is characterized by significant uncertainty, which affects the *confidence* of the classification-based vulnerability model: in our work, we define the confidence in a classification assignment as in Ref. 10, that is, as the probability that the class assigned by the model to a given (single) pattern is the correct one. Obviously, there is the possibility that a classification model assigns correctly a very large (expected) fraction of patterns (i.e., the model is very accurate), but at the same time *each* (correct) assignment is affected by significant uncertainty (i.e., it is characterized by low confidence). It is worth mentioning that besides the scarcity of training data, there are many additional sources of uncertainty in classification problems (e.g., the accuracy of the data, the suitability of the classification technique used): however, they are not considered in this work.

The performance of the classification model (i.e., the classification accuracy—resp., error—and the confidence in the classification) needs to be quantified: this is of paramount importance for taking robust decisions in the vulnerability analyses of safety-critical systems.[7,8]

In this article, three different approaches are used to assess the performance of a classification-based MR-Sort vulnerability model in the presence of small training data sets. The first is a model-retrieval-based approach,[6] which is used to assess the expected percentage error in assigning new alternatives. The second is based on *bootstrapping* the available training set in order to build an ensemble of vulnerability models;[9] the method can be used to assess both the accuracy and the confidence of the model: in particular, the confidence in the assignment of a given alternative is given in terms of the full (probability) distribution of the possible vulnerability classes for that alternative (built on the bootstrapped ensemble of vulnerability models).[10] The third is based on the leave-one-out cross-validation (LOOCV) technique, in which one element of the available data set is (left out and) used to test the accuracy of the classification model built on the remaining data: also this approach is employed to estimate the accuracy of the classification vulnerability model as the expected percentage error, that is, the fraction of alternatives incorrectly assigned (computed as an average over the left-out data).

The contribution of this work is twofold:

- classification models have proved useful in a variety of fields including finance, marketing, environmental and energy management, human resources management, medicine, risk analysis, fault diagnosis, etc.,[11] but to the best of the authors' knowledge, this work is the first to propose a classification-based hierarchical framework for the analysis of the vulnerability to intentional hazards of safety-critical systems;
- the bootstrap method is originally applied to estimate the confidence in the assignments provided by the MR-Sort classification model, in terms of the probability that a given alternative is correctly classified.

The article is organized as follows. The next section presents the hierarchical framework for vulnerability analysis to intentional hazards. Section 3 shows the classification model applied within the proposed framework. Section 4 describes the learning process of a classification model by the disaggregation method. In Section 5 three approaches are proposed to analyze the performance of the classification model. Then, the proposed approaches are validated on the case study of a group of nuclear power plants (NPPs) in Section 6. Finally, Sections 7 and 8 present the discussion and conclusions of this research.

2. GENERAL FRAMEWORK: VULNERABILITY TO INTENTIONAL HAZARDS

Vulnerability is defined in different ways depending on the domains of application, for example, a measure of possible future harm due to exposure to a hazard,[1] the identification of weaknesses in security, focusing on defined threats that could compromise a system's ability to provide a service,[12] the set of conditions and processes resulting from physical, social, economic, and environmental factors that increase the susceptibility of a community to the impact of hazards.[13]

With the focus on the susceptibility to intentional hazards, the three-layers hierarchical model developed in Ref. 14 is considered and shown in Fig. 1. The susceptibility to intentional hazards is characterized

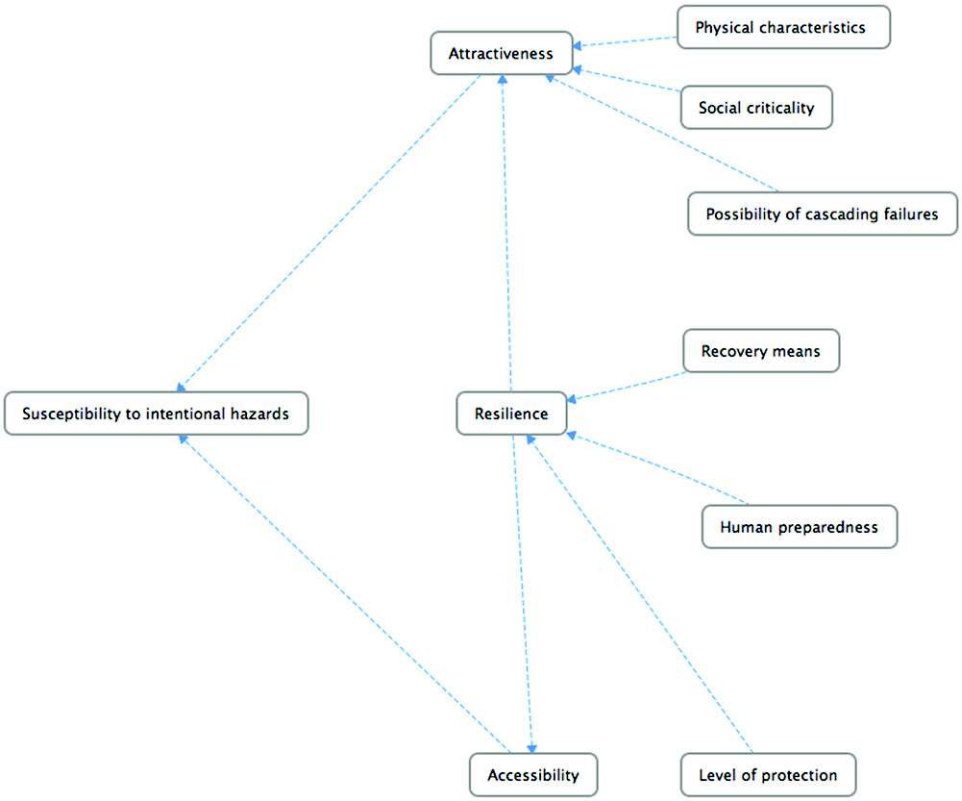


Fig. 1. Hierarchical model for susceptibility to intentional hazards.

in terms of attractiveness and accessibility. These are hierarchically broken down into factors that influence them, including resilience seen as pre-attack protection (which influences on accessibility) and post-attack recovery (which influences on attractiveness). The decomposition is made in six criteria, which are further decomposed into a layer of basic subcriteria, for which data and information can be collected. The details of the general framework of analysis are not given here for brevity; the interested reader is referred to Ref. 14 and to Appendix A.

For the purpose of this article, only six criteria are considered: physical characteristics, social criticality, possibility of cascading failures, recovery means, human preparedness, and level of protection (Fig. 1). These six criteria are used as the basis to assess the vulnerability of a given safety-critical system of interest (e.g., an NPP). Four levels (or categories) of vulnerability are considered: satisfactory, acceptable, problematic, and serious. In this view, the issue of assessing vulnerability is here tackled within a classification framework: given the characterization of a critical system in terms of the six criteria mentioned above, a proper vulnerability category (or class) has to be selected for that system. A description of the algorithm used to this purpose is given in the following section.

It is worthy to mention that the cyber characteristics are not taken into account in this work; in future work they will be added for the criteria physical characteristics and protection.

3. CLASSIFICATION MODEL FOR VULNERABILITY ANALYSIS: THE MR-SORT METHOD

The MR-Sort method is a simplified version of ELECTRE Tri, an outranking sorting procedure in which the assignment of an alternative to a given category is determined using a complex concordance-non-discordance rule.[15,16] We assume that the alternative to be classified (in this article, a safety-critical system or infrastructure of interests, e.g., an NPP) can be described by an n-tuple of elements $x = \{x_1, x_2, ..., x_i, ..., x_n\}$, which represent the evaluation of the alternative with respect to a set of n

criteria (by way of example, in this article the criteria used to evaluate the vulnerability of a safety-critical system of interest may include its physical characteristics, social criticality, level of protection, and so on: see Section 2). We denote the set of criteria by $N = \{1, 2, ..., i, ..., n\}$ and assume that the values x_i of criterion i range in the set X_i[9] (e.g., in this article all the criteria range in [0, 1]). The MR-Sort procedure allows assigning any alternative $x = \{x_1, x_2, ..., x_i, ..., x_n\} \in X = X_1 \times X_2 \times ... \times X_i \times ... \times X_n$ to a particular predefined category (in this article, a class of vulnerability), in a given ordered set of categories, $\{A^h : h = 1, 2, ..., k\}$; as mentioned in Section 2, $k = 4$ categories are considered in this work: A^1 = satisfactory, A^2 = acceptable, A^3 = problematic, A^4 = serious.

To this aim, the model is further specialized in the following way:

- We assume that X_i is a subset of $\mathbb{R}$ for all $i \in \mathbb{N}$ and the subintervals $(X_i^1, X_i^2, ..., X_i^h, ..., X_i^k)$ of X_i are compatible with the order on the real numbers, that is, for all $x_i^1 \in X_i^1, x_i^2 \in X_i^2, ..., x_i^h \in X_i^h, ..., x_i^k \in X_i^k$, we have $x_i^1 > x_i^2 > ... > x_i^h > ... > x_i^k$. We assume furthermore that each interval $x_i^h, h = 2, 3, ..., k$ has a smallest element b_i^h, which implies that $x_i^{h-1} \geq b_i^h > x_i^h$. The vector $b^h = \{b_1^h, b_2^h, ..., b_i^h, ..., b_n^h\}$ (containing the lower bounds of the intervals X_i^h of criteria $i = 1, 2, ..., n$ in correspondence of category h) represents the lower limit profile of category A^h.
- There is a weight ω_i associated with each criterion $i = 1, 2, ..., n$, quantifying the relative importance of criterion i in the vulnerability assessment process; notice that the weights are normalized such that $\sum_{i=1}^n \omega_i = 1$.
  In this framework, a given alternative $x = \{x_1, x_2, ..., x_i, ..., x_n\}$ is assigned to category $A^h, h = 1, 2, ..., k$, if

$$\sum_{i \in \mathbb{N}: x_i \geq b_i^h} \omega_i \geq \lambda \; and \sum_{i \in \mathbb{N}: x_i \geq b_i^{h+1}} \omega_i < \lambda, \quad (1)$$

  where λ is a threshold ($0 \leq \lambda \leq 1$) chosen by the analyst. Rule (1) is interpreted as follows. An alternative x belongs to category A^h if: (1) its evaluations in correspondence of the n criteria (i.e., the values $\{x_1, x_2, ..., x_i, ..., x_n\}$) are at least as good as b_i^h(lower limit of category A^h with respect to criterion i), $i = 1, 2, ..., n$, on a subset of criteria that has sufficient importance (in other words, on a subset of criteria that has a weight larger than or equal to the threshold λ chosen by the analyst); and at the same time (2) the weight of the subset of criteria on which the evaluations $\{x_1, x_2, ..., x_i, ..., x_n\}$ are at least as good as b_i^{h+1}(lower limit of the successive category A^{h+1} with respect to criterion i), $i = 1, 2, ..., n$, is not sufficient to justify the assignment of x to the successive category A^{h+1}. Notice that alternative x is assigned to the best category A^1 if $\sum_{i \in \mathbb{N}: x_i \geq b_i^1} \omega_i \geq \lambda$ and it is assigned to the worst category A_k if $\sum_{i \in \mathbb{N}: x_i \geq b^{-k-1}} \omega_i < \lambda$. Finally, it is straightforward to notice that the parameters of such a model are the $k \cdot n$ lower limit profiles (n limits for each of the k categories), the n weights of the criteria $\omega_1, \omega_2, ..., \omega_i, ..., \omega_n$, and the threshold λ, for a total of $n(k+1)+1$ parameters.

4. CONSTRUCTING THE MR-SORT CLASSIFICATION MODEL

In order to construct an MR-Sort classification model, we need to determine the set of $n(k+1)+1$ parameters described in Section 2, that is, the weights $\omega = \{\omega_1, \omega_2, ..., \omega_n\}$, the lower profiles $b = \{b^1, b^2, ..., b^h, ..., b^k\}$,with $b^h = \{b_1^h, b_2^h, ..., b_i^h, ..., b_n^h\}, h = 1, 2, ..., k$, and the threshold λ; in this article, λ is considered a fixed, constant value chosen by the analyst (e.g., $\lambda = 0.9$).

To this aim, the decision maker provides a training set of classification examples $D_{TR} = \{(x_p, \Gamma_p^t), p = 1, 2, ..., N_{TR}\}$, that is, a set of N_{TR} alternatives (in this case, NPPs) $x_p = \{x_1^p, x_2^p, ..., x_i^p, ..., x_n^p\}, p = 1, 2, ..., N_{TR}$ together with the corresponding real preassigned categories (i.e., vulnerability classes) Γ_p^t (the superscript t indicates that Γ_p^t represents the true, *a priori* known vulnerability class of alternative x_p).

The calibration of the $n(k+1)$ parameters is done through the learning process detailed in Ref. 6. In extreme synthesis, the information contained in the training set D_{TR} is used to restrict the set of MR-Sort models compatible with such information, and to finally select one among them.[6] The *a priori* known assignments generate constraints on the parameters of the MR-Sort model. In Ref. 6, such constraints have a linear formulation and are integrated into a mixed integer program (MIP) that is designed to select one (optimal) set of such parameters ω^* and b^* (in other words, to select one classification model $M(\cdot|\omega^*, b^*)$) that is coherent with

the data available and maximizes a defined *objective function*. In Ref. 6, the optimal parameters ω^* and b^* are those that maximize the value of the minimal slack in the constraints generated by the given set of data D_{TR}. Once the (optimal) classification model $M(\cdot|\omega^*, b^*)$ is constructed, it can be used to assign a new alternative x(i.e., a new NPP) to one of the vulnerability classes $A^h, h = 1, 2, ..., k$: in other words, $M(x|\omega^*, b^*) = \Gamma_x^M$ where Γ_x^M is the class assigned by model $M(\cdot|\omega^*, b^*)$ to alternative x and assumes one value among $\{A^h : h = 1, 2, ..., k\}$. Further mathematical details about the training algorithm are not given here for brevity: the reader is referred to Ref. 6 and to Appendix B.

Obviously, the number N_{TR} of available classification examples is finite and quite small in most real applications involving the vulnerability analysis of safety-critical systems. As a consequence, the model $M(\cdot|\omega^*, b^*)$ is only a partial representation of reality and its assignments are affected by uncertainty: this uncertainty, which needs to be quantified to build confidence in the decision process that follows the vulnerability assessment.

In the following section, three different methods are presented to assess the performance of the MR-Sort classification model.

5. METHODS FOR ASSESSING THE PERFORMANCE OF THE CLASSIFICATION-BASED VULNERABILITY ANALYSIS MODEL

5.1. Model-Retrieval-Based Approach

The first method is based on the model-retrieval approach proposed in Ref. 6. A fictitious set D_{TR}^{rand} of N_{TR} alternatives $\{x_p^{rand} : p = 1, 2, ..., N_{TR}\}$ is generated by random sampling within the ranges X_i of the criteria, $i = 1, 2, ..., n$. Notice that the size N_{TR} of the fictitious set D_{TR}^{rand} has to be the same as the real training set D_{TR} available, for the comparison to be fair. Also, an MR-Sort classification model $M(\cdot|\omega^{rand}, b^{rand})$ is constructed by randomly sampling possible values of the internal parameters, $\{\omega_i : i = 1, 2, ..., n\}$ and $\{b_h : h = 1, 2, ..., k-1\}$. Then, we simulate the behavior of a decision-maker (DM) by letting the (random) model $M(\cdot|\omega^{rand}, b^{rand})$ assign the (randomly generated) alternatives $\{x_p^{rand} : p = 1, 2, ..., N_{TR}\}$. In other words, we construct a learning set D_{TR}^{rand} by assigning the (randomly generated) alternatives using the (randomly generated) MR-Sort model, that is, $D_{TR}^{rand} = \{(x_p^{rand}, \Gamma_p^M) : p = 1, 2, ..., N_{TR}\}$, where Γ_p^M is the class assigned by model $M(\cdot|\omega^{rand}, b^{rand})$ to alternative x_p^{rand}, that is, $\Gamma_p^M = M(x_p^{rand}|\omega^{rand}, b^{rand})$. Subsequently, a new MR-Sort model $M'(\cdot|\omega', b')$, compatible with the training set D_{TR}^{rand}, is inferred using the MIP formulation summarized in Section 3 and in Appendix B. Although models $M(\cdot|\omega^{rand}, b^{rand})$ and $M'(\cdot|\omega', b')$ may be quite different, they coincide on the way they assign elements of D_{TR}^{rand}, by construction. In order to compare models M and M', we randomly generate a (typically large) set D_{test}^{rand} of *new* alternatives $D_{test}^{rand} = \{x_p^{test,rand} : p = 1, 2, ..., N_{Test}\}$ and we compute the percentage of assignment errors, that is, the proportion of these N_{Test} alternatives that models M and M' assign to different categories.

In order to account for the randomness in the generation of the training set D_{TR}^{rand} and of the model $M(\cdot|\omega^{rand}, b^{rand})$, and to provide robust estimates for the assignment errors ϵ, the procedure outlined above is repeated for a large number N_{sets} of random training sets $D_{TR}^{rand,j}$, $j = 1, 2, ..., N_{sets}$; in addition, for each set j the procedure is repeated for different random models $M(\cdot|\omega^{rand,l}, b^{rand,l})$, $l = 1, 2, ..., N_{models}$. The sequence of assignment errors thereby generated, e_{jl}, $j = 1, 2, ..., N_{sets}$, $l = 1, 2, ..., N_{models}$, is then averaged to obtain a robust estimate for ϵ. The procedure is sketched in Fig. 2.

Notice that this method does not make any use of the original training set D_{TR} (i.e., of the training set constituted by real-world classification examples). In this view, the model-retrieval-based approach can be interpreted as a tool to obtain an absolute evaluation of the expected error that an "average" MR-Sort classification model $M(\cdot|\omega, b)$ with k categories, n criteria, and trained by means of an "average" data set of given size N_{TR} makes in the task of classifying a new generic (unknown) alternative.

5.2. The Bootstrap Method

A way to assess *both* the accuracy (i.e., the expected fraction of alternatives correctly classified) *and* the confidence of the classification model (i.e., the probability that the category assigned to a given alternative is the correct one) is by resorting to the bootstrap method,[17] which is used to create an ensemble of classification models constructed on different data sets bootstrapped from the original one:[18] the final class assignment provided by the ensemble

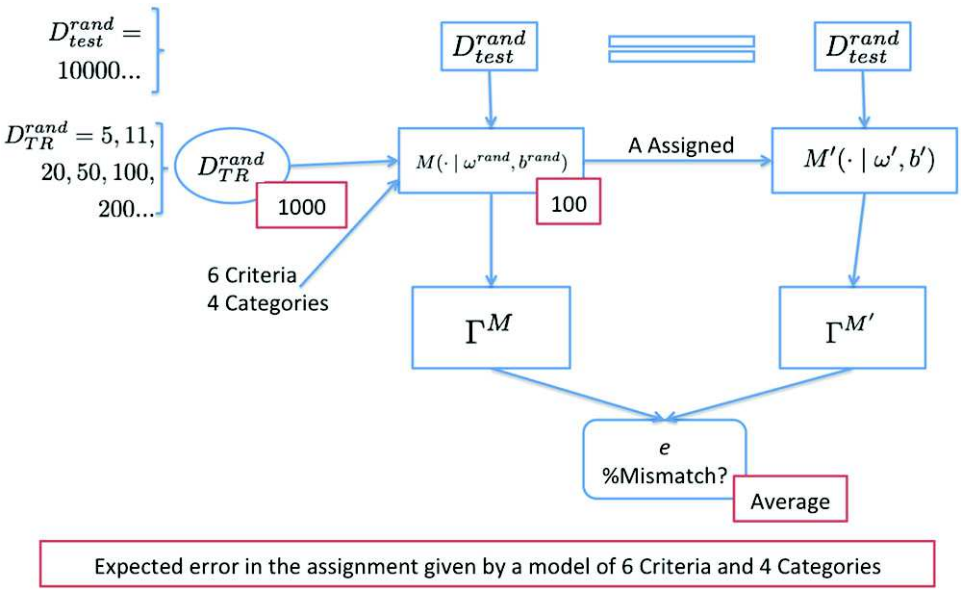


Fig. 2. The general structure of the model-retrieval approach.

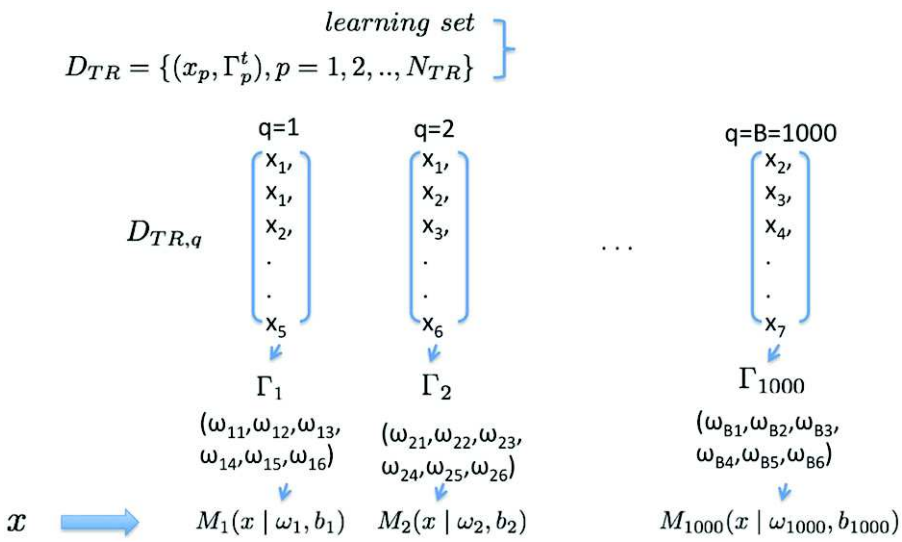


Fig. 3. The bootstrap algorithm.

is based on the combination of the individual output of classes provided by the ensemble of models.[10]

The basic idea is to generate different training data sets by random sampling with replacement from the original one:[17] such different training sets are used to build different individual classification models of the ensemble. In this way, the individual classifiers of the ensemble possibly perform well in different regions of the training space and thus they are expected to make errors on alternatives with different characteristics; these errors are balanced out in the combination, so that the performance of the ensemble of bootstrapped classification models is in general superior to that of the single classifiers.[18,19] This is a desirable property since it is a more realistic simulation of the real-life experiment from which our data set was obtained. In this article, the output classes of the single classifiers are combined by *majority voting*: the class chosen by most classifiers is the ensemble assignment. Finally, the

accuracy of the model is given by the fraction of the patterns correctly classified. The bootstrap-based empirical distribution of the assignments given by the different classification models of the ensemble is then used to measure the confidence in the classification of a given alternative x that represent the probability that this alternative is correctly assigned.[10,20]

In more detail, the main steps of the bootstrap algorithm are as follows (Fig. 3):

(1) Build an ensemble of B (typically of the order of 500–1,000) classification models $\{M_q(\cdot|(\omega_q, b_q) : q = 1, 2, ..., B)\}$ by random sampling with replacement from the original data set D_{TR} and use each of the bootstrapped models $M_q(\cdot|\omega_q, b_q)$ to assign a class $\Gamma_x^q, q = 1, 2, ..., B$, to a given alternative x of interest (notice that Γ_x^q takes a value in $A^h, h = 1, 2, ..., k$). By so doing, a bootstrap-based empirical probability distribution $P(A^h|x), h = 1, 2, ..., k$ for category A^h of alternative x is produced, which is the basis for assessing the confidence in the assignment of alternative x. In particular, repeat the following steps for $q = 1, 2, ..., B$:
   (i) Generate a bootstrap data set $D_{TR,q} = \{(x_p, \Gamma_p^t) : p = 1, 2, ..., N_{TR}\}$, by performing random sampling with replacement from the original data set $D_{TR} = \{(x_p, \Gamma_p^t) : p = 1, 2, ..., N_{TR}\}$ of N_{TR} input/output patterns. The data set $D_{TR,q}$ is thus constituted by the same number N_{TR} of input/output patterns drawn among those in D_{TR}, although due to the sampling with replacement some of the patterns in D_{TR} will appear more than once in $D_{TR,q}$, whereas some will not appear at all.
   (ii) Build a classification model $\{M_q(\cdot|\omega_q, b_q) : q = 1, 2, ..., B\}$, on the basis of the bootstrap data set $D_{TR,q} = \{(x_p, \Gamma_p^t) : p = 1, 2, ..., N_{TR}\}$.
   (iii) Use the classification model $M_q(\cdot|\omega_q, b_q)$ to provide a class $\Gamma_x^q, q = 1, 2, ..., B$ to a given alternative of interest, that is, $\Gamma_x^q = M_q(x|\omega_q, b_q)$.

(2) Combine the output classes $\Gamma^q, q = 1, 2, ..., B$ of the individual classifiers by majority voting: the class chosen by most classifiers is the ensemble assignment Γ_x^{ens}, i.e., $\Gamma_x^{ens} = argmax_{A^h}[card_q\{\Gamma_x^q = A^h\}]$.

(3) As an estimation of the confidence in the majority-voting assignment Γ_x^{ens}(step 2, above), we consider the bootstrap-based empirical probability distribution $P(A^h|x)$, $h = 1, 2, ..., k$, that is, the probability that category A^h is the correct category given that the (test) alternative is Ref. 6. The estimator of $P(A^h|x)$ here employed is: $P(A^h|x) = \frac{\sum_{q=1}^{B} I\{\Gamma_q = A^h\}}{B}$, where $I\{\Gamma_q = A^h\} = 1$, if $\Gamma_q = A^h$, and 0 otherwise.

(4) Finally, the error of classification is presented by the fraction of the number of the alternatives being assigned by the classification model and the total number of the alternatives. The accuracy of the classification model is defined as the complement to 1 to the error.

5.3. The LOOCV Technique

LOOCV is a particular case of the cross-validation method. In cross-validation, the original training set D_{TR} is divided into N partitions, $A_1, A_2, ..., A_N$, and the elements in each of the partitions are classified by a model trained by means of the elements in the remaining partitions (leave-p-out cross-validation).[20] The cross-validation error is, then, the average of the N individual error estimates. When N is equal to the number of elements N_{TR} in D_{TR}, the result is LOOCV, in which each instance $x_p, p = 1, 2, ..., N_{TR}$ is classified by all the instances in D_{TR} except for itself.[21] For each instance $x_p, p = 1, 2, ..., N_{TR}$ in D_{TR}, the classification accuracy is 1 if the element is classified correctly and 0 if it is not. Thus, the average LOOCV error (resp., accuracy) over all the N_{TR} instances in D_{TR} is ϵ/N_{TR} (resp., $1 - \epsilon/N_{TR}$), where ϵ(resp., $N_{TR} - \epsilon$) is the number of elements incorrectly (resp., correctly) classified. Thus, the accuracy in the assignment is estimated as $1 - \epsilon/N_{TR}$.

With respect to the leave-p-out cross-validation, the LOOCV produces a smaller bias of the true error rate estimator. However, the computational time increases significantly with the size of the data set available. This is the reason why the LOOCV is particularly useful in the case of small data sets. In addition, for *very sparse* data sets (e.g., of size lower than or equal to 10), we may be *forced* to use LOOCV in order to maximize the number of training examples employed and to generate training sets containing an amount of information that is sufficient and reasonable for building an empirical model.[22] In Fig. 4, the algorithm is sketched with reference to a training set D_{TR} containing $N_{TR} = 11$ data (like in the case study considered in the following section).

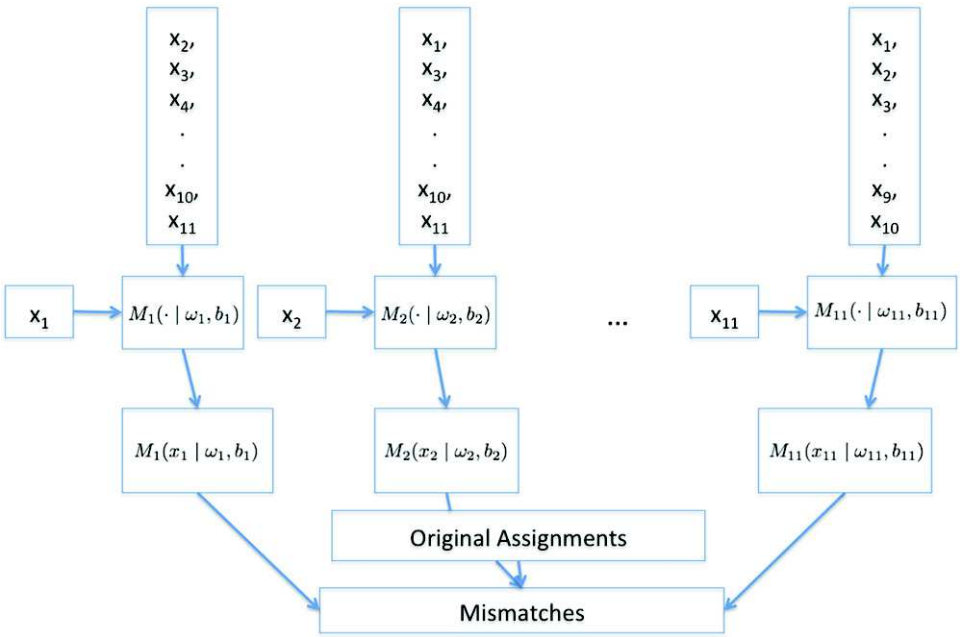


Fig. 4. Leave-one-out cross-validation study procedure.

6. APPLICATION

The methods presented in Section 5 are here applied on an exemplificative case study concerning the vulnerability analysis of NPPs.[14] We identify $n = 6$ main criteria $i = 1, 2, ..., n = 6$ by means of the hierarchical approach presented in Ref. 14 (see Section 2); x_1 = physical characteristics, x_2 = social criticality, x_3 = possibility of cascading failures, x_4 = recovery means, x_5 = human preparedness, and x_6 = level of protection. Then, $k = 4$ vulnerability categories A^h, $h = 1, 2, ..., k = 4$ are defined as: A^1 = satisfactory, A^2 = acceptable, A^3 = problematic, and A^4 = serious (Section 2). The training set D_{TR} is constituted by a group of $N_{TR} = 11$ NPPs x_p with the corresponding *a priori* known categories Γ^t_p, that is, $D_{TR} = \{(x_p, \Gamma^t_p) : p = 1, 2, ..., N_{TR} = 11\}$. The training set is summarized in Table I.

In what follows, the three techniques of Section 5 are applied to assess the performance of the MR-Sort classification-based vulnerability analysis model built using the training set D_{TR} of Table I.

Table I. Training Set with $N_{TR} = 11$ Assigned Alternatives

Alternatives, x_p	Vulnerability Class Γ^t_p
$x_1 = \{0.61, 0.6, 0.75, 0.86, 1, 0.94\}$	A^1
$x_2 = \{0.33, 0.27, 0, 0.575, 0.4, 0.72\}$	A^3
$x_3 = \{0.55, 0.33, 0.5, 0.725, 0.7, 0.71\}$	A^2
$x_4 = \{0.55, 0.33, 0.75, 0.8, 0.7, 0.49\}$	A^3
$x_5 = \{0.39, 0.23, 0.5, 0.6, 0.6, 0.62\}$	A^3
$x_6 = \{0.39, 0.27, 0.75, 0.725, 0.7, 0.68\}$	A^2
$x_7 = \{0.61, 0.7, 0.5, 0.725, 0.9, 0.94\}$	A^2
$x_8 = \{0.16, 0.1, 0.5, 0.475, 0.3, 0.59\}$	A^4
$x_9 = \{0.1, 0, 0.25, 0.5, 0.6, 0.61\}$	A^4
$x_{10} = \{0.1, 0, 0, 0.3, 0.3, 0.43\}$	A^4
$x_{11} = \{0.61, 0.7, 0.75, 1, 1, 0.94\}$	A^1

6.1. Application of the Model-Retrieval-Based Approach

We generate $N_{sets} = 1,000$ different training sets $D^{rand,j}_{TR}$, $j = 1, 2, ..., N_{sets}$, and for each set j, we randomly generate $N_{models} = 100$ models $M(\cdot|\omega^{rand,l}, b^{rand,l})$, $l = 1, 2, ..., N_{models} = 100$. By so doing, the expected accuracy (1-ϵ) of the corresponding MR-Sort model is obtained as the average of $N_{sets} \cdot N_{models} = 1,000 \cdot 100 = 100,000$ values $(1 - \epsilon_{jl})$, $j = 1, 2, ..., N_{sets}$, $l = 1, 2, ..., N_{models}$ (see Section 5.1). The size N_{test} of the random test set D^{rand}_{TR} is $N_{test} = 10,000$. Finally, we perform the procedure of Section 5.1 for different sizes N_{TR} of the random training set D^{rand}_{TR} (even if the size of the real training set available is $N_{TR} = 11$; see Table I): in particular, we choose $N_{TR} = 5, 11, 20, 50, 100,$ and 200. This analysis serves the purpose of outlining the behavior

of the accuracy $(1-\epsilon)$ as a function of the amount of classification examples available.

The results are summarized in Fig. 5 where the average percentage assignment error ϵ is shown as a function of the size N_{TR} of the learning set (from 5 to 200). As expected, the assignment error ϵ tends to decrease when the size of the learning set N_{TR} increases: the higher the cardinality of the learning set, the higher (resp., lower) the accuracy (resp., the expected error) in the corresponding assignments. Comparing these results with those obtained by Leroy *et al.* [6] using MR-Sort models with $k=2$ and 3 categories and $n=3$–5 criteria, it can be seen that for a given size of the learning set, the error rate (resp., the accuracy) grows (resp., decreases) with the number of model parameters to be determined by the training algorithm $= n(k+1)+1$. It can be seen that for our model with $n=6$ criteria and $k=4$ categories, in order to guarantee an error rate inferior to 10% we would need training sets consisting of more than $N_{TR}=100$ alternatives. Typically, for a learning set of $N_{TR}=11$ alternatives (like that available in the present case study), the average assignment error ϵ is around 30%; correspondingly, the accuracy of the MR-Sort classification model trained with the data set D_{TR} of size $N_{TR}=11$ available in the present case is around $(1-\epsilon)=70\%$: in other words, there is a probability of 70% that a new alternative (i.e., a new NPP) is assigned to the correct category of vulnerability.

In order to assess the randomness intrinsic in the procedure used to obtain the accuracy estimate mentioned above, we have also calculated the 95% confidence intervals for the average assignment error ϵ of the models trained with $N_{TR}=11, 20,$ and 100 alternatives in the training set. The 95% confidence interval for the error associated to the models trained with 11, 20, and 100 alternatives as learning set are [25.4%, 33%], [22.2%, 29.3%], and [10%, 15.5%], respectively. For illustration purposes, Fig. 6 shows the distribution of the assignment mismatch built using the $N_{sets} \cdot N_{models} = 100,000$ values ϵ_{jl}, $j=1,2,...,N_{sets}=1,000$, $l=1,2,...,N_{models}=100$, generated as described in Section 5.1 for the example of 11 alternatives.

6.2. Application of the Bootstrap Method

A number B (= 1,000) of bootstrapped training sets $D_{TR,q}$, $q=1,2,...,1,000$ of size $N_{TR}=11$ is built by random sampling with replacement from D_{TR}. The sets $D_{TR,q}$ are then used to train $B=1,000$ different classification models $\{M_1, M_2, ..., M_{1000}\}$.

Table II. Number of Patterns Classified with Confidence Value

Confidence range	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]
Number of patterns	1	2	0
Confidence range	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Number of patterns	1	2	5

This ensemble of models can be used to classify new alternatives. Fig. 7 shows the probability distributions $P(A_h|x_p)$, $h=1,2,...,k=4$, $p=1,2,...,N_{TR}=11$, empirically generated by the ensemble of $B=1,000$ bootstrapped MR-Sort classification models in the task of classifying the $N_{TR}=11$ alternatives of the training set $D_{TR}=\{x_1, x_2, ..., x_{N_{TR}}\}$. The categories highlighted by the rectangles are those selected by the majority of the classifiers of the ensemble: it can be seen that the assigned classes coincide with the original categories of the alternatives of the training set (Table I), that is, the accuracy of the inferred classification model based on the given training set (with 11 assigned alternatives) is 1.

In order to investigate the confidence of the algorithm in the classification of the test patterns, the results achieved testing one specific pattern taken in turn from the training set are analyzed. For each test of a specific pattern x_i, the distribution of the assignments by the $B=1,000$ classifiers shows the confidence of the assignment of the classification model on this specific pattern. By way of example, it can be seen that alternative x_3 is assigned to Class A^2 (the correct one) with a confidence of $P(A^2|x_3)=0.81$, whereas alternative x_6 is assigned to the same class A^2, but with a confidence of only $P(A^2|x_6)=0.56$.

Notice that the most interesting information regards the confidence in the assignment of the test pattern to the class with the highest number of votes, that is, the class actually assigned by the ensemble system according to the majority voting rule adopted.[10] In this respect, Table II reports the distribution of the confidence values associated to the class to which each of the 11 alternatives has been assigned.

Thus, a $10/11 \approx 91\%$ of all class assignments with confidence bigger than 0.5 are correct.

6.3. Application of the LOOCV Method

Based on the original training set D_{TR} of size $N_{TR}=11$, we generate 11 "new" training sets $D_{TR,i}$, $i=1,2,...,11$ (each containing $N_{TR}-1=1-$ assigned alternatives) by taking out each time one of the alternatives from D_{TR}. These 11 training

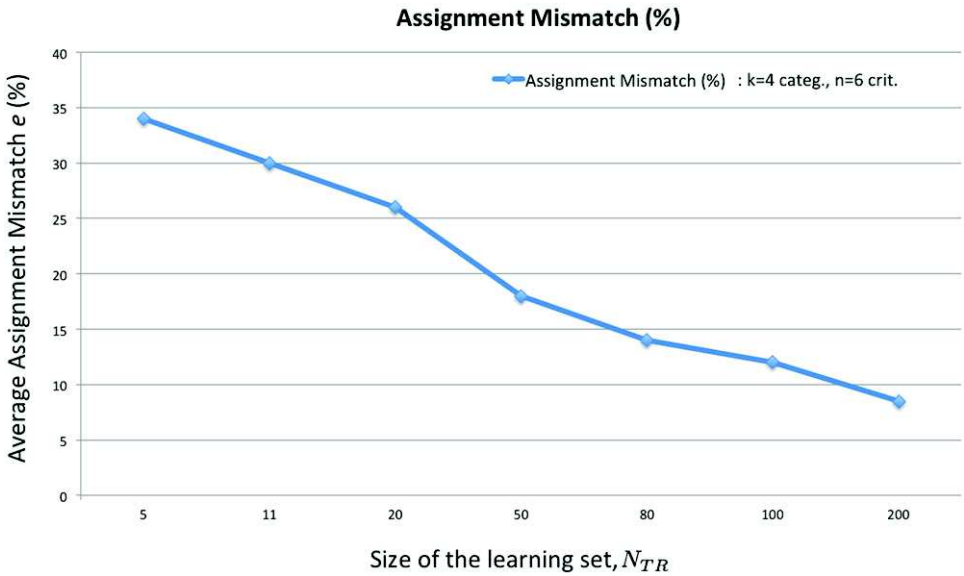


Fig. 5. Average assignment error ϵ (%) as a function of the size N_{TR} of the learning set according to the model-retrieval-based approach of Section 5.1.

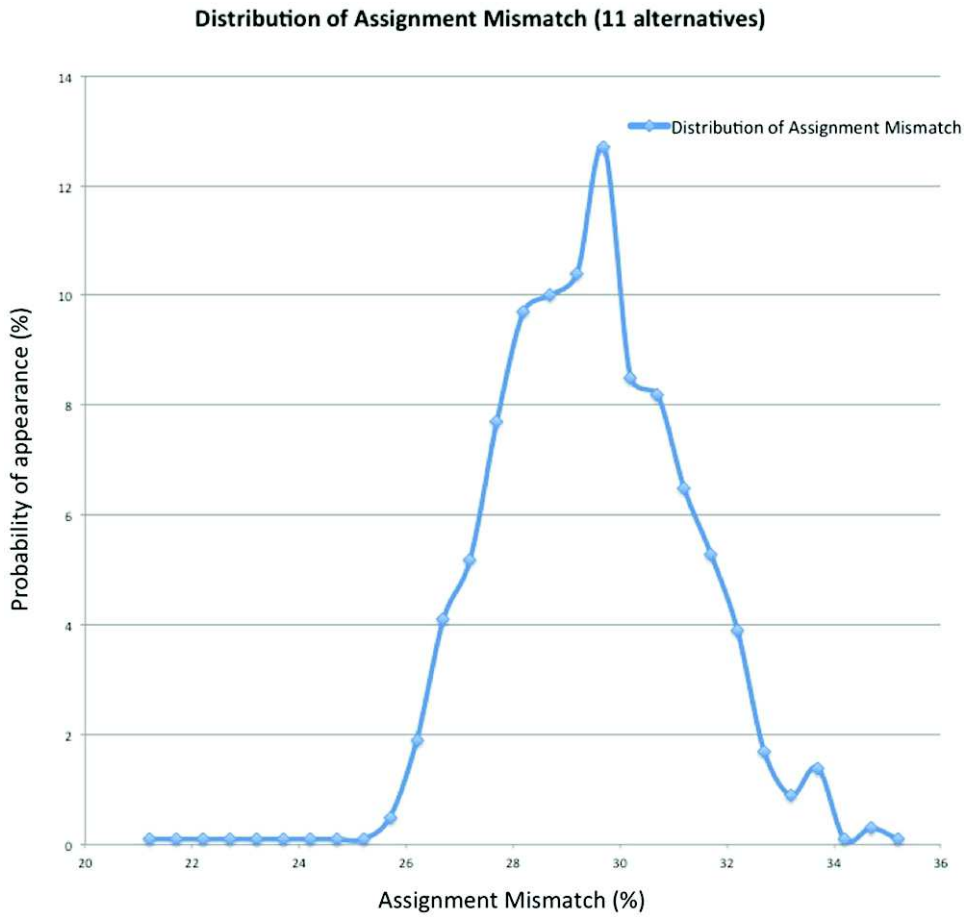


Fig. 6. Distribution of the assignment mismatch for an MR-Sort model trained with $N_{TR} = 11$ alternatives (%).

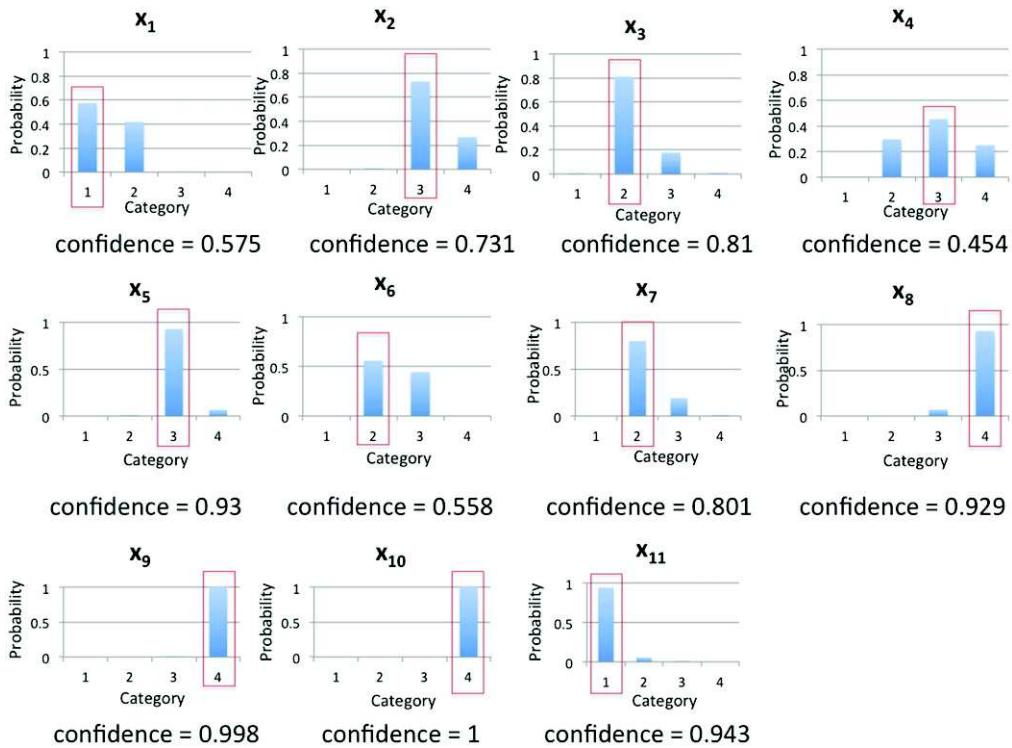


Fig. 7. Probability distributions $P(A_h|x_p)$, $h = 1, 2, ..., k = 4$, $p = 1, 2, ..., N_{TR} = 11$ obtained by the ensemble of $B = 1{,}000$ bootstrapped MR-Sort models in the classification of the alternatives x_p contained in the training set D_{TR}.

Table III. Comparison Between the Real Categories and the Assignments Provided by the LOOCV Models

Alternative	Real Categories, Γ_p^t	Assignments by LOOCV Method
x_1	1	1
x_2	3	3
x_3	2	2
x_4	3	2
x_5	3	3
x_6	2	3
x_7	2	2
x_8	4	4
x_9	4	4
x_{10}	4	4
x_{11}	1	1

sets are then used to train 11 different classification models $M_1, M_2, ..., M_{11}$. Each of these 11 models is used to classify the alternative correspondingly taken out. Table III shows the comparison between the real classes Γ_p^t of the alternatives of the training set and the categories assigned by the trained models.

It can be seen that $\epsilon = 2$ out of the $N_{TR} = 11$ alternatives are assigned incorrectly (alternatives x_4 and x_6). Thus, the accuracy in the classification is given by the complement to 1 of the average error rate, that is, $1 - \epsilon/N_{TR} = 1 - 2/11 = 1 - 0.182 = 0.818$. Notice that the 95% confidence interval for this recognition rate is [0.5901, 1].

7. DISCUSSION OF THE RESULTS

The three proposed methods provide conceptually and practically different estimates of the performance of the MR-Sort classification model.

The model-retrieval-based approach provides a quite general indication of the classification capability of a vulnerability model with given characteristics. Actually, in this approach the only constant, fixed parameters are the size N_{TR} of the training set (given by the number of real-world classification examples available), the number of criteria n, and the number of categories k (given by the analysts according to the characteristics of the systems at hand). On this basis, the space of all possible training sets of size N_{TR} and the space of all possible models with the

above-mentioned structure (n criteria and k categories) are randomly explored (again, notice that no use is made of the original real training set): the classification performance is obtained as an average over the possible random training sets (of fixed size) and random models (of fixed structure). Thus, the resulting accuracy estimate is a realistic indicator of the expected classification performance of an "average" model (of given structure) trained with an "average" training set (of given size). In the case study considered, the average assignment error (resp., accuracy) is around 30% (resp., 70%).

On the contrary, the bootstrap method uses the real training set available to build an ensemble of models compatible with the data set itself. In this case, we do not explore the space of all possible training sets as in the model-retrieval-based approach, but rather the space of all the classification models compatible with that particular training set constituted by real-world examples. In this view, the bootstrap approach serves the purpose of quantifying the uncertainty intrinsic in the particular (training) data set available when used to build a classification model of given structure (i.e., with given numbers n and k of criteria and categories, respectively). In this case study, the accuracy evaluated by the bootstrap method is much higher (equals to one) than that estimated by the model-retrieval-based approach: this is reasonable because the latter evaluates the accuracy on a wider (i.e., in a broad sense, more uncertain) space of possible models and training sets; on the other hand, in the former method the training set adopted is given and it represents possibly only one of those randomly generated within the model-retrieval-based approach. In addition, notice that differently from the model-retrieval-based approach, the bootstrap method does not provide only the global classification performance of the vulnerability model, but also the confidence that for each test pattern a class assigned by the model is the correct one: this is given in terms of the full probability distribution of the vulnerability classes for each alternative to be classified.

Finally, also the LOOCV method has been used to quantify the expected classification performance of the model trained with the particular training data set available. In order to maximally exploit the information contained in the training set D_{TR}, $N_{TR} = 1$ "reduced" (training) sets are built, each containing $N_{TR} - 1 = 10$ assigned alternatives: each "reduced" set is used to build a model whose classification performance is evaluated on the element correspondingly left out. The average error rate (resp., accuracy) turns out to be 18.2% (resp., 72.8%). The 95% confidence interval for the error rate (resp., accuracy) is approximately [0, 0.4099] (resp., [0.5901, 1]).

8. CONCLUSIONS

In this article, the issue of quantifying the vulnerability of safety-critical systems (in the example, NPPs) with respect to intentional hazards has been tackled within an empirical classification framework. To this aim an MR-Sort model has been trained by means of a small-sized set of data representing *a priori* known classification examples. The performance of the MR-Sort model has been evaluated with respect to: (i) its classification *accuracy* (resp., error), that is, the expected fraction of patterns correctly (resp., incorrectly) classified; (ii) the *confidence* associated to the classification assignments (defined as the probability that the class assigned by the model to a given [single] pattern is the correct one). The performance of the empirically constructed classification model has been assessed by resorting to three approaches: a model-retrieval-based approach, the bootstrap method, and the LOOCV technique. To the best of the authors' knowledge, it is the first time that:

- A classification-based hierarchical framework is applied for the analysis of the vulnerability of safety-critical systems to intentional hazards;
- The confidence in the assignments provided by an MR-Sort classification model is quantitatively assessed by the bootstrap method in terms of the probability that a given alternative is correctly classified.

From the results obtained it can be concluded that although the model-retrieval-based approach may be useful for providing an upper bound on the error rate of the classification model (obtained by exploring the space of all possible random models and training sets), the bootstrap method seems to be advisable for the following reasons: (i) it makes use of the training data set available from the particular case study at hand, thus characterizing the uncertainty intrinsic in it; (ii) for each alternative (i.e., safety-critical system) to be classified, it is able to assess the confidence in the classification by providing the probability that the selected vulnerability class is

the correct one. This is of paramount importance in the decision-making processes involving the vulnerability assessment of safety-critical systems, since it provides a metric for quantifying the "robustness" of a given decision.

APPENDIX A:

As described in Section 2, the hierarchical model developed in Ref. 14 is considered to analyze the vulnerability of NPPs to intentional hazards. The susceptibility to intentional hazards (first layer) is characterized in terms of attractiveness and accessibility (second layer). These are hierarchically broken down into factors that influence them, including resilience seen as preattack protection (which influences on accessibility) and postattack recovery (which influences on attractiveness); this decomposition is made in six criteria: physical characteristics, social criticality, possibility of cascading failures, recovery means, human preparedness, and level of protection (third layer). These six third-layer criteria are further decomposed into a layer of basic subcriteria, for which data and information can be collected (fourth layer) (see Table A1). The criteria of the layers are assigned preference directions for treatment in the decision-making process. The preference direction of a criterion indicates toward which state it is desirable to lead it to reduce susceptibility, that is, it is assigned from the point of view of the defender of an attack who is concerned with protecting the system. Although only the six criteria of the third level of the hierarchy are considered in the NPPs vulnerability analysis considered in this article, examples of evaluation of the basic subcriteria of the fourth layer are proposed in what follows for exemplification purposes: in particular, we describe an example of the procedure employed to calculate the numerical values of the third-layer criteria on the basis of the characteristics of the fourth-layer subcriteria.

In extreme synthesis, the subcriteria of the fourth layer can be characterized by crisp numbers or linguistic terms, depending on the nature of the subcriterion. These descriptive terms and/or values of the fourth-layer subcriteria are then scaled into numerical categories. The influence to the corresponding third-layer criterion of each of the subcriteria is analyzed.

To get the values of the six main third-layer criteria, (i) we assign arbitrary weights to each subcriterion and (ii) we apply a simple weighted sum to the categorical values of the constituent subcriteria.

A.1 Illustrative Example: Evaluation of the Criterion Physical Characteristics

The criterion "physical characteristics" is taken as an illustrative example. It is constituted by the subcriteria "number of workers," "nominal power production," and "number of production" or "service units." The description and category scales are presented as follows.

Number of Workers

This criterion can be seen to contribute to the attractiveness for an attack from various points of view, for example: (1) the more workers, the more work injuries and deaths from an attack; (2) the more workers, the easier for the attackers to sneak into the system; (3) the more workers, the higher the possibility that one of them can be turned into an attacker. Limiting the number of workers can, then, contribute to the security of the plant and, thus, reduce its attractiveness for an attack. Table A2 reports some reference values typical of NPPs.

Nominal Capacity

The higher the production capacity, the larger the potential consequences of lost production or security in case of an attack. Then, it is preferable to have a site with low capacity. Of course, for a fixed amount of total capacity needed, this would lead to its distribution on multiple sites, with an increase in the number of multiple targets, though each of them would lead to milder consequences if attacked. Table A3 shows some reference values of power generation capacity at NPP sites.

Number of Production or Service Units

Locally, within a single site, this criterion represents the number of potential attack points. Preference would go toward having a small number of targets on a site. Table A4 gives some reference values for NPPs.

We choose NPP x_1 as an example to show the calculation of the numerical value associated to the main criterion "physical characteristics" starting from the data relative to the three corresponding subcriteria (i.e., number of workers, nominal power production, and number of production or service units). The original data of the three subcriteria of x_1 are listed in Table A5.

Table A1. Criteria, Subcriteria, and Preference Directions

Criterion	Physical Characteristics	Social Criticality	Possibility of Cascading Failures
Subcriteria	Number of workers	Percentage of contribution to the welfare	Connection distance
	Nominal power production	Size of served cities	
	Number of production units		
Preference direction	Min	Min	Min
Criterion	Recovery Means	Human Preparedness	Level of Protection
Subcriteria	Number of installed backup components	Training	Physical size of the system
	Duration of backup components	Safety management	Number of accesses
	Duration of repair and recovery actions		Entrance control
	External emergency measures		Surveillance
Preference direction	Max	Max	Max

Table A2. Number of Workers

Level	Number of Workers
1	500
2	1,000
3	1,500
4	2,000
5	2,500

Table A3. Nominal Power Production

Level Level	Nominal Power Production
1	1,000 MWe
2	3,000 MWe
3	5,000 MWe
4	7,000 MWe
5	10,000 MWe

Table A4. Number of Production or Service Units

Level	Number of Production or Service Units
1	2
2	4
3	6

In scaling them onto corresponding category, we obtain the categorical value of alternative x_1 (Table A6).

Then, the numerical values of Table A6 are normalized (i.e., rescaled Between 0 and 1 based on the predefined scales) as shown in Table A7.

Table A5. Corresponding Subcriteria Original Data of Main Criterion Physical Characteristics of x_1

Alternative	Number of Workers	Nominal Power Production (MWe)	Number of Production or Service Units
x_1	600	1,000	2

Table A6. Categorical Value for the Subcriteria Corresponding to the Main Criterion "Physical Characteristics" of Nuclear Power Plant x_1

Alternative	Number of Workers	Nominal Power Production	Number of Production or Service Units
x_1	2	2	1

Table A7. Normalized Categorical Value for Corresponding Subcriteria of Main Criterion Physical Characteristics of x_1

Alternative	Number of Workers	Nominal Power Production	Number of Production or Service Units
x_1	0.4	0.4	0.33

Using the weights of these three subcriteria (arbitrarily assigned by the authors) in Table A8, we can apply a simple weighted sum to calculate the cumulative value for main criterion "physical characteristics": $0.4 \times 0.3 + 0.4 \times 0.5 + 0.33 \times 0.2 = 0.386$.

Finally, considering the preference directions of Table A1 (i.e., minimization for criterion "physical characteristics") and setting for each main criteria the value "0" as the worst case and "1" as the best

Table A8. Weights of Subcriteria for Physical Characteristics

Main Criterion: Physical Characteristics	Number of Workers	Nominal Power Production	Number of Production or Service Units
Weights	0.3	0.5	0.2

one, we convert the cumulative weighed value obtained earlier to its complement to "1," that is, $1 - 0.386 = 0.614$.

For the other five main third-layer criteria, the process of calculation is the same as for criterion "physical characteristics."

APPENDIX B: MATHEMATICAL DETAILS ABOUT THE ALGORITHM OF DISAGGREGATION OF AN MR-SORT CLASSIFICATION MODEL

We consider the case involving k categories that are, thus, separated by $(k-1)$ frontier denoted $b = \{b^1, b^2, ..., b^h, ..., b^{k-1}\}$, where $b^h = \{b_1^h, b_2^h, ..., b_i^h, ..., b_n^h, h = 1, 2, ..., k\}$, n is the number of criteria that are taken into account. Let $D_{TR} = \{(x_p, \Gamma_p^t), p = 1, 2, ..., N_{TR}\}$ be the training set, where N_{TR} is the number of alternatives, and $(A^1, A^2, ..., A^k)$ be the partition of the training set, ordered from the best to worst alternatives.

For each alternative $x_p \in D_{TR}$, in category A^h of the learning set D_{TR} (for $h = 2, 3, ..., k-1$), let us define $2n$ binary variables δ_{ip}^h and δ_{ip}^{h-1}, for $p = 1, 2, ..., N_{TR}$, such that δ_{ip}^l equals to 1 iff $g_i(x_p) \geq b_i^l$ for $l = h-1, h$ and $\delta_{ip}^h = 0 \Leftrightarrow g_i(x_p) < b_i^h$. We introduce $2n$ continuous variables $c_{ip}^l (l = h-1, h)$ constrained to be equal to ω_i if $\delta_{ip}^l = 1$ and to *0* otherwise.

We consider an objective function that describes the robustness of the assignment. We introduce two more continuous variables, y_p and z_p, for each $x_p \in D_{TR}$ and α. In maximizing α, we maximize the value of the minimal slack in the constraints.

We resume all the constraints in the following mathematical program:

$$max\ \alpha, \tag{A1}$$

$$\alpha \leq y_p, \alpha \leq z_p, \forall x_p \in D_{TR}, \tag{A2}$$

$$\sum_{i,p \in \mathbb{N}} c_{ip}^l + y_p + \epsilon = \lambda, \forall x_p \in A^{l-1}, \tag{A3}$$

$$\sum_{i,p \in \mathbb{N}} c_{ip}^l = \lambda + z_p, \forall x_p \in A^l, \tag{A4}$$

$$c_{ip}^l \leq \omega_i, \forall x_p \in D_{TR}, \forall i \in \mathbb{N}, \tag{A5}$$

$$c_{ip}^l \leq \delta_{ip}^l, \forall x_p \in D_{TR}, \forall i \in \mathbb{N}, \tag{A6}$$

$$c_{ip}^l \geq \delta_{ip}^l - 1 + \omega_i, \forall x_p \in D_{TR}, \forall i \in \mathbb{N}, \tag{A7}$$

$$M\delta_{ip}^l + \epsilon \geq g_i(x_p) - b_i^l, \forall x_p \in D_{TR}, \forall i \in \mathbb{N}, \tag{A8}$$

$$M(\delta_{ip}^l - 1) \leq g_i(x_p) - b_i^l, \forall x_p \in D_{TR}, \forall i \in \mathbb{N}, \tag{A9}$$

$$\sum_{i,p \in \mathbb{N}} \omega_i = 1, \lambda \in [0.5, 1], \tag{A10}$$

$$\omega_i \in [0, 1], \forall i \in \mathbb{N}, \tag{A11}$$

$$c_{ip}^l \in [0, 1], \delta_{ip}^l \in \{0, 1\}, \forall x_p \in D_{TR}, \forall i \in \mathbb{N}, \tag{A12}$$

$$y_p, z_p \in \mathbb{R}, \forall x_p \in D_{TR}, \tag{A13}$$

$$\alpha \in \mathbb{R}, \tag{A14}$$

M is an arbitrary large positive value, and ϵ an arbitrary small positive quantity.

The case in which x_p belongs to one of the extreme categories (A^1 and A^k) is simple. It requires the introduction of only n binary variables and n continuous variables. In fact, if x_p belongs to A^1 we just have to express that the subset of criteria on which x_p is at least as good as b_1 has sufficient weight. In a dual way, when x_p lies in A^k, the worst category, we have to express that it is at least as good as b_k on a subset of criteria that has not sufficient weight.

REFERENCES

1. Kröger W, Zio E. Vulnerable Systems. London: Springer, 2001.
2. Aven T. Foundations of Risk Analysis. NJ: Wiley, 2003.
3. Aven T. Some reflections on uncertainty analysis and management. Reliability Engineering and System Safety, 2010; 95: 195–201.
4. Aven, T. Misconceptions of Risk. Chichester, UK: Wiley, 2010.
5. Aven T, Heide B. Reliability and validity of risk analysis. Reliability Engineering and System Safety, 2009; 94:1862–1868.
6. Leroy A, Mousseau V, Pirlot M. Learning the parameters of a multiple criteria sorting method. Pp. 219–233 in Brafman RI, Roberts F, Tsoukias A (eds). The Second International Conference on Algorithmic Decision Theory, Algorithmic Decision Theory. ADT 2011, LNAI 6992. Berlin: Springer,2011.
7. Aven T, Flage R. Use of decision criteria based on expected values to support decision-making in a production assurance and safety setting. Reliability Engineering and System Safety, 2009; 94:1491–1498.

8. Milazzo MF, Aven T. An extended risk assessment approach for chemical plants applied to a study related to pipe ruptures. Reliability Engineering and System Safety, 2012; 99:183–192.
9. Rocco C, Zio E. Bootstrap-based techniques for computing confidence intervals in Monte Carlo system reliability evaluation. Pp. 303–307 in Proceedings of the Annual Reliability and Maintainability Symposium. IEEE, 2005.
10. Baraldi P, Razavi-Far R, Zio E. A Method for Estimating the Confidence in the Identification of Nuclear Transients by a Bagged Ensemble of FCM Classifiers. Las Vegas, NV:NPIC&HMIT, 2010.
11. Doumpos M, Zopounidis C, Multricriteria Decision Aid Classification Methods. Netherlands: Kluwer Academic Publishers, 2002.
12. NWRA. N. W. R. A. Risk Assessment Methods for Water Infrastructure Systems. Kingston, RI: Rhode Island Water Resources Center, University of Rhode Island, 2012.
13. Hofmann M, Kjølle G, Gjerde O. Development of indicators to monitor vulnerabilities in power systems. Presented at the 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012), Helsinki, Finland, 2012.
14. Wang T-R, Mousseau V, Zio E. A hierarchical decision making framework for vulnerability analysis. Pp. 1–8 in ESREL2013, Amsterdam, The Netherlands, 2013.
15. Roy B. The outranking approach and the foundations of ELECTRE methods. Theory and Decision, 1991; 31:49–73.
16. Mousseau V, Slowinski R. Inferring an ELECTRE TRI model from assignment examples. Journal of Global Optimization, 1998; 12:157–174.
17. Efron B, Thibshirani RJ. An Introduction to the Bootstrap. Monographs on Statistics and Applied Probability, Vol. 57. New York: Chapman and Hall, 1993.
18. Zio E. A study of the bootstrap method for estimating the accuracy of artificial neural networks in predicting nuclear transient processes. IEEE Transactions on Nuclear Science, 2006; 53(3):1460–1470.
19. Cadini F, Zio E, Kopustinskas V, Urbonas R. An empirical model based bootstrapped neural networks for computing the maximum fuel cladding temperature in a RBMK-1500 nuclear reactor accident. Nuclear Engineering and Design, 2008; 238: 2165–2172.
20. Baraldi P, Razavi-FraR, Zio E. Bagged ensemble of fuzzy C means classifiers for nuclear transient identification. Annals of Nuclear Energy, Elsevier Masson, 2011; 38(5):1161–1171.
21. Wilson R, Martinez TR. Combining cross-validation and confidence to measure fitness. Pp. 1409–1416 in Proceedings of the International Joint Conference on Neural Networks (IJCNN'99). Washington, DC: IEEE.
22. Gutierrez-Osuna R. Pattern analysis for machine olfaction: A review. IEEE Sensors Journal, 2002; 2(3).