Contribution to the demonstration of nuclear safety in a model-based engineering context : Methodological proposal

Emir Roumili

THÈSE POUR OBTENIR LE GRADE DE DOCTEUR DE L'INSTITUT MINES-TELECOM (IMT) – ÉCOLE NATIONALE SUPÉRIEURE DES MINES D'ALÈS (IMT MINES ALÈS)

En SYstèmes, Automatique et Micro-électronique

École doctorale I2S – Information, Structures, Systèmes portée par l'Université de Montpellier

Unité de recherche : Laboratoire des Sciences des Risques (LSR), IMT Mines Alès

Contribution to the demonstration of nuclear safety in a model-based engineering context: Methodological proposal

Présentée par Emir ROUMILI

le 07 décembre 2022

Sous la direction de Vincent CHAPURLAT
et de Nicolas DACLIN

Devant le jury composé de :

Christophe MERLO, Professeur des Universités, ESTIA LAPS	Rapporteur
Jean-Yves CHOLLEY, Professeur des Universités, ISAE-SUPMECA	Rapporteur
Robert PLANA, Chief Technology Officer, Assystem	Examinateur
Jean-François BOSSU, Ingénieur, Assystem	Examinateur
Jérôme TIXIER, Maitre-Assistant IMT Mines Alès	Encadrant
Nicolas DACLIN, Maitre-Assistant, IMT Mines Alès	Co Directeur de thèse
Vincent CHAPURLAT, Professeur, IMT Mines Alès	Directeur de thèse

COLLÈGE DOCTORAL UNIVERSITÉ DE MONTPELLIER

IMT Mines Alès
École Mines-Télécom

"I saw that no one ever wrote a book
without, on the following day, saying:
'Had such-and-such been changed
It would have been better;
had such-and-such been added
it would have been more acceptable;
had such-and-such been stated earlier
it would have been preferable;
and had such-and-such been omitted
it would have been more elegant.'

Such a phenomenon is one of the great lessons
and evidence of the inherent insufficiency
of all members of the human race."

al-Qādī al-Fadil 'Abd al-Rahim al-Bisānī al-'Asqalānī
Advisor and confidant of Saladin.
1131 - 1199

Acknowledgements:

With the end of this thesis work, it is important to thank the people who have marked this long adventure. To do so, I will start with the people without whom this thesis would not have been possible. I would like to thank Thierry DESPEYSSE for his great efforts to bring together the right stakeholders and initiate this reflection. Thanks to Jacques LEVESQUE for having chosen to start this work within the Assystem group.

I would then like to thank the people who were also initiators of this thesis as well as active contributors throughout these three years. Thanks to Vincent CHAPURLAT and Jean-François BOSSU who have never doubted since the beginning and have never stopped encouraging me even when I could have doubts. Thanks to Nicolas DACLIN and Jérôme TIXIER for their continuous efforts and their relevant contributions. Many thanks to Robert PLANA for being a sponsor of this work and for providing me with an adequate environment and relevant advice and actions to give this thesis a scope within the group and with the actors of the nuclear sector. Thanks also to Francesco VITILLO, my manager, who always wanted this work to take place in the best conditions. Thanks also to Elise BOURLOT and her teams who were able to provide me with the appropriate reflections and data about nuclear safety and application cases. Thanks to Aleksei IANCHERUK for his undeniable help with artificial intelligence. I would also like to thank Adrien GUERIN and El-Mehdi AZZOUZI for their wise advice and ideas on systems engineering and the potential links with nuclear safety.

A big thank you to Sofiane who did his summer internship with me and who was decisive and central in the development work. Thanks to Mehdi and Adem for their contribution to some elements of this work.

I also thank my two reviewers, Jean-Yves CHOLEY as well as Christophe MERLO who were able to immerse themselves in the thesis manuscript, understand its essence and propose very detailed reports which led me to look at the work with a new eye and will help in the development and continuation of the work presented below.

Finally, I cannot complete these thanks without mentioning my family. Special thanks to my wife for her patience and her constant support. I want to thank my son for the motivation he has given me. He was born at the beginning of this thesis and is celebrating his 3rd birthday and his first day of school at the same time as the ending of my PhD. I would also like to thank all my family for their support, especially my parents without whom nothing would have been possible. The result I can provide today is only due to the efforts they have been making since my birth. Thank you all!

Content

Table of figures

Glossary - Acronyms

ASN	French Nuclear Safety Authority
AADL	Architecture Analysis and Design Language
AAR	Automatic Reactor Shutdown
AEOS	Assystem Engineering and Operation Services
AFCEN	French association for the rules of design, construction, and monitoring in operation of nuclear boiler equipment
AI	Artificial Intelligence
API	Application Programming Interface
APR	Advanced Power Reactor
ARE	Normal power supply to the SG
ASG	Auxiliary water supply to the SG
ASG	Auxiliary power supply to the SG
ASME	American Society of Mechanical Engineers
BERT	Bidirectional Encoder Representations from Transformers
BESEP	Benchmark Exercise on Safety Engineering Practices
BPMN	Business Process Modeling Notation
CA	Expected Characteristics
CAE	Claim Argument Evidence
CEA	Atomic Energy and Alternative Energies Commission
DSML	Domain-Specific Modeling Languages
ED	Defined Requirements
EDF	Électricité de France - French Nuclear Operator
EPR	initially European pressurized reactor, renamed Evolutionary power reactor
EX	High level Safety Requirements
FPI	Interest Protection Functions
GCT	Global Turbine Bypass
GMPP	Primary Motor Pump Unit
HMI	Human Machine Interface
HPC	Hinkley Point C
I&C	Instrumentation & Control
IAEA	International Atom Energy Agency
IFOP	French Institute of Public Opinion
IIP	Important Item for Protection
INB	Basic Nuclear Installation
INSAG	International Nuclear Safety Group
IP	Important for Protection
IRSN	Institute for Radiation Protection and Nuclear Safety
IS	Safety Injection
ISMP	Safety Medium Pressure Injection

ISO	International Organization for Standardization
ITER	International Thermonuclear Experimental Reactor
KRT	Radioprotection measurement
MA	Measurement of Radioactivity
MBSA	Model Based Safety Analysis
MCC	Matthews Correlation Coefficient Formula
MCNP	Monte-Carlo N-Particle transport
MDTE	External Voltage Shortage
NLP	Natural Language Processing
OGS	Safety Global Objectives
ONR	Office for Nuclear Regulation
PCC	Operating Condition Studies
PCSR	Pre-Construction Safety Report
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
PZR	Pressurizer
RA	Reactor Off mode
RBS	Safety Borication Circuit
RCC	The Design and Construction Compendiums of Materials
RCV	Chemical and Volumetric Control of the primary circuit
REK	Repository of Knowledge and Expertise
RESRAD	RESidual RADioactive materials
REX	Return of EXperience
RGE	General Operating Rules
RIS	Primary circuit safety injection
SAFIR	Finnish research programme on nuclear power plant safety
SAUNA	Integrated safety assessment and justification of nuclear power plant automation
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SMART	Specific, Measurable, Achievable, Realistic and Time-related
SoI	System of Interest
SR	Safety Report
SRBS	Safety Requirements Breakdown Structure
SUTD	System Used To Do
VDA	Main Steam Relief Train
VIV	Steam Isolation Valve
VVP	Main steam circuit
WIP	Work In Progress
V&V	Verification and Validation

1 General Introduction

Reduced availability of water and food resources, impact on health in all regions of the world, reduction of the distribution areas of animal and plant species by half, are some of the current effects observed by the GIEC experts with global warming (+1.09 °C in 2021). The 2022 report also states that sustained efforts must be made in several sectors, in particular the energy transition in order to reduce CO2 emissions [1]. In line with these objectives of carbon neutrality by 2050, the choice of the nuclear industry is one of the energies put forward. France is a strong performer in this area, with nuclear power accounting for approximately 70% of its electricity production in 2019, or approximately 379.5 TWh. In comparison, the share of this energy in the world is only 10% with 443 reactors in 30 countries. [2] In addition to its reactor fleet, France wants to embark on an ambitious EPR construction program [3]. On the international scene, the industry is also seeing an expansion in construction, particularly of EPRs (China, England, Finland, India, etc.). Thus, this industry is identified as a key player in the energy transition. The high efficiency of this energy and its low CO2 emissions in kWh [4], [5] is leading more and more countries to consider nuclear energy as a viable option. [6] The confidence placed by the public in nuclear safety, the safety authorities and the IAEA are among the reasons that make it possible to consider this energy despite the few large-scale nuclear accidents in history. This high level of safety is not achieved without difficulties. Indeed, these major construction projects of these new types of reactors reach levels of safety and complexity never achieved. The various stakeholders involved in these projects also have high expectations. However, the collaboration of heterogeneous stakeholders with unshared usages and practices and different points of view does not make the task straightforward At the heart growing difficulty, the demonstration of nuclear safety aims to prove that the installation is designed, operated and dismantled without any consequences for humans and their environment. Without the proof of safety, the installation will never be able to start up, so it is important for the stakeholders involved to be sure that nuclear safety performs well and can fulfil its role. However, in the context of these multidisciplinary projects involving several organisations, the nuclear safety profession has an interaction with each of them. The latter have their own objectives related to their discipline but must facilitate the various technological choices that will ensure the safety of the installation. The complexity and volume of this heterogeneous data is increasing in these construction projects, thus classifying these issues as "big data". All this makes it difficult to conduct those nuclear safety demonstrations that ensure the confidence of all. The R&D work we present in this thesis aims to conceptualise, facilitate, formalise and therefore, to a certain extent, make more generic this key stage of the nuclear safety demonstration. It is part of a CIFRE thesis between IMT Mines Alès and the Assystem Engineering and Operation Services (AEOS) group.

The Risk Sciences Laboratory of IMT Mines Alès and, in particular, the Complex Systems Engineering for Risk Activities axis, works on the development of conceptual, methodological and technical aspects to support complex system engineering activities.

The Assystem Group has been involved in engineering, engineering assistance and the management of complex projects, including nuclear infrastructure, for over 50 years. It also operates in the fields of conventional energy, transport, industry and defence, with a presence in 15 countries in Europe, the Middle East, Africa and Asia. The group constitutes the 2nd largest independent nuclear engineering company in the world, and is notably present in the fields of safety, security, digitalisation and systems engineering. Its role is to support its clients in the design, construction supervision, commissioning, and operation of these facilities, with a particular focus on safety and performance. The group has recently focused its efforts on the development and deployment of digital tools to support engineering and the development of field service management solutions. All of this is aimed at providing so-called "more efficient" engineering in the context of the digital transition of the nuclear industry in particular.

This thesis therefore summarises the research and development of an approach combining principles, techniques, and tools from both Model-Based Systems Engineering and Artificial Intelligence.

The plan of this manuscript is as follows. We will start by placing our study in the context of nuclear safety, its definition, its regulatory texts as well as its different concepts and methods. We will then analyse in more detail the problems perceived in nuclear safety demonstration conducts. We will then continue with an analysis of the state of the art on the subject to understand the findings on these problems as well as the proposals for solutions by researchers in the field. Taking these proposals into account, we will present the choices we have made and the contributions that we have provided. We will then discuss these results and their limits. We will apply these contributions to two practical cases. We will conclude with a synthesis, followed by perspectives that we consider interesting for the possible continuation of our work.

2 Context

This section provides an overview of the field of nuclear safety to better define the issues and some simplifying and limiting assumptions adopted in this work.

2.1 Nuclear safety

Several definitions exist for nuclear safety. They may be issued by national or international bodies, in connection with the country's regulations, with operators or with safety authorities. However, two definitions emerge:

- At the national level, the French Nuclear Safety Authority (ASN) and the regulations (Article L.591-1 of the Environmental Code) define nuclear safety as: *"all the technical provisions and organisational measures relating to the design, construction, operation, shutdown and decommissioning of basic nuclear installations, as well as to the transport of radioactive substances, taken with a view to preventing accidents or limiting their effects".* [7].

This definition highlights technical and organisational concepts as well as the different phases of the life cycle of a nuclear installation. The Figure 1 [8] diagram shows the different phases of the life cycle of a nuclear installation and the main control phases. Similarly, the notions of incidents and accidents are clearly shown, as well as the need to prevent and/or mitigate them.

The IAEA defines safety as "the *achievement of correct operating conditions, prevention of accidents or mitigation of their consequences, resulting in the protection of workers, the public and the environment from industrial radiological hazards.*" [9].

This definition puts forward the notions of protection of workers, the public and the environment designated by the protection of interests in Article L. 593-1 of the Environmental Code: "*public safety, health and hygiene or the protection of nature and the environment*".

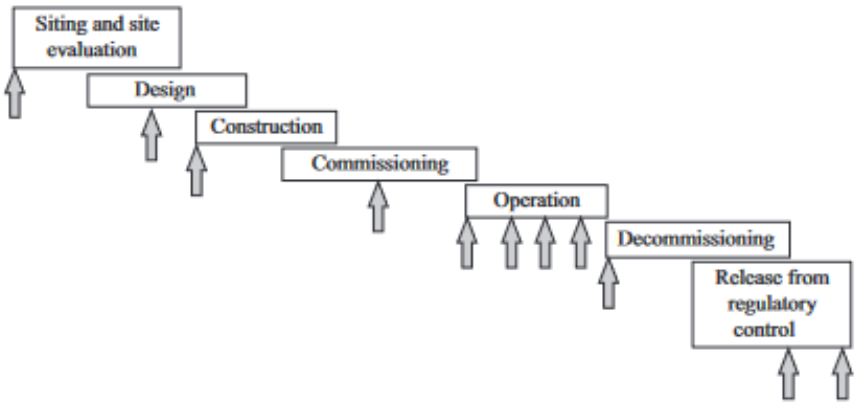


Figure 1 Generic implementation stages of a nuclear power plant project.

2.2 Nuclear Safety and its demonstration

The Order of 07/02/2012 [10] *"sets out the general rules for basic nuclear installations* (INBs) and incorporates international best practice [11]. It is one of the central elements of the French legislation dealing with nuclear safety.

In this respect, the order defines the **demonstration of nuclear safety** as *"all the elements contained or used in the preliminary safety report and the safety reports mentioned in Articles 8, 20, 37 and 43 of the aforementioned Decree of 2 November 2007 and contributing to the demonstration mentioned in the second paragraph of Article L. 593-7 of the Environment Code, which justify that the risks of accidents, radiological or otherwise, and the extent of their consequences are, taking into account the state of knowledge, practices and the vulnerability of the installation environment, as low as possible under acceptable economic conditions;"*

The IAEA Safety Glossary also defines a safety case as *"A collection of arguments and evidence in support of the safety of a facility or activity.*

These two definitions underline the crucial need to provide justifications for all the choices made in the design of the installation where there is a possibility of risks to the protection of the interests mentioned in section. 2.1. It is also mentioned that this demonstration is analysed in relation to the state of the art in the fields concerned while considering the economic aspect for the choices aimed at reducing the risks. The notion of arguments and evidence and the link with the "claims" (assertions) that we will introduce later are the basic elements of this demonstration.

It is therefore logical that the very notion of nuclear safety entails the need for a robust demonstration of the latter, a demonstration required by all stakeholders including the authorities in charge of applying the regulations and the operators of the installations concerned.

The importance given to the demonstration of nuclear safety is also part of the problem of this industry acceptance by the population. Recent debates on the place of nuclear power in the energy mix and the geopolitical context have led national opinion to look at the nuclear industry in a new light. Indeed, in a recent poll (September 2022) *"65% of French people say they are in favour of the construction of new reactors on national territory. This is an increase of 14 points in the space of a few months (51% last October), due to current events*. [12] It is added in this IFOP (French Institute of Public Opinion) study that *"the image that nuclear energy has among the French. 81% of the population consider it to be essential for France's energy independence, 71% consider it to be reliable, [...] Nuclear power has a rather positive image in the minds of the French, even if the risk posed by this sector remains very present in people's minds.*

This acceptance is reinforced by the level of safety achieved and by people's perceptions of the safety of the installations. This level of safety, which has been achieved and well demonstrated, constitutes a performance that the INB concerned must achieve in the same way as its other performances.

2.2.1 Body of regulatory text

The highest authority concerning nuclear industry is the country's nuclear safety authority. This authority must be independent [13] to ensure that it is not subject to political, operational, or other influence. In France, the ASN (Nuclear Safety Authority) issues several types of documents, some are mandatory, and some are recommendations. The ASN has responsibility on accepts on behalf of the state the demonstration of safety. It is therefore advisable to consider all the recommendations. In the figure below (Figure 2), the various documents issued in the context of the safety and linked to the nuclear safety demonstration.

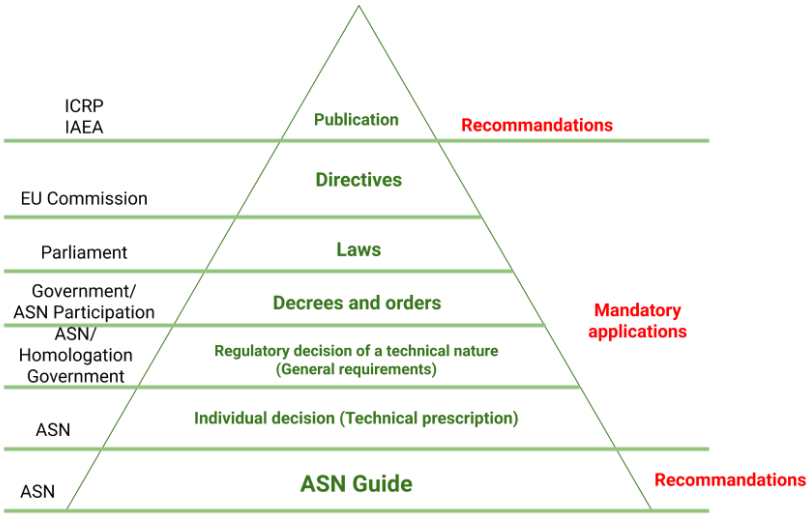


Figure 2 Body of regulatory text and their applications

The International Atomic Energy Agency (IAEA) is an international organization under the aegis of the United Nations seeking to promote the peaceful uses of nuclear energy and to limit the development of its military applications. In this role, the IAEA informs and publishes standards for the stability and safety of nuclear installations. These standards are recommendations, but since the IAEA is an extension of the safety authorities of the nuclear industry founding countries and is often adopted as a standard by nuclear industry emerging countries, their standards have a prominent place.

2.2.2 Introduction to the elements of nuclear safety

In order to understand the scope and the elements specific to the demonstration of safety, it is necessary to understand the safety report, which is the *"document drawn up by an operator, which presents the safety analysis of its installation and justifies the adequacy of the provisions adopted to meet the safety objective"* [14].

The preliminary version of this report will allow the issuing of an authorisation decree for the creation of the installation. The updated version will allow the issuing of the authorisation for the commissioning of the installation (licensing). It will evolve throughout the life of the installation (operation, dismantling etc.). This report therefore presents the safety provisions and takes the general form described in the Figure 3. The descriptive part aims at highlighting the elements of the installation, the site, the structure, the systems, their components, and the safety guiding principles applied to the design. The demonstration part requires to produce the results of several analysis studies that operate at several levels of scale. Finally, the issue of commissioning (elements linked to the commissioning of the installation, licensing, etc.) and decommissioning is considered from the outset and is reflected in this safety report.

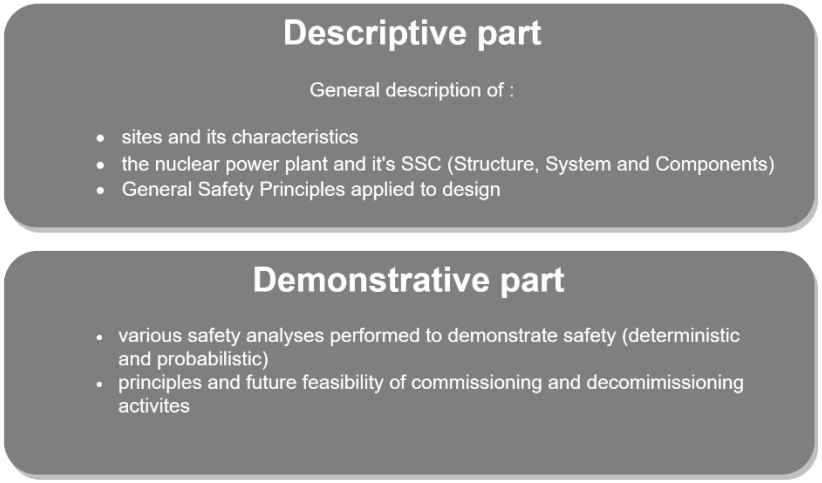


Figure 3 General parts of a safety report

In particular, the demonstrative part mainly uses two types of approaches:

- The deterministic approach: *"design provisions retained by the operator are justified by the study of a series of design basis accidents and by the application of rules and criteria that include margins and conservatisms*." [15]
- Probabilistic approach: *"risk assessment method based on a systematic investigation of accidental scenarios. They consist of a set of technical analyses that make it possible to assess the frequency of feared events and their consequences. From that we can obtain an overall assessment of the level*

of safety, integrating both the reliability of equipment and the behaviour of operators." [15]

As stated in the 2012 decree [11] *The nuclear safety demonstration* shall *be carried out using a conservative deterministic approach [...]. The nuclear safety demonstration shall also include, unless the operator demonstrates that it is not relevant, probabilistic analyses of accidents and their consequences.*"

The deterministic approach is supplemented by probabilistic studies but forms the basis of the demonstration. The deterministic approach is, in fact, privileged in our work.

2.2.2.1. General objective

The subject of nuclear safety has its peculiarities in relation to the history of the industry. The discovery of the power of this energy was accompanied by the realization of its dangerousness. This led to early consideration of the subject. With the development of the industry, nuclear safety has been developed in parallel, always aiming to reduce the risk according to the ALARA (As Low As Reasonably Achievable) principle. [16] This search for the safest possible level of safety begins with the principle of "justification", which questions the real interest of using nuclear materials (cf. radium phosphor materials built between 1918 and 1963 [17]). Nuclear safety is an integral part of the quality assurance of the design of nuclear facilities and this is now an ISO standard (evolution of ISO 9001): ISO 19443. [18]
The field of nuclear safety has thus been developed along with the industry to which it applies, with its own terminologies, concepts and processes, practices, etc.

The European Council Directive 2014/87/EURATOM of 8 July [19] refers in its Article 8 to the objective of nuclear safety: *"nuclear installations shall be designed, sited, constructed, commissioned, operated and decommissioned with the aim of preventing accidents and, in the event of an accident occurring, of mitigating its consequences and avoiding it:*

a) Early radioactive discharges that would require off-site emergency measures but without enough time to implement them;

b) Large-scale radioactive discharges that would require protective measures that could not be limited in space or time.

The general objective of the safety demonstration is the control of releases from the installation. The importance of this objective is well illustrated by the public's familiarity with Chernobyl and Fukushima accidents. The case of the Three Mile Island

accident is less well known because, in this accident, the third containment barrier (a concept discussed in section 2.2.2.3) was able to play its role in limiting radioactive releases from the facility.

In the following sections, we will discuss various concepts developed in the field of nuclear safety, explaining the elements of the Figure 4 as we go along. These concepts are fundamental to understanding the method that we will develop in the contributions (section 5).

2.2.2.2. Basic safety functions

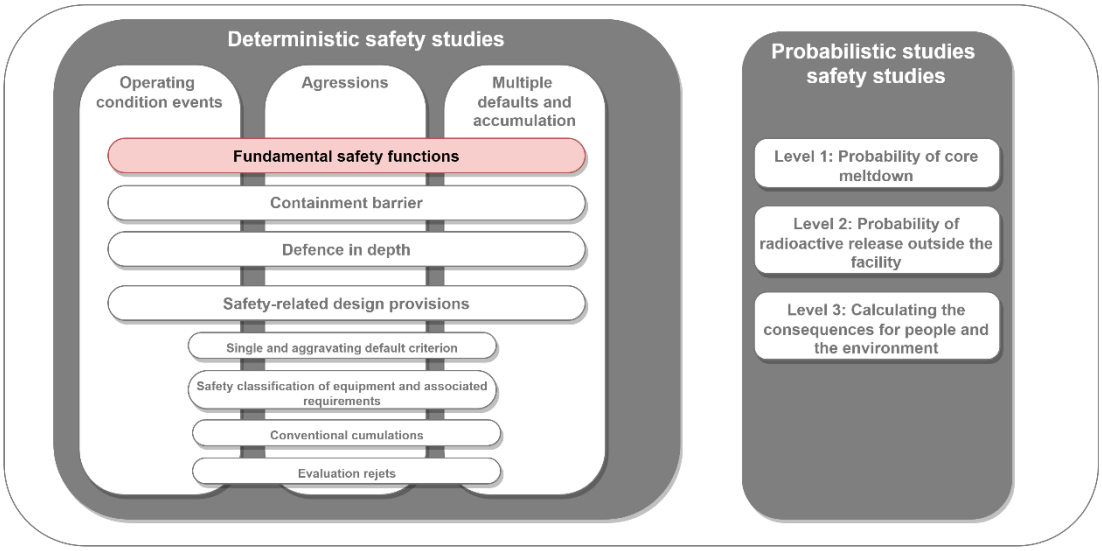


Figure 4 General diagram of nuclear safety concepts and fundamental safety functions

The specificities of the nuclear industry have led to the consideration of fundamental safety functions (cf. Figure 4) for the protection of man and the environment [10] :

- The control of the nuclear chain reaction: a subject mainly treated in the field of criticality.
- Thermal power removal: power from radioactive substances and nuclear reactions.
- Containment of radioactive substances: depending on the type of installation considered, these substances will be in various places.
- Protection of persons and the environment against ionising radiation: 4ème function added in the French regulation.

These functions must be provided in all possible states of the installation. They are also called "FPIs" or Interest Protection Functions.

2.2.2.3. Containment barriers

A barrier (cf. Figure 5) is a set of physical elements interposed between radioactive material, humans, and the environment. This concept has thus inspired in part the concept of defence in depth in the nuclear industry, described in the next section.

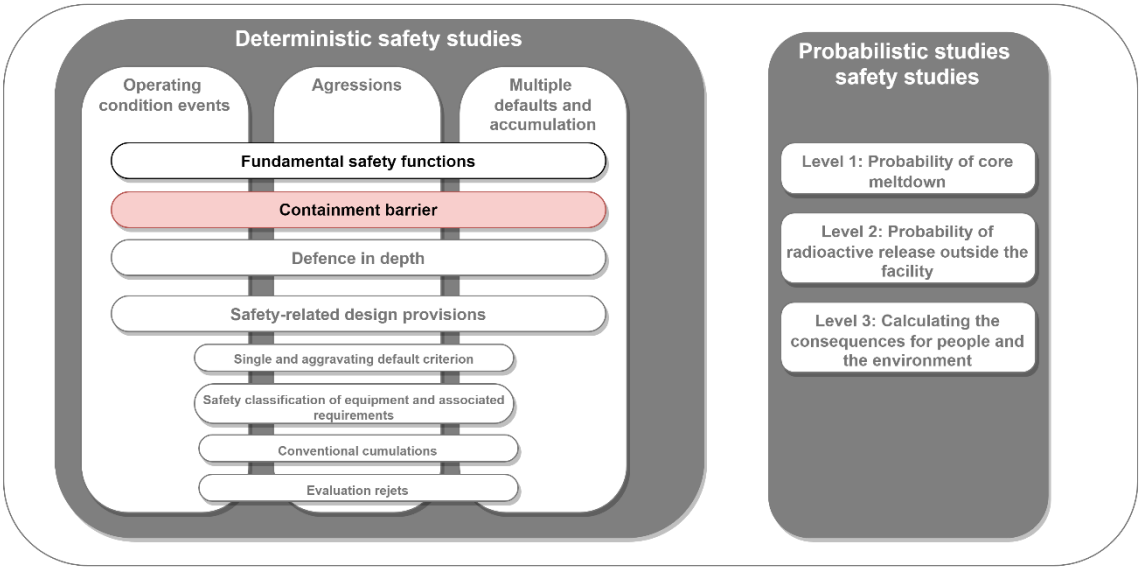


Figure 5 General scheme of nuclear safety concepts and containment barriers

The ASN thus defines a barrier as:

"In a nuclear reactor, the set of sealed devices interposed between the sources of radiation (fission products present in the reactor) and the outside environment in order to isolate the radionuclides in the fuel from the environment. [20]

These barriers, usually three or four in number, should be sealed and robust. [21]

For a reactor, there are three essential barriers (see Figure 6 [21]) :

- The fuel sheath;
- The primary circuit cladding (pressurised water circuit in the reactor vessel which heats up when in contact with the fuel);
- The containment (a sealed reinforced concrete building inside which the reactor vessel, the reactor core, the steam generators, and the pressuriser are located). This barrier can be extended to include certain circuits necessary to control the incident or accident.

The strength and tightness of these barriers are studied in the context of normal operation, normal INB transients and accidental transients. [21]

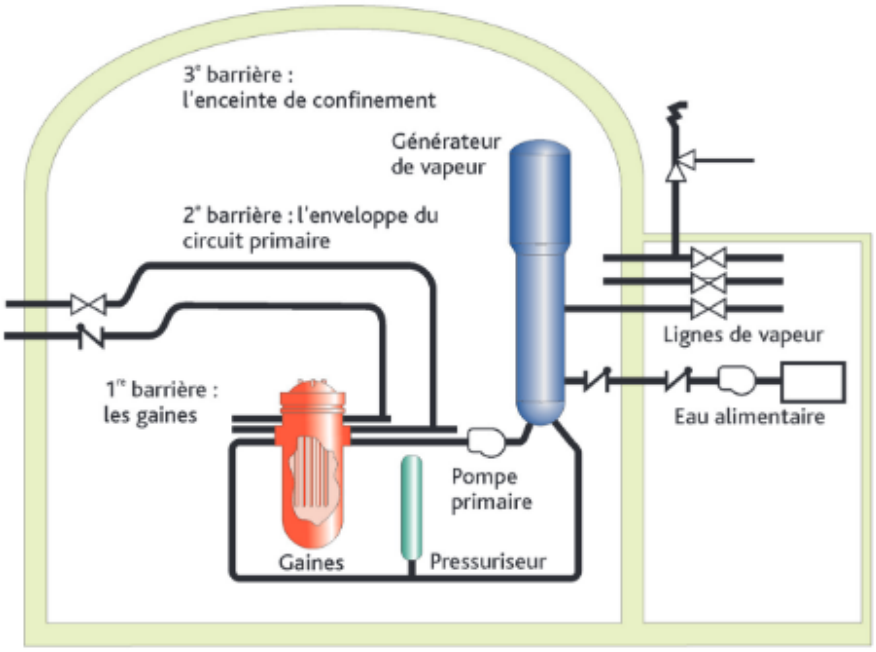


Figure 6 Containment barrier of a pressurised water reactor.

2.2.2.4. Defence in depth

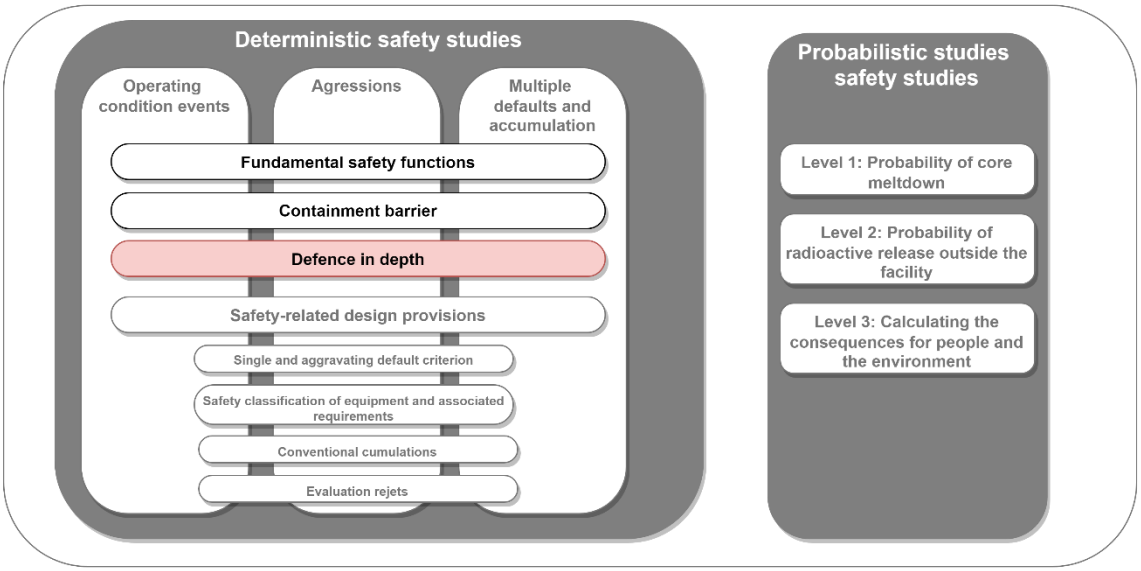


Figure 7 General diagram of nuclear safety concepts and defence in depth

A concept developed in the 1960s (cf.Figure 7) in the United States, and structured in the 1990s. IAEA defines this notion of defence in depth as: *"A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.*

This concept is also highlighted in the 2012 Order [11] :

"The operator shall apply the principle of defence in depth, consisting of the implementation of successive and sufficiently independent levels of defence.

This defence in depth is mainly based on the implementation of defence levels, particularly in the choice of materials, procedures, organisational and human resources. These levels retain an independence that ensures safety in the event of failure of one level. These levels are based on the "Swiss cheese" model of risk management developed by James Reason in association with the nuclear engineer John Wreathall and which has benefited mainly from research funds from the nuclear industry. [22] These levels are called strong lines of defence, the possible failure of which must then be considered by detailing more precise lines of defence at the levels of the sub-systems and components, devices and structures that make up the targeted INB (cf. Figure 8).

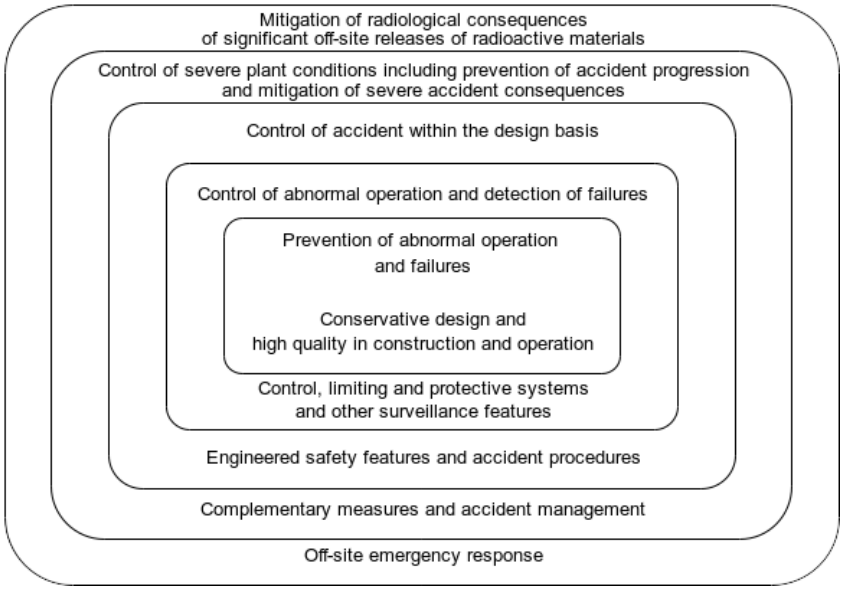


Figure 8 Levels of defence in depth

Defence in depth is structured around the levels recommended in the IAEA INSAG-10 report [23]. They are implemented in different ways depending on the country and the type of INB considered. These levels range from 1 to 5, from the prevention of an incident/accident (level 1) to the limitation of the consequences of an accident in relation to the general objective introduced above, which sets out the operator's commitment in the event of an accident or incident (level 5).

The instantiation of these levels in the French regulation is found in the 2012 order as follows [11] in article 3.1:

"prevent incidents;

- detect incidents and implement actions to prevent them from leading to an accident and to restore normal operation or, failing that, to achieve and maintain a safe state of the installation;

- Controlling unpreventable accidents or, failing that, limiting their worsening, by regaining control of the installation in order to bring it back to and maintain it in a safe state;

- to manage accident situations that could not be controlled in such a way as to limit the consequences, particularly for people and the environment.

The fifth level, dealing with crisis management in conjunction with the competent authorities, is not included in Article 3.1 but is found in Article 7.5 of the Order. These levels are more detailed in the guides (see regulatory pyramid, section 2.2.1) and in particular in guide 22 written by the ASN and the IRSN (Institute for Radiation Protection and Nuclear Safety) which details these levels for the design of pressurised water reactors.

2.2.2.5. Events considered and operating conditions

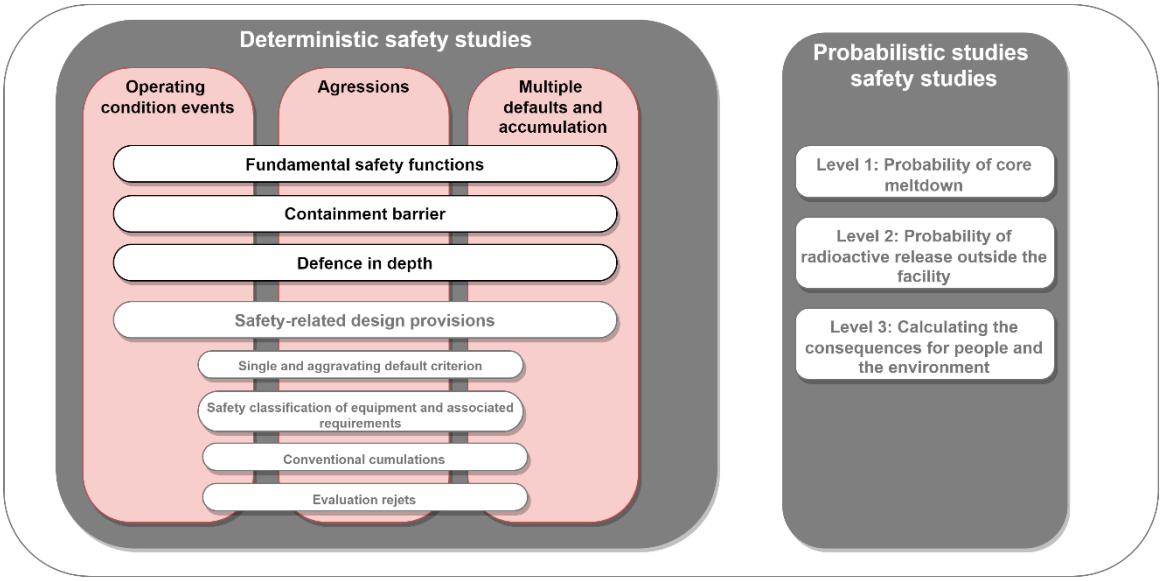


Figure 9 General scheme of nuclear safety concepts and events considered

The notion of event is at the heart of the nuclear safety demonstration. It is the basis of the deterministic approach. ASN Guide 22 [24] states that :

"The general approach to the design of the installation must be based on a prudent deterministic approach based on the principle of defence in depth supplemented by a probabilistic approach. It requires determining the events likely to affect a barrier or a safety function and then defining the provisions to be implemented in the installation to prevent these events and limit their consequences if they are plausible."

These events affect a barrier or a safety function. They are then considered to occur. The technical, organisational, and human provisions are established in the framework of defence in depth. The following levels will therefore be considered: prevention, detection, return to normal operation, control, mitigation and accident management.

Reference operating conditions

Among these initiating events, those related to an internal malfunction are considered. These events are numerous. It is necessary to structure them into groups according to common characteristics (safety functions affected, etc.). The most representative and conservative events (in terms of consequences) are analysed in the incidental and accidental scenarios they cause. This conservative group of events has the historical name in France of "design basis operating conditions" (or "reference

operating condition" in ASN guide 22 [24]). These groups of events are categorised according to the estimated frequencies as summarised in the Table 1, thanks to feedback from experience. Examples of these events are given in the Table 2.

Table 1 Classification of operating conditions

Categories of operating conditions	Order of magnitude of the estimated annual frequency of the initiator, per reactor
CATEGORY 1 Normal operating conditions	Number according to the operating programme.
CATEGORY 2 Minor but frequent incidents	Up to a few occurrences per year.
CATEGORY 3 Unlikely accidents	$10^{-4} < f < 10^{-2}$
CATEGORY 4 Hypothetical accidents	$10^{-6} < f < 10^{-4}$

Table 2 Examples of initiating events by category and safety function

Categories	Functions	Events
Category 2	Reactivity	Progressive uncontrolled dilution of boric acid
Category 2	Reactivity	Starting an inactive primary circuit loop
Category 3	Primary breaches	Loss of primary coolant through a small breach
Category 4	Releases of radioactivity	Fuel assembly handling accident

Consideration of aggression

In addition to considering internal initiating events specific to operation, hazards are considered. They are studied regarding the impact they may have on the equipment and therefore their ability to ensure the safety of the installation. Attacks are defined in ASN guide 22 as: *"Any event or situation originating inside or outside the basic nuclear installation which may directly or indirectly cause damage to elements important for protection or call into question compliance with the defined requirements.*

Attacks are divided into two types according to their origin:

- Internal: source of the aggression from within the installation (fire, etc.)
- External: source of the aggression coming from outside the installation (earthquakes, flooding, etc.).

To address this, a IIP is an "*Important item for the protection of interests [...]" i.e. any structure, equipment, system (programmed or not), material, component, or software [...] performing a function necessary for the demonstration [...] or controlling that this*

function is performed" [24]). It is understood from this definition that hazards are considered according to their impact on the elements of the installation that have been identified in the protection of safety functions in incidental and accidental states.
To protect IIPs, two strategies are used:

- Establish provisions to prevent the effects of the attack from reaching the equipment.
- Establish a design that qualifies the equipment for operation despite the aggression. This equipment must then be qualified for the type of aggression (seismic qualification, etc.)

We will therefore need:

1) An analysis of the characteristics of the aggression.
2) Its possible impact(s) on the installation, in particular on IIPs.
3) The demonstration of adequate protection of the latter.

Multiple defaults and accumulation

As mentioned in the section 2.2.2.5 For the reference operating conditions, the scenarios are derived from a single event. The study of multiple failures and situations involving core meltdown is also carried out in the context of a so-called "complementary event design". This field is included in the Design Extension Conditions (DEC) field and is described in ASN Guide 22:
"In order to achieve the objectives set out in Chapter II.1.2, provisions shall be implemented to:
- ensure the capability of the installation to cope with more complex or severe initiating events than those considered in the design basis domain;
- limit the release of radioactive substances into the environment during such events. The situations arising from such events constitute the extended design basis."

This complementary field includes:

- Internal events related to equipment:
    - DEC-A: Multiple equipment failures
    - DEC-B: Core Meltdown Situations
- Internal and external stresses that are more severe than those included in the basic design.

2.2.2.6. Deterministic and probabilistic approach

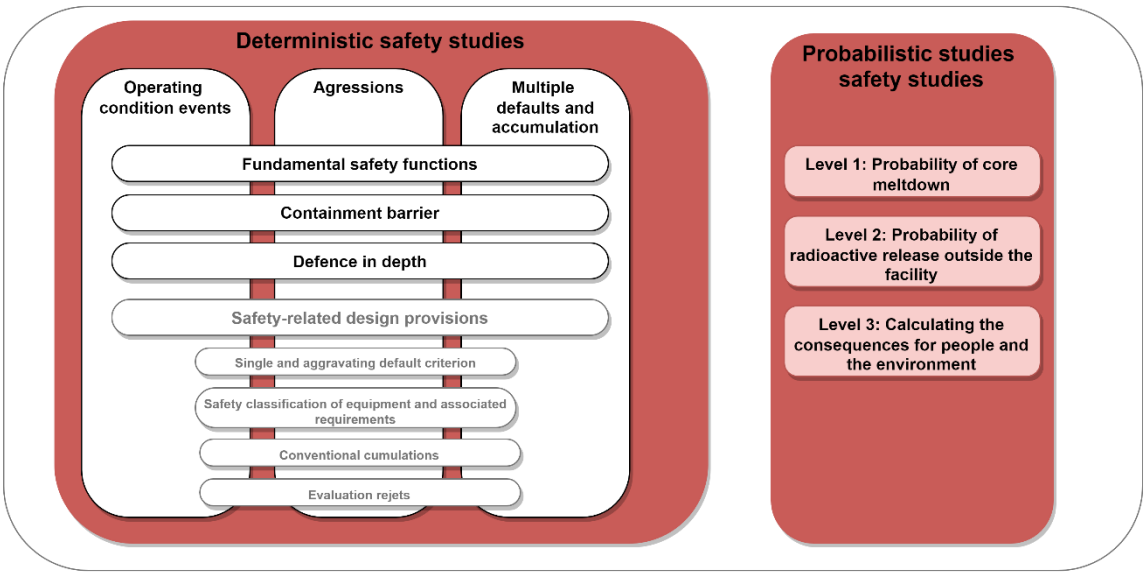


Figure 10 General outline of nuclear safety concepts: deterministic and probabilistic studies.

As mentioned above, both deterministic and probabilistic approaches coexist in nuclear safety analysis (cf. Figure 10). The deterministic approach is built based on the elements presented above. By assumption, events are considered to occur and the elements of each level of defence in depth (Part 2.2.2.4) will have to fulfil their mission and objectives. In the framework of probabilistic Safety Assessment (PSA), which are complementary to deterministic studies, the probability of occurrence of initiating events is analysed through analyses combining event trees of accidental scenarios with fault trees. Data about components is coming from manufacturers' databases and feedback from equipment in the field. These PSA studies are divided into 3 levels:

- Level 1: Analysis of the probability of core meltdown;
- Level 2: Analysis of the probability of radioactive releases outside the facility;
- Level 3: Analysis of the consequences for people and the environment.

2.2.2.7. Design provisions associated with safety considerations

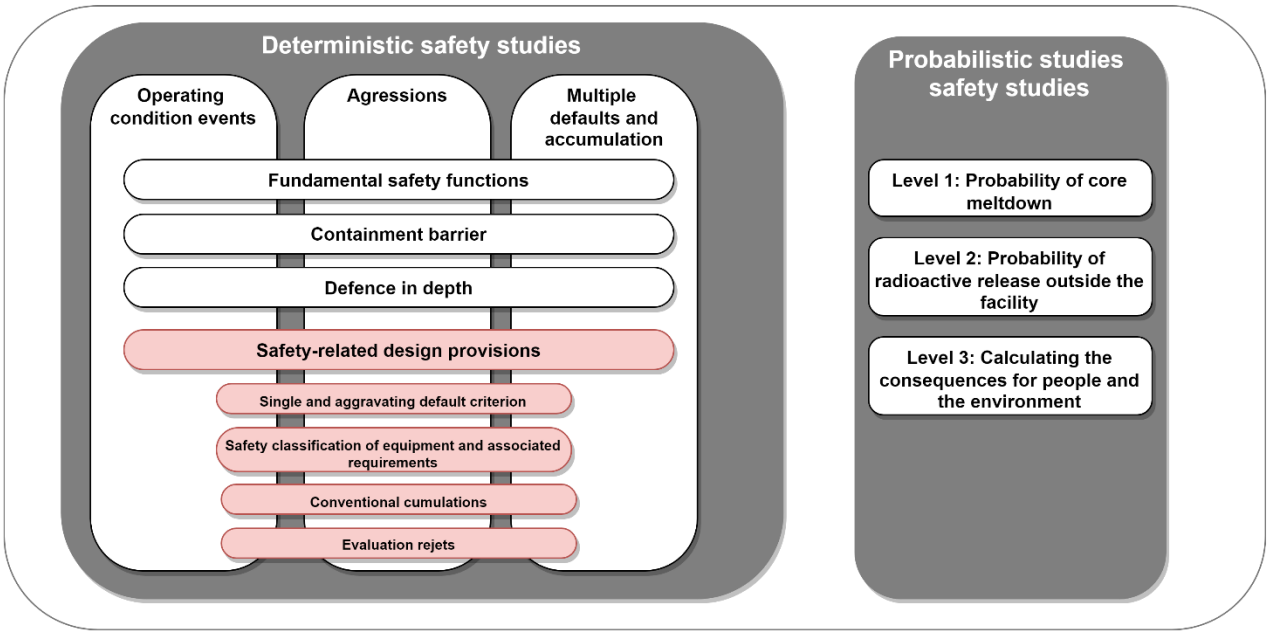


Figure 11 General scheme of nuclear safety concepts: design provision

After introducing the concepts on which nuclear safety is based, this chapter discusses various design provisions related to nuclear safety.

Single and aggravating failure criterion

This criterion is described in ASN Guide 22: *"The single failure criterion (SFC) is a deterministic design requirement applicable to certain IP* (Important for Protection) *systems; it introduces a requirement for redundancy and independence between the IP equipment of the IP system(s) that performs a safety function, with the objective of making the performance of that function more reliable. An IP system is designed according to the single failure criterion if it can perform its safety function despite a single failure in any of its equipment, the failure being independent of the event for which the IP system responds.*

It is a requirement to take a safety measure in a systematic way on equipment classified as IIP that performs safety functions. The single failure criterion aims to ensure that the function of the system will be fulfilled despite the failure of one of its components (RFS I.3.a [25]). In concrete terms, it will be considered that when the system is loaded, one of its components does not work. To be conservative, it is the component whose malfunctioning leads to the most serious consequences that is considered as

failing. This choice will of course depend on the state of the system under consideration.

The solutions to this problem have led to the requirements (cf. Figure 12) mentioned in the definition of the guide 22:

- Redundancy of the systems, each one being able to ensure 100% of the function (the consideration of hardware unavailability can lead to the presence of quadruple redundancy);
- System independence:
    - Attacks should not affect redundant equipment (made difficult by geographical distance);
    - Prevent simultaneous failures of identical or similar equipment (common mode failures).

It is also essential to consider the human factor in the analysis.

An "aggravator" is considered in the analysis of accident scenarios. The latter is a single failure that must be independent of the initiating event considered and the most penalising possible for the operating condition considered. For this reason, ASN Guide 22 states: *"The term 'single failure criterion applied to the nuclear safety demonstration' may be used instead of the term 'aggravator'".*

The Figure 12 illustrates safety features on which a consideration of the single failure criterion is based (separation principle, diversity principle etc.)

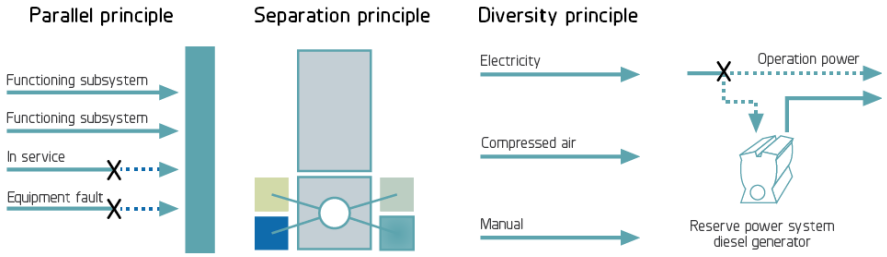


Figure 12 Safety features used for defence in defence-in-depth considerations [26]

Safety classification of equipment

The conduct of the studies as described (in a simplified manner) leads to the classification of equipment according to the roles they will have to play regarding the safety functions and the level of defence in depth considered (prevention, limitation of consequences, protection against aggression). The typology of the equipment is also considered [21] Mechanical, electrical, instrumentation & control (I&C), etc.

The concept of safety class also facilitates design. Generic requirements are established according to the class and are of increasing constraint for the design of the equipment according to the level of safety to be provided for the equipment.

For the example of the EPR case, the safety classes reflect the importance of the safety function that the systems perform (functional classification) and the importance as a containment barrier of the consequences of a failure in terms of release (mechanical classification). Other classification typologies also exist. (Mechanical, electrical etc.)
In the case of mechanical classification and in connection with the notion of barrier we find [27] :

- Class M1: main primary circuit;
- Class M2: equipment or parts of circuits which are intended to operate in situations where a primary liquid may flow but the integrity of the fuel sheaths is not guaranteed (e.g. safety injection);
- Class M3: Other classified mechanical equipment or parts of mechanical circuits not falling within the considerations of classes 1 and 2.

Generic requirements associated with the different safety classes

Generic requirements are associated with the different classes of equipment. All classified equipment will have a common base of requirements reflecting the robustness of the design of the equipment. The higher the classification, the higher the design requirements reflecting a high level of reliability. These requirements were initially derived from American codes, e.g. ASME (American Society of Mechanical Engineers) codes, but are tending to be replaced by the French design and construction codes of AFCEN (French association for the rules of design, construction and monitoring in operation of nuclear boiler equipment).
Material Design and Construction Compendiums (RCC) exist for several areas:

- RCC-M for the mechanical field.
- RCC-E for the electrical and I&C field.
- RCC-C for nuclear fuel.
- RCC-CW for civil engineering.
- RCC-F for fire.

The Hinkley Point C EPR (Evolutionary Power Reactor) Pre-Construction Safety Report (PCSR-3 [28]) specifies, for example, the link between equipment classification and the accepted design code in terms of component requirements (see Figure 13).

	Component safety class	Robustness against LOOP	Robustness against earthquake	Qualification for accident conditions	Component Requirement	Design code	Level of quality
	Pressure retaining mechanical						
See section 7.4.3	1	Assigned from SFG			M1	RCC-M1	Nuclear quality
					M2	RCC-M2 or equiv[13]	
					M3	RCC-M3	
	2				M2	RCC-M2 or equiv[12]	Nuclear quality
					M3	RCC-M3	
	3				M2	RCC-M2 or equiv[12]	Industrial or nuclear quality
					M3	RCC-M3 or equiv[14]	
					NR	HES[15]	

Figure 13 Mechanical classification of components and level of requirements

Conventional events cumulations

As mentioned in section 2.2.2.5, events cumulations are not supposed to be part of the basic design domain. However, some events cumulations are considered. In the case of the 4th category of events (cf. Table 1), the event is cumulated with the "external voltage shortage" (MDTE) in case it would be penalising for this transient. This conventional cumulation is historically linked to the study of scenarios involving large category 4 breaches with the occurrence of earthquakes that result in the loss of transmission lines. In line with what has been discussed for the single failure criterion, each of the redundant transmission paths will need to be supported by an earthquake qualified backup diesel. An approach integrating the criteria considered for the 4th category for the analysis of the relevance of this accumulation and its analysis for the 2nd and 3rd category events is considered. This approach has been repeated in the design of the EPR.

Evaluation of releases

Finally, as mentioned at the beginning of our general presentation of the methodology required in nuclear safety, the assessment of the releases from the installation is a key element of the demonstration. This assessment is an essential element in achieving the overall objective of the nuclear safety demonstration.
The steps for conducting this assessment are as follows:

- Assessment of the nature and quantities of radioactive substances in the installation (core, circuits, pool etc.);
- Release rate of these substances depending on the situation.
- Methods of transfer and deposition of radioactive substances in the installation;
- Leakage rate to the outside atmosphere and corresponding filtration;
- Duration of rejects and emission height.

These steps are carried out using pessimistic assumptions as mentioned in the 2012 decree [11]: *"the assumptions used to calculate releases must be reasonably pessimistic and the exposure scenarios must be based on realistic parameters without, however, taking into account any actions to protect the population that may be implemented by the public authorities".*

This release study is consistent with the study rules introduced for the deterministic analysis (aggravating etc.). The assumptions made for the installation are those described in the safety report in terms of requirements (requirements, classification of systems, etc.) and the general operating rules for the installation ("*The RGE (General Operating Rules) are a collection of rules approved by the ASN which define the authorised area of operation of the installation and the associated operating requirements").* [29]

2.2.3 Perceived issues in conducting projects including nuclear safety demonstrations.

It is important to understand that the safety of the installations considers the best safety practices in the state of the art of the design period, which is regularly reviewed after the commissioning and during the periodic re-evaluations of the installation every 10 years. The level of safety must be as high as the level of scientific and technical progress etc. permits. In this context, this safety demonstration is complex in its scope and in the perimeter it covers. In the case of a nuclear reactor, there are more than 50 buildings, 500 km of piping, 500,000 components and more than 100 million units of data (requirements, reports, diagrams, etc.). Also, as time goes on, the complexity of the projects increases. However, this demonstration of safety is encapsulated in industrial projects that must meet the constraints of [30] quality and time constraints (scope, resources, budget, etc.).

This demonstration is by its very nature based on collaboration between stakeholders who are responsible for highly complex, heterogeneous areas ranging from mechanical engineering to operator psychology. It is based on collaboration and iteration to design the safest possible installation. Despite this objective, a document-centric approach is used to carry out this work.

After presenting the context of our study and the principles of nuclear safety, the following section provides an in-depth analysis of the issues surrounding the conduct of nuclear safety demonstrations. We have identified the root causes of these problems, which we will call "barriers".

3 Problematic

3.1 Observations and direct or indirect effects of the current conduct of nuclear safety demonstrations.

There are several findings at the origin of potential unwanted effects when performing any nuclear safety demonstration, including:

- The lack of time in nuclear safety projects.
- The difficulty in having the overall vision necessary in a global installation safety demonstration process.
- The possible cost drift, or even the stopping of a project due to a lack of efficiency in the conduct of this demonstration.
- The possible lack of quality and confidence of certain studies that could lead to refusal of licensing (refusal to continue for an installation towards the operating phase by the ASN). Also, the confidence that is placed in these studies and the elements put forward.
- The large amounts of data considered in conducting the studies.
- A separation between engineering and safety, which remain effectively the work of different actors by definition, by habit and by usage in the nuclear field as in other fields.

There are many causes for these observations. We can mention the multi-disciplinary nature of the teams and the different objectives of each of them, the complexity of the installations and the lack of a common vocabulary in relation to the demonstration of safety. Also, the use of a document-oriented approach does not help to solve these problems, on the contrary it catalyses them [31].

Therefore, we will observe several effects to this type of conduct of nuclear safety demonstrations (document oriented, multidisciplinary team etc.). These effects are multiple but in general they lead to two main elements that are of concern for the nuclear industry:

- The increase in the time spent on studies, the value of time being correlated with the financial aspects, there is therefore an explosion in costs.
    - If we consider the case of the Flamanville EPR [32] the delay is now 10 years and the cost has been multiplied by more than 3 (from 3.3 billion to about 11 billion euros, without

considering the additional cost linked to the repair of the welds, possibly estimated at 1.5 billion euros).

- The stopping and abandoning of certain projects following several feasibility studies and therefore having incurred often significant costs.
    - Of course, the first consequence is often the cause of the second. Indeed, the longer projects are delayed, the greater the likelihood that they will be abandoned.

Other consequences may follow in projects, where methodologies and tools are not adapted to deal with complexity. We have illustrated this increasing complexity in safety studies through our introduction to nuclear safety in chapter 2.2.2 and the issues in chapter 2.2.3. For example, higher turnover rates leading to the loss of key resources for successful projects.

3.2 Barriers

In terms of identified barriers, we agree with the work [33] which lists some of the following elements, which we have restructured into 4 categories; conceptual (what are the origins of problems in terms of concepts, principles and basics?), methodological (what are the origins of problems in terms of processing?), technical (what are the origins of problems in terms of tools, techniques and other technical means?) and organisational/human (what are the origins of problems in terms of human skills and profile of competence, expectations. And how organizing the whole?).

3.2.1 Conceptual

Among the conceptual barriers related to the conduct of the safety demonstration are

- Lack of agreement on common terminology in relation to the demonstration of nuclear safety
- Definition of elements strongly present in safety such as:
    - Requirements,
    - Safety argumentation (CAE framework [34])
- How to link the nuclear safety demonstration to the design of the installation?
    - The work on this topic (called "Golden Thread" in the English regulation) aims to obtain a complete view on safety in a way that is efficient and traceable. [35] in the English regulation) aims to obtain a complete view of safety in a way that is efficient and traceable. The English government

website states that *"the golden thread will have to be kept in a digital format".*

3.2.2 Methodological

The methodological barriers we are considering are the following:

- How to facilitate communication between stakeholders?
- How to facilitate collaboration between different domains?
- How to conduct the safety demonstration?
- How to integrate nuclear safety into MBSE models as a viewpoint?
- How to have a traceability of safety requirements?
- Lack of clear vision in the standards of the methodology to adopt.
- Scattered information, fragmented documentation.
- How can AI help on nuclear safety demonstration?

3.2.3 Techniques

The technical barriers are as follows:

- How can the tools/techniques enable the lifting of these barriers?
- What tools can be used to integrate the approach to both the safety demonstration and the design in order to have an integrated approach to safety in the project.
- What type of AI is to be considered for nuclear safety tasks?

3.2.4 Organisational and human

Finally, at the organisational and human level, here are the barriers considered:

- Document-oriented work.
- Volume of data considered.
- Lack of staff with multi-disciplinary experience and a global vision.
- Financial: lack of money to make the budgetary drift of projects acceptable.
- Psychological: difficulty of cognition of complexity in a "document-oriented" project context.
- Usage: reductionism in engineering which prevents the adoption of the understanding postures of other disciplines, and which is not facilitated by the document-oriented approach.

- Ethics: nuclear demonstration often leads to mistrust by default because of past accident records, leading to increased rigor in this field.

3.3 Assumptions

In this section, we will explain the assumptions made based on the introduction to nuclear safety in section 2.1 and the general scheme of nuclear safety concepts introduced (Figure 14.).

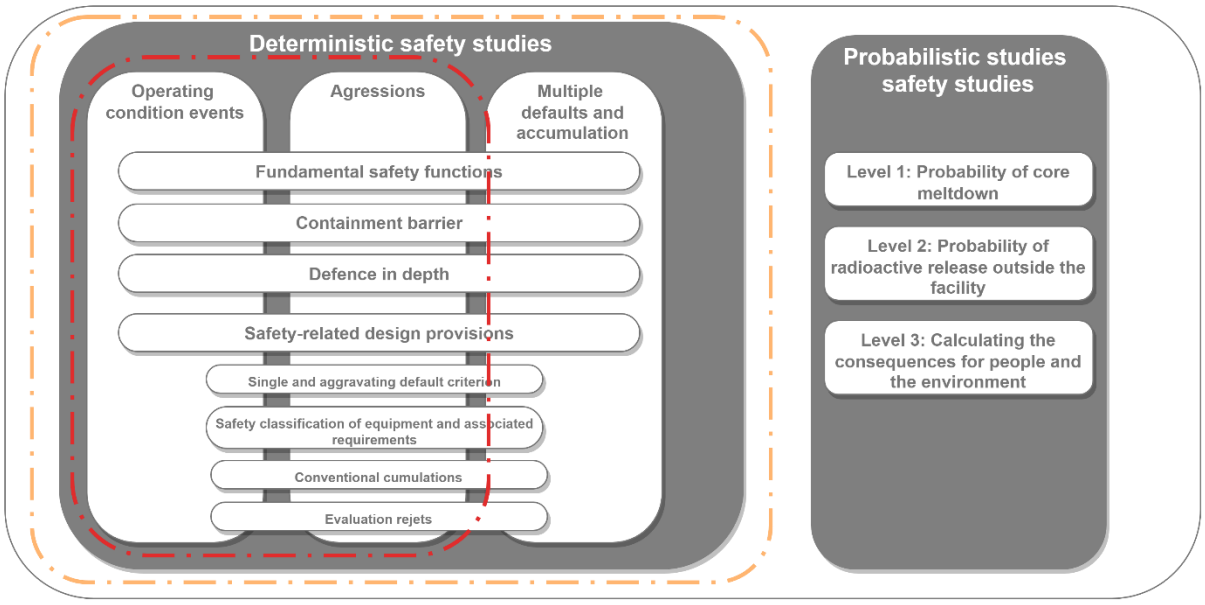


Figure 14 Simplified scheme of the concepts of nuclear safety demonstration and the scope of our study

The following assumptions were made:

- Assumption 1: The work proposed in the following focuses on deterministic studies of the nuclear safety demonstration (in orange in the Figure 14) as this form the basis of the nuclear safety demonstration.

- Assumption 2: In the deterministic approach, research work has focused on design basis topics (in red in the Figure 14), thus excluding non-conventional accumulations and analyses of severe accidents (non-dimensional analyses). This choice was motivated by the lack of time and the need to lay the foundations of nuclear safety concepts. These elements can be extended in later work.

The first part aimed at setting the context of our study and introducing the broad field of nuclear safety. This allowed us to understand that this field has its own concepts, terminologies, methods and has developed along with the industry for many years. In a second step, the issues related to nuclear safety were identified and the barriers were drawn up. We have classified these barriers into four main groups: conceptual, methodological, technical, organisational, and human barriers. In the rest of this work, we will analyse what other works on these problems have put forward to solve them. We will try to identify a space for potential solutions.

4 State of the art

4.1 Choice of elements

This part constitutes our analysis of the state of the art of the proposals about the demonstration of nuclear safety in relation to the barriers cited in the section 0. The proposals seem to converge towards a proposal to digitalise this demonstration. The literature refers to the concept of "digital safety case". This digitisation is mainly related to the disciplines of MBSE and Artificial Intelligence. This analysis has allowed us to understand precisely what exists and to direct our work towards the elements that have been successful in order to abandon those that do not seem to be conclusive. However, work on the specific subject of coupling MBSE and Nuclear Safety Demonstration is quite rare. In this chapter, we will position these works and comment on them in the light of the objectives set in our work. The division chosen in this section is that of our groups of barriers identified in the previous section. We thought it wise to focus on work that at least links MBSE and nuclear safety, or AI and nuclear safety. Each of these fields taken independently has an abundant literature that would not necessarily be relevant to the objectives set.

4.2 Barriers considered

The following table shows the barriers considered in our work.

Table 3 Barriers considered

Type of barrier	N°	Barrier
Conceptual	1	Lack of agreement on common terminology in relation to the demonstration of nuclear safety
	2	Definition of elements strongly present in safety such as: Requirements, Safety argumentation (CAE framework [34])
	3	How to link the nuclear safety demonstration to the design of the installation?
Methodological	4	How to facilitate communication between teams?
	5	How to facilitate collaboration between different domains?
	6	How to conduct the safety demonstration?
	7	How to integrate nuclear safety into MBSE models as a viewpoint?
	8	How to have a traceability of safety requirements?

	9	Lack of clear vision in the standards of the methodology to adopt.
	10	Scattered information, fragmented documentation.
	11	How can AI help on nuclear safety demonstration?
Technical	12	How can the tools/techniques enable the lifting of these barriers?
	13	What tools can be used to integrate the approach to both the safety demonstration and the design to have an integrated approach to safety in the project.
	14	What type of AI is to be considered for nuclear safety tasks?
Human and Organisational	15	Document-oriented work
	16	Volume of data considered.
	17	Lack of staff with multi-disciplinary experience and a global vision
	18	Financial: lack of money to make the budgetary drift of projects acceptable.
	19	Psychological: difficulty of cognition of complexity in a "document-oriented" project context.
	20	Usage: reductionism in engineering which prevents the adoption of the understanding postures of other disciplines, and which is not facilitated by the document-oriented approach.
	21	Ethics: nuclear demonstration often leads to mistrust by default because of past accident records, leading to increased rigor in this field.

4.2.1 Conceptual barriers

In this section, the work that has provided information on these barriers will be summarised. We remind you of these barriers in the Table 4.

Table 4 Conceptual element barriers

Type of barrier	N°	Barrier
Conceptual	1	Lack of agreement on common terminology in relation to the demonstration of nuclear safety
	2	Definition of elements strongly present in safety such as: Requirements, Safety argumentation (CAE

		framework [34]
	3	How to link the nuclear safety demonstration to the design of the installation?

These barriers relate to what has been termed "Conceptual". It seems important to have a definition of each of the terms and concepts specific to the field of nuclear safety to integrate them into a SE method and to create, in the long run, the basis of a common and shared vocabulary supposed to be consensual. By choice in the framework of this work, the definition of each concept implies to give a unique definition and to integrate it into a rigorous metamodel in which it will then be put in relation with other concepts. This approach makes it possible to prepare an ontological support for safety demonstration in the nuclear domain.

Among the simple definitions that have been made of nuclear safety concepts (Linosmaa) [36] attempts to define the terms "safety case", "safety demonstration", "structured safety demonstration". Subsequently, within the framework of the SAFIR (Finnish research programme on nuclear power plant safety) 2018 programme, several definitions of these concepts are provided through the report "Conceptual model for safety requirements specification and management in nuclear power plants". [37]. In this report, an introduction is given to the problem of safety requirements and the importance of having clear terminology. Indeed, depending on the stakeholder considered, the same terms will not have the same meaning and will be part of their own objectives. The importance of the notion of view and viewpoint in the definition of requirements (Safety requirements, Operational requirements, etc.) is therefore mentioned. A first metamodel/mindmap of 13 concepts is proposed to introduce the concepts to be considered if safety modelling for installations is undertaken. It includes the concepts of "Safety requirements", "Hazard", "PIE" (Postulated Initating Event). The notion of class (important in our work) is also introduced for the specific case of I&C systems. The SAFIR programme aims to improve nuclear safety approaches in the Finnish context (a follow-up to a previous programme: SAFIR 2014). The work of Valkonen et al. [38] "Safety demonstration of nuclear I&C" also helps with the present semantic blurring (safety cases, safety demonstration etc.). The interest of this work lies in the link with ISO 15288 [39] in order to take a step back on the specificity of the demonstration and to connect it with the standards of other industries. Also, the approach is more rigorous in its linking of safety concepts with those of the life cycle of a system (ISO/IEC 15288 [39]). Some of the contributions shed light on the issues to be considered in nuclear safety modelling. For example, "Demonstrating and arguing safety of I&C systems - challenges and recent experiences" [33] published at NPIC&HMIT (a conference specialising in I&C for the nuclear industry). In the latter, the authors analyse several interviews conducted with nuclear industry regulators

across several countries by the Institute for Energy Technology Norway (IFE) through the Halden Reactor Project (HRP). The lack of clarity in terminology is identified as a blocking point, as well as the clear definition of the terms "requirements", etc. In the same line, [40] highlights this problem of terminology. We find in the Conformity assessment data model work [41] definitions around some safety concepts that are provided at the beginning of the report. The concepts of requirements, claims and qualifications are developed in this work. Also, although the work is done for one requirement, the objective of the work is to prove the interest of linking and even simulating the respect of a requirement for a design element. Of course, the concrete application for all types of requirements and for the high volume of requirements remains a complex issue. The reflection on the integration of nuclear safety in architecture models is taken up in [42] through the application of AADL (Architecture Analysis and Design Language) modelling in order to analyse at early stages of the design the I&C choices on safety aspects. The application case is an APR-1400 system (Korean PWR licence currently under licensing for the Baraka plant in the United Arab Emirates). This idea is briefly mentioned in [43] through the need to integrate safety into the design "models" of the plant.

In conclusion, the work we have highlighted on the conceptual contribution of nuclear safety integration proves that the need is present and necessary. However, the work only considers a few concepts and is limited to the field of I&C. The modelling approach present in industrial computing may explain this limitation to the field of I&C.

4.2.2 Methodological challenges

In this section, the work that has provided information on these barriers will be summarised. We remind you of these barriers in the Table 5.

Table 5 Methodological barriers

Type of barrier	N°	Barrier
Methodological	4	How to facilitate communication between teams?
	5	How to facilitate collaboration between different domains?
	6	How to conduct the safety demonstration?
	7	How to integrate nuclear safety into MBSE models as a viewpoint?
	8	How to have a traceability of safety requirements?
	9	Lack of clear vision in the standards of the methodology to adopt.
	10	Scattered information, fragmented documentation.
	11	How can AI help on nuclear safety demonstration?

In the previous section, we stressed the importance of a clear definition, if possible, through a rigorous metamodel, of the concepts of nuclear safety. The issues highlighted here concern methodology. Several issues arise when conducting nuclear safety studies. They are integrated into complex projects with heterogeneous stakeholders. The fields are not the same, but the nuclear safety profession must guarantee the safety level of the installation. The issues of communication, effective collaboration, traceability, global and detailed vision of the project are not effectively dealt with by document-oriented project management. The above-mentioned report of the SAUNA project (Integrated safety assessment and justification of nuclear power plant automation) [38] and [40] considers the importance of systems engineering standards for the conduct of safety demonstrations. Thus, the elements of collaboration and communication are considered important. Demonstration work is also paralleled by qualification processes. The strong contribution of this work lies in the link made with systems engineering (although it is introductory). However, it is unfortunate that the MBSE is not mentioned. It should be noted that in this barrier, the focus is on standards from the nuclear field, which are numerous, and it is not always easy to have an overall view of these guides and details on the "how" of the demonstration. This work is based on the findings of [36]. In particular, we find the question of the difficulty of demonstrating nuclear safety and the scattered and high-volume aspect of the

information. In [33] and [40] the communication between the actors involved, or stakeholders, was clearly identified as a challenge in the demonstration of nuclear safety. MBSE is identified as an interesting solution for the case of nuclear safety. However, it is also identified that a paradigm shift (from documents to models) can be blocking for the institutions and operations already in place. The issue of traceability as well as the lack of detail in guides and standards is one of the barriers identified for project management including nuclear safety It is conventional to provide general good practice so as not to constrain demonstration methods, but this makes the expectation of the demonstration ambiguous. Added to these difficulties is the large number of documents and the difficulty of sharing information. Linosmaa et al. in [43] provides interesting elements on the link between SE and nuclear safety demonstration. This work is part of the BESEP (Benchmark Exercise on Safety Engineering Practices) project under the European funding "Horizon 2020". The field of nuclear safety is analysed within the framework of the ISO 15288 processes in a more thorough manner than in [38] which was mainly in the suggestion of this link and in a first surface analysis of ISO/IEC 15288. This coherence with system engineering brings interesting elements on the communication and collaboration of the teams, since it is one of the objectives of system engineering. The conduct of the demonstration is approached here in a process-oriented approach and as part of the installation's life cycle (even if it is mentioned that the processes are concentrated on the design phases). This leads to a reflection on how to conduct the demonstration. The lack of a clear vision in the standards for conducting the demonstration (more "good practice" oriented) was mentioned earlier. Ouni et al. in [44] which is quite similar to [42] attempts to improve I&C modelling methods in the nuclear field. This modelling approach aims to facilitate the collaborative work of teams through domain-specific viewpoints. Thus, the engineers have in their modelling interface the elements that concern them. Here, the safety domain does not really have its own viewpoint, but safety concepts can be found in the viewpoint of I&C engineers (safety functions, safety classes). Indeed, this work aims to facilitate the modelling work of I&C engineers in a safety context. It does not aim to provide modelling elements to nuclear safety engineers (except in part for the I&C field). The elements of methodology and traceability were also taken into account in [36]. The data model provided in [41] also aims to provide elements that, if equipped, can help with traceability. This model also attempts to provide elements of reflection on the sparse aspect of data through the storage of artefacts that have enabled the qualification of the system. This issue of traceability through safety functions and viewpoint integration is also discussed in [37]. An interesting reflection on the link between MBSE and MBSA is conducted on this methodological aspect in [45]. MBSA (Model Based Safety Analysis) is an approach in which the design and safety engineers share a common system model created using a model-based development process.

MBSA intends to act as a bridge between design engineers and safety engineers reducing the time required to verify the safety of a new designed system [46]. This work sheds light on the pitfalls to be avoided in linking MBSE and MBSA. Some expert modelling in safety areas cannot be based on design models which do not carry in their essence the information and modelling specific to these analyses. In [36] Linnosmaa et al. analyse the issue of integrating nuclear safety into an architecture model. This analysis is based on the AADL language (here specific to I&C and through three concepts/attributes; Defence in Depth (DiD), safety function, safety class). The INCREMENT [47] method provides interesting elements on information retrieval and search space reduction with elements from a metamodel designed with I&C experts. It includes elements on the traceability of requirements as well as on the search for information in regulatory texts. In line with the reflection on the subject of information volumetry and the use of AI [48]. The modelling approaches presented so far assume that we do all our projects via MBSE best practice, but this has not been the case for a long time. NLP (Natural Language Processing) techniques can help to facilitate the work of modelling, ontology populating, and REX exploitation on a document-oriented work. Other, more general, work involves thinking about transients (in relation to the initiating events previously introduced). For example, in the synthesis work [49] the author summarises the work done in several sub-domains of the nuclear industry. Although not directly related to the demonstration of nuclear safety, the consideration of AI in the identification of transients, accidents, or failures may be of interest in this discipline.

In conclusion of these contributions of the literature on the methodological elements, we see that the elements aiming at answering the conceptual barriers limit the possible methodology. Indeed, the languages, diagrams and methods that are developed are based on the concepts defined. Our conclusion is similar to our previous section on conceptual barriers. The developed or theoretical methods consider the elements of traceability, safety integration, collaboration etc. but are limited to I&C. Also, we find some proposals related to AI but very few are coupled with MBSE practices.

4.2.3 Technical barriers

This section summarises some of the work that has provided information on the issues raised in the Table 6.

Table 6 Technical barriers

Type of barrier	N°	Barrier
Technical	12	How can the tools/techniques enable the lifting of these barriers?
	13	What tools can be used to integrate the approach to both the safety demonstration and the design in order to have an integrated approach to safety in the project?
	14	What type of AI is to be considered for nuclear safety tasks?

These barriers refer here to the tools in which the conceptual elements and languages are instantiated. The reflection on the methodology must also include these tools. The level of maturity of the conceptual and methodological reflections will limit the potential of the tools which are only the last step. As such, [36] proposes an analysis of the tools available for drafting "digital safety cases". This work is taken up in several works by the same research team [38], [40]. The questioning of tools is conducted from the perspective of the MBSA and the languages and tools that are specific to each discipline in [45]. The link between the demonstration of safety and the design is enlightening in the step back and the classification of MBSA approaches. This MBSA approach must be considered in the context of our work without losing sight of the many contributions in the field. This work allows a synthesis and classification as well as a step back from our discipline and our objective. It should be noted that the objective is not to provide a new way of conducting reliability/safety analyses, a field that is more represented in operational safety. These safety analyses are well developed, the calculation software attached to them is known and qualified by the safety authorities and they allow the modelling of expert sub-domains which have their own research communities (criticality, radiation protection etc.). Beyond the reflections on the possible link between design and demonstration. The "demonstration" aspect can be found in the field of quality assurance/safety mentioned in the previous proposals and relating to the ISO 15026 standard [50] . This approach may allow linking the assertions to be proven to bundles of evidence from the different safety analyses of the domains mentioned (as well as from other design evidence etc.). It would then be interesting to link these demonstrations to the design in a manner consistent with the design of the installation.

In the work aiming to carry out a reflection on the integration of nuclear security (malicious acts) in PSAs we inevitably find a consideration of tools. The approach of this work aims at an integration towards tools, the very selection of PSA software is consistent with a possible integration in the existing probabilistic demonstration processes. The consideration of design in the conduct of failure analysis following

attacks is reflected in this work. Although it does not concern the type of study concerned by this thesis, it should be considered in a more global approach to digitisation in the field of nuclear safety. In [42] the approach is tool oriented in order to use these models to verify safety requirements on I&C, although the approach seems unsuccessful on the language proposed in the study. The integration of safety in design is at the heart of this approach through this language and this approach to modelling the I&C architecture. This work is interesting in the approach of integration with the architecture and reflection on the concepts that are most likely to be paralleled on the AADL and I&C safety side. However, the language used is aimed at expert simulations in the field of industrial computing and does not include the entire nuclear safety demonstration methodology. It is actually stated at the end of the paper "*"In addition to improving the analysis capabilities of our model, the further work on the topic would require fitting the modelling approach and tools support better to be part of the systems engineering processes of the overall design to be truly useful for the nuclear engineers".* In [44] Although limited to the field of I&C the work seems to be of interest in the coherence of the approach and the choice of developing a tailor-made tool. It also seems clear that the perfect solution does not exist and that we must try to develop it, for example by means of a DSML [51], [52]. A Domain Specific Language (DSL) is defined as "a programming language or executable specification language that provides, through appropriate notations and abstractions, expressive power focused on, and usually limited to, a particular domain." [53]. A DSML will use the latter for modelling. The choice of the Papyrus tool under Eclipse seems to be interesting. Although the work focuses on an expert understanding of I&C, some safety elements are mentioned, and the methodology is interesting. Documentation generation, functional simulation and export to other I&C tools (requiring interoperability) are however not presented. The work on NLP [48] work is tool-oriented and a choice is made to use AI algorithms. This choice is based on a symbolic approach to NLP (we will introduce these approaches in section 4). Other choices of algorithms are proposed in the work on the INCREMENT [47] method, and further reflection on the coupling with MBSE practices. This is not the case for [49] which is more general on nuclear industry domains, although some topics concern activities specific to nuclear safety demonstration. In the work [41] the authors of this research were interested in tooling through the desire to move towards a data model that could be tooled. However, this does not solve the problem of the "how" of this tool.

Physical tools and implementations should come last in a systemic thinking. There is little conceptual and methodological work on the integration of nuclear safety with SE modelling approaches and their possible coupling with AI. Thus, the state of the art of tools (software etc.) is also very limited. There are scattered initiatives on some of the

topics, but the software addresses the problem we pose in a partial or very partial manner.

4.2.4 Human organisational barriers

In this section, the work that has provided information on these barriers will be summarised. We remind you of these barriers in the Table 7

Table 7 Organisational and human barriers

Type of barrier	N°	Barrier
Human and Organisational	15	Document-oriented work
	16	Volume of data considered.
	17	Lack of staff with multi-disciplinary experience and a global vision
	18	Financial: lack of money to make the budgetary drift of projects acceptable.
	19	Psychological: difficulty of cognition of complexity in a "document-oriented" project context.
	20	Usage: reductionism in engineering which prevents the adoption of the understanding postures of other disciplines and which is not facilitated by the document-oriented approach.
	21	Ethics: nuclear demonstration often leads to mistrust by default because of past accident records, leading to increased rigor in this field.

Here, we are talking about the barriers related to the organisations and humans who are stakeholders in the conduct of these safety demonstrations. The latter may be the safety engineers themselves, experts in other fields, project managers or heads of organisations, as well as the public who of course have an interest in these demonstrations. All the work mentioned so far contributes to lifting these barriers to some extent. In the work [36] there is a desire to reflect on means other than documents, while considering the possibility of generating documentation from software. The difficulty of appropriating the large volume of documents in document-oriented processes is also a driving force in this work. In [37]the reflection on safety requirements and their possible modelling aims to move away from document-oriented processes. The reflection on the MBSE aims at facilitating the understanding of this complexity inherent to nuclear safety and resulting from a high level of heterogeneous layers intrinsically linked to each other (functions, physical architectures, different professions, etc.). The desire to provide processes based on models is a reflection to decompartmentalise the professions and to allow thinking about a holistic solution

considering all the professions with the objective that each one contributes to the solution as well as their relationship to safety. In the report [38], the introductory reflection on other work on processes leads to the OMG's metamodels and the tools for moving towards digital safety cases. The reflections on the possibilities of digitalisation aim to facilitate the understanding of engineers working on these subjects and to have tools to help them. Systems thinking is present in the consideration of ISO standards for systems engineering. The will to fight against reductionism and to bring a holistic approach in the framework of a transverse domain like nuclear safety is relevant. It is this idea that motivated this thesis work. We find in [40]The MBSE approach and what it brings in addition to the SE in the change of the "document-oriented" paradigm and the possibility of generating documentation from the models is briefly mentioned. The interest of documentation generation is to satisfy this type of current operation in the nuclear industry. The question of institutional evolution is a question that must be asked by the actors of this industry as a whole. This model-oriented approach, as well as the problem of cognition of a complex exercise such as the safety demonstration and its possible resolution only through a holistic approach, is taken up in the work on the data model [41] already mentioned. The cognition of such complex systems is recognised in these works and there is a will to move towards models allowing better visualisation of the problems and to analyse the requirements through simulation approaches. Holism is considered in its qualification objective approach without considering the reductionist approach which would only consider the disciplines in a separate way. Especially since I&C is at the centre of this interdisciplinarity. The approach of prioritising requirements in top claims is interesting but is here applied in detail to the case of I&C for one guide in the Finnish regulation. As notified in the report, a real investigation work would have to be set up if several guides and several sources are considered (this is the case when considering the safety demonstration in its globality and interdisciplinarity). The compliance approach is interesting and its formalisation by data model allows its use on lower-level subjects (such as an earthquake qualification of a material for example). However, the simulation approach is studied for I&C and cannot be easily reproduced as the modelling [54] requires expert knowledge of the domains considered. In order to extend this approach to simulating compliance with requirements, it is important to consider the work on MBSA [45] to identify the type of safety analysis performed in the proposed classification and whether they are directly demonstrable from the models. This is outside the scope of this thesis but is an interesting perspective for further work (more on this in the conclusion). In the work aimed at developing a method for modelling I&C and its relationship to nuclear safety [44], there is a desire to move away from the DBSE (Document Based System Engineering) approach towards MBSE. We note that through this name (DBSE) the authors consider that SE

approaches are known in this field, which does not seem to be the case for the work of the SAFIR programme. The multidisciplinary modelling approach aims to move away from reductionism towards holism in engineering processes. The work related to the INCREMENT [47] method aims to work on the high volume of data in nuclear projects. The modelling approach integrating several disciplines also aims at holism in these projects. The link with AI in the meta-analysis [49] and in the NLP work on safety procedures [48] is interesting in the response it provides to the high volume of data and the possibility of facilitating the cognition of this volume and related complexity. This is mainly what our work expects from AI. NLP and document processing are streams of AI use that have emerged precisely to navigate more easily in a document-oriented world. It is useful, however, that this transitional state remains so and that processes evolve instead towards model-driven engineering in which each element is put in its proper place and exists to serve a system purpose. If this is not taken into account, we can fall back into the problem of knowledge held by a few people who know the project but are limited to their domain. Research on the challenges of the discipline [33] mentions the lack of personnel with a multidisciplinary vision and a global view. We can put this element in the mirror of the processes pushing for reductionism in engineering practices. This paper seems to us to be particularly interesting in terms of taking a step back from nuclear safety. The elements cited were found indirectly in the previous work of this team, but their formalisation in this paper makes it possible to identify some of the root causes posing problems in the conduct of safety demonstrations. We have also taken up some of the problems identified in the construction of our work. The solutions mentioned are also based on the same disciplines that we are considering to remove these barriers. Although the reflection is general, the interest of the research group is always focused on I&C. This paper is an analysis of the problems and proposals for areas that could help solve them, but it does not propose a clear path for lifting these barriers. It is, however, a first step in a coherent research effort. The MBSA discipline review [45] discipline review emphasises the consideration of the objective (teleology) in a holism of the system and its components. It is important to step back from 'local' system analyses of components within the scope of a larger system. Also, in the work on PSA [54] and the integration of security into them, the approach is holistic and aims to bring together the safety and security domains directly into the PSA models. The work in relation to the BESEP project (introduced earlier) aims to get closer to SE processes and therefore aims at holism. This is the essence of the project, considering all stakeholders and interdisciplinarity in a project efficient way.

All the work presented so far highlights the importance of the issues raised and the need for a systemic and holistic approach to the complexity of an interdisciplinary

field such as nuclear safety. The high volume of data must also be considered when conducting these projects. The document-oriented approach is not optimised for working under these conditions. This is an important observation and a first step; however, the different works are mainly focused on I&C. AI is considered to allow a certain reduction in effort and time spent with greater exhaustiveness. However, it is not very consistent with MBSE approaches. In the end, this work proves that the nuclear industry is increasingly embracing MBSE approaches, but the work is scattered and nuclear safety is not considered in its entirety. Thus, the nuclear industry will be able to benefit from the MBSE advances of other industries (aerospace, aeronautics etc.) in what is common to both industries. However, an effort must be made to have coherent proposals on areas specific to the nuclear industry. Nuclear safety is at the top of the list.

4.2.5 Summary

In the following table, we find in columns the different barriers and on our rows the different works presented. By crossing the columns and rows, we identify whether or not these works have dealt with the barrier in question. In this table, we do not wish to integrate a "level" of treatment of the barrier under consideration, as seen in the section on the "Level of treatment" in section 4.2, each of these works has its own objectives. Although some barriers are dealt with, they are never fully dealt with, so we prefer to refer via an "**x**" to the works that deal, even in a minimal way, with the barrier under consideration or refer to it (for the details of the link with the barriers cf. section 4.2).

Work	Conceptual			Methodological								Technical			Human and organisational						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Linosmaa	x					x		x		x		x			x				x		
Tommila et al.	x	x					x	x							x				x	x	
Valkonen et al.	x	x		x	x	x			x	x		x							x	x	
Valkonen et al (2)	x	x		x			x	x	x	x							x				
Valknonen et al (3)	x			x	x							x			x						
Lisagor et al.							x					x	x							x	
Papakonstantinou et al (1)						x						x	x							x	
Papakonstantinou et al (2)						x						x	x							x	
Linnosmaa et al (2)			x				x					x	x								
Alanen et al.	x	x	x					x		x					x				x	x	
Ouni et al.				x	x		x					x	x		x					x	

Work	Conceptual			Methodological								Technical			Human and organisational						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Hutchison et al.								**x**		**x**	**x**			**x**		**x**					
Suman											**x**			**x**		**x**					
Choi et al.										**x**		**x**		**x**		**x**			**x**		

Two areas emerge from the analysis of these studies. These are System Engineering (SE), and particularly Model Based System Engineering (MBSE), and Artificial Intelligence (AI). The following parts introduce these two areas, then we will present the interest of these approaches in the framework of our study before entering the part of the contributions related to these two areas.

4.3 SE and MBSE

The model approach is not new in the world of engineering, these mathematical models often limited to equations in engineering reports have gradually been integrated into software that has become more sophisticated with time and increasing computational power. It has always been important to describe our model, its limitations and assumptions in order to properly consider its contribution to the study. Also, in the field of nuclear safety, several models of the installation co-exist and make it possible to simulate elements of reality for which it would have been complex to determine without having to multiply the experiments (MCNP [55], RESRAD [56], etc.).

Systems engineering [39], [57] has proven advantages in various industrial fields for coordinating complex systems engineering projects. MBSE [58] is the practice of developing a set of related system models that help define, design, and document a system under development. These models provide an efficient way to explore, update, and communicate system aspects to stakeholders, while significantly reducing or eliminating dependence on traditional documents. In this way, system engineering (MBSE) models elements that are both specific to the System of Interest (SoI), i.e., the nuclear installation, and to the System Used To Do (SUTD), i.e., the processes specific to project management, those specific to system management and the processes shared between the two (requirements management, etc.). Thus facilitating complexity management of the latter two processes. So, SE based on systemic principles, proposes more suitable processes, and promotes particularly modelling activities and models handling in opposition to documents management. In this sense, as stated during INCOSE Symposium in 2007 [59] Model Based System Engineering (MBSE) "*enhances the ability to capture, analyze, share, and manage the information*". Depending on their role in the project stakeholders can benefit from a view of the model adapted to their needs (viewpoint). [60] This engineering approach that inherits from SE allows a

better cognition and information sharing between engineering teams with less ambiguities by using models, highlighting the following benefits:

- Improved communications.
- Increased ability to manage system complexity.
- Improved product quality.
- Enhanced knowledge capture.
- Improved ability to teach and learn systems engineering fundamentals.

The MBSE approach is more and more used and known in the nuclear world. [61] [62] However the elements related to the demonstration of nuclear safety remain poorly considered (cf. introduction to safety in section 2.2.2), and there is then a problem in the appropriation of the modelling way usages and analysis of models, by nuclear engineers.

4.4 Artificial intelligence

Artificial Intelligence is defined as the study of "intelligent agents" [63]: any system that perceives its environment and takes actions that maximize its chance of achieving its goals. The improvement in computational power has allowed the advent of a period where connectionist models, usage of an inductive approach on data allowing for learning à travers le machine learning et le deep learning are overrepresented. In comparison to the so-called “symbolic approaches”, using a deductive approach, mainly instructions to the machine in the form of code but also approaches clearly linked to the use of mathematical logic and inference rules like Prolog [64]. (cf.Figure 15)

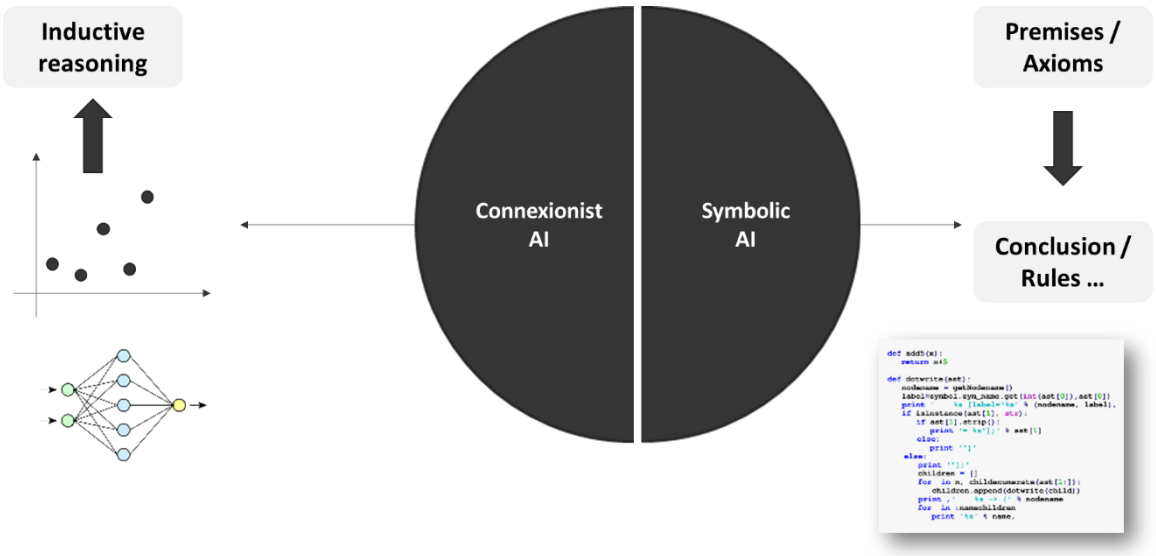


Figure 15 Difference between symbolic and connectionist approaches

Symbolic approaches "*represent things within a domain of knowledge through physical symbols, combine symbols into symbol expressions, and manipulate symbols and symbol expressions through inference processes."* [65]. Thus, these "symbols" are combined (in a deductive logic) in order to produce rule engines (called "expert systems"). In the field of NLP (Automatic Natural Language Processing), which we will introduce later, linguistic theories are used to perform various tasks, in particular information extraction or retrieval. Graph theory can also be exploited/used in this sense to represent knowledge, to make inferences and to structure information.

Connectionist approaches make connections in data to make inductions through a generalisation of observations. This is the approach on which machine learning and deep learning (deep neural networks) models are based. State-of-the-art models combine these two approaches in various ways. [66]

In 6 years, AI-related publications on arXiv *("free distribution service and an open-access archive for scholarly articles in the fields of physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics")* have increased from 5478 to 34736 in 2020 with an acceleration from 2019 to 2020 (34.5% compared to 19.6% from 2018 to 2019). [67]

This new paradigm in research allows for innovative approaches and a new way of working. It also saves a lot of time in a context where projects are becoming more and more complex and where this resource may be lacking to have complete and detailed safety studies. However, it is necessary to understand how these algorithms work to avoid pitfalls in their use. Approaches to learning algorithms (connexionist approaches) are generally divided into three, depending on the data available and the intended goals [68]:

- Supervised learning: *"We can have examples of data where we have both the inputs and outputs: (i,o)"*
- Unsupervised learning: *"For some data, we only have the inputs i".*
- Reinforcement learning: *"Sometimes we have no direct access to the "correct" output, but we can get some measure of the quality of an output o following input i"*

Supervised Learning makes predictions, based on labelled data, and learns from its mistakes. Unsupervised Learning discovers underlying structure and use it for example to cluster data. In Reinforcement Learning, the learning agent search for the optimal way in a system of steps rewarding and maximisation of final cumulated reward.

4.4.1 Natural Language Processing

Automatic natural language processing (NLP) is a subfield of computer science, artificial intelligence, and linguistics. Among the many definitions, [69] defines NLP as: *"a theoretically motivated range of computational techniques for analyzing and representing naturally occurring texts at one or more levels of linguistic analysis for the purpose of achieving human-like language processing for a range of tasks or applications."*

We find in this definition the notion of "techniques" that allow us to analyse and represent language as used between several stakeholders, these exchanges not having a (basic) computational post-processing objective. The notion of linguistic levels refers to structuring in modern linguistics (cf. Figure 16).

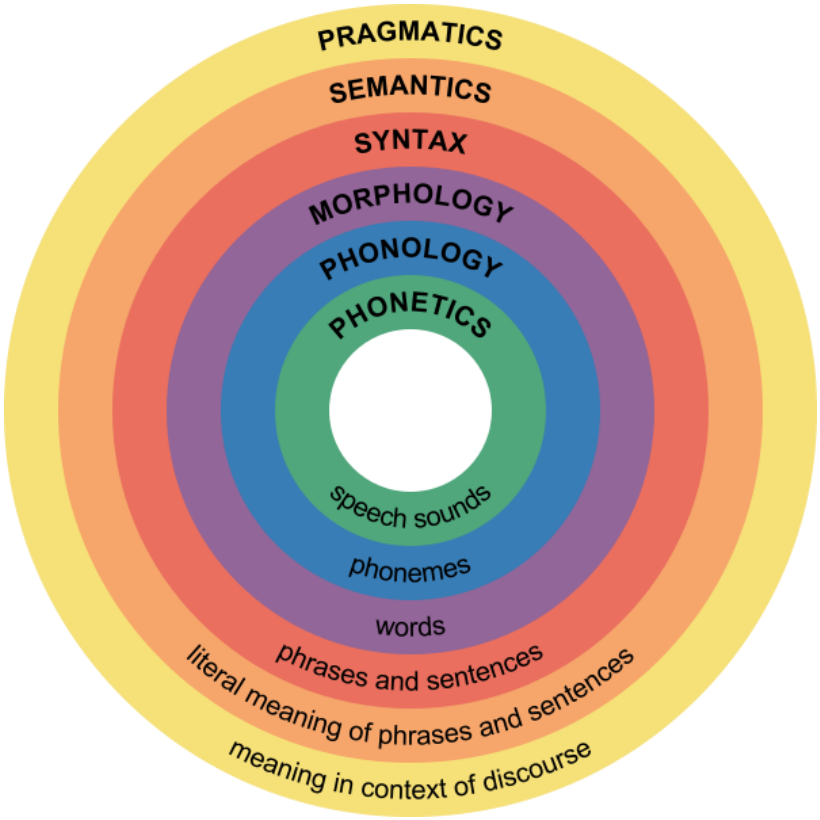


Figure 16 Major levels of linguistic structure

The analysis of text in its consideration of symbols representing elements of reality and being part of a system represented in linguistics through these different levels is a difficult task. The objective of NLP is the development of language models that can then be used to solve tasks that would require human work, and these algorithms have the advantage of being adapted to the processing of a large volume of data. The first work in this field coincided with the development of AI in the mid-20th century Alan Turing's test [70] test is linked to the field of NLP. Naturally, the development of this field first went through the conversion of linguistic theories (Saussure [65], Chomsky [66], etc.) into symbolic AI (expert systems). The wave of connectionist AI from the late 90's until today has been oriented towards the development of neural deep learning models, more and more massive in terms of parameters (neurons) and trained on large amounts of data. The approach of training on data makes it easier to consider the complexity inherent in language and difficult to transcribe by finite rules. However, in the training techniques, or in the application of these models to specific tasks, we find the strong contribution of linguistics. These language models are oriented around the

use of Transformers [73], transfer learning techniques facilitating work with less data, and the contribution of Deep Mind to bidirectional training where the BERT [74], [75] model was for a while the state of the art in the field (more on that in the following section).

4.4.1.1. Introduction to language models in a connectionist approach

As seen in our state of the art, if one decides to use artificial intelligence it is important to consider the type of data to analyse. In the case of nuclear safety, the main data sources are textual. In this section, we will introduce the sub-domain of AI that aims at processing documents written in natural language. As mentioned in the previous section, three approaches coexist in training:

- Supervised learning.
- Unsupervised learning.
- Reinforcement learning.

Depending on the domain, these types of learning will solve different tasks. For NLP, current trends tend to relegate the intrinsic difficulty of the language and language levels described in previous section and Figure 16. These models have gone through different stages, in parallel with the models devoted to image processing (reference to the "Imagenet moment of NLP"). [76]), different stages (cf. Figure 17)

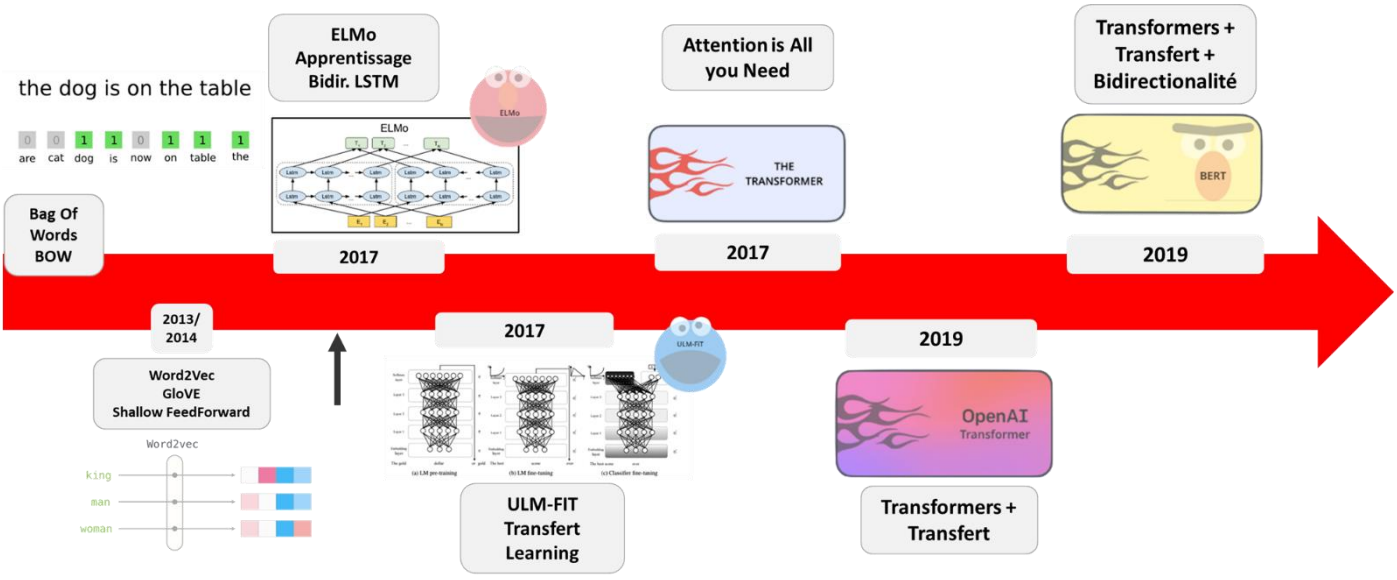


Figure 17 Different steps in NLP from Bag of words to Language Models

Among the elements that have highlighted the use of artificial intelligence, the digitisation of unconventional data is an important element. The multimodality of the models now dealing with images, sound and text was not

achieved in a short time. In the case of word processing, the digitisation techniques include vectorisation (or embedding [77]) of words, paragraphs, documents etc. The first approaches were simple and consisted of templates called "bag of words": *"A very common feature extraction procedures for sentences and documents is the bag-of-words approach (BOW). In this approach, we look at the histogram of the words within the text, i.e. considering each word count as a feature."* [78]. Subsequently, the models became more complex. In the case of Word2vec [79] and ELMo [80] the models are still vectors. However, the latter integrate a relative semantic allowed by a training of the model on a large quantity of documents to locate the statistics of representation of such word in relation to others. The ELMo model adds the nuance of the meaning of the word according to the context (which was not the case for Word2Vec or GloVe [81]). At this stage, the NLP field is starting to benefit from models trained in the laboratories of the digital giants (Google, OpenAI, Facebook etc.). With the ULM-Fit model, transfer learning techniques will be brought to the fore. This makes it possible to train a model on unsupervised tasks and to use this pre-trained model on more specific tasks with better performance despite a smaller amount of data. The problem of lack of data to make models converge is recurrent in small companies or laboratories. These models are trained on the language model task (hence the name “language model”) which consists of predicting the next word from a given word string. The main turning point in NLP research is linked to the publication of the paper "Attention is all you need" [73] in which a new type of architecture is put forward: the "Transformers". This type of architecture offers greater performance and allows for parallelized learning. The latter was mainly sequential in NLP (processing one word after another) using time series processing models. Also, Transformers allow a better consideration of the relationship between a word and the others in a given sentence through the attention mechanism. The fusion of the contributions on transfer-learning and Transformers were used by Open-AI on their famous GPT-2 model. Bert which would later add some state of the art features. Among these features, the bidirectional training (processing of the sentence from left to right and right to left by the model during training.) on sentences to have more context to determine the next word (the elements coming after the word are of great help to understand the intended meaning). Since 2019, many heir models to these language models have emerged. A lot of research is focused on improving them but also on the possible uses in various fields. The field of engineering and Industry 4.0 is no exception, and it seems obvious to us that MBSE techniques that offer a general view of engineering should be coupled with AI and NLP techniques.

The latter are exploited through 'pipelines' (series of algorithms put together), each of whose elements performs discrete tasks. The end-to-end nature of these pipelines allows for continuous processing of data to achieve the goals set by the stakeholders.

4.4.1.2. Training of the BERT model on classification tasks

As introduced in the previous section, language models are usually pre-trained on large amounts of data. In the case of BERT [74] this pre-training was done on data from BooksCorpus (800M words) and the entire English wikipedia (2,500M words).
Once this model is pre-trained, it is used to perform new tasks. This mechanism is called "fine-tuning" and allows the best results in general on NLP tasks. We will present our result using this approach in the contribution section (cf. 5).

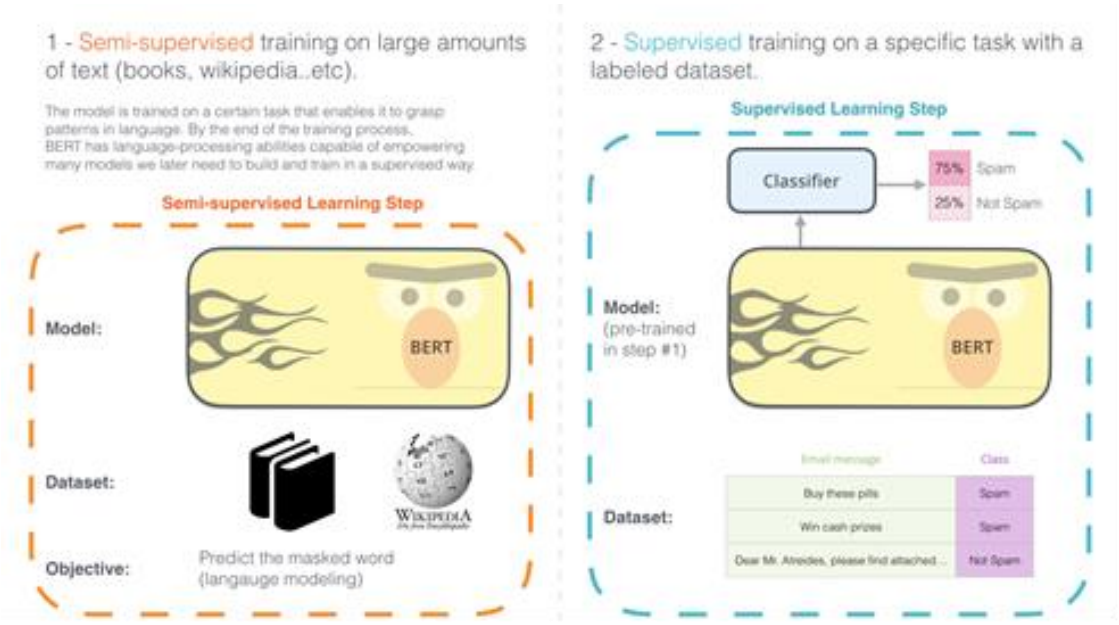


Figure 18 Pre-training and training of BERT model

4.5 Interest of MBSE and AI for nuclear safety demonstration

To evoke the interest for the demonstration of safety, it is interesting to draw a parallel with the recent work of the Working groups of the AFIS (Association Française d'Ingénierie Système) on the subject of agility [82]. Let us first introduce this work. Indeed, these agile methods facilitate collaboration and optimisation of value creation in less time. The question of the mix between systems engineering practices and the new so-called "agile" methodologies [83] are leading to an evolution of the agility manifesto [84] to highlight the practices of systems engineering to frame the practice of agility, which is sometimes unclear on certain aspects of project/system management (cf. Table 8)

Table 8 Differences between Agile Manifesto for Software and the adaptation from AFIS to MBSE

In the past	Agile software	Agile MBSE	Details
Processes and tools	Individuals and interactions	Individuals and interactions based on models, common digital repository	Requirements repository, system architecture mode, test model
Comprehensive documentation	Working software	Showable systems	Model as a contributor to a virtual representation of the system
Contract negotiation	Customer collaboration	All stakeholders collaboration	The model as a more concrete and understandable mean to exchange and assess the progress of the project
Following a plan	Responding to change	Mastering changes	The model, an efficient support to identify impacts on the system

It seems interesting to draw a parallel between these elements of an 'agile' project management practice reflected by what the MBSE practice can bring to the conduct of projects and demonstration of nuclear safety. In the case of those projects that include safety, there are multidisciplinary teams with many stakeholders. Communication through document exchange hinders good collaboration. Modelling allows a better global vision for each of the professions of the subjects which are specific to it while allowing each one to collaborate on a general model of the installation.

Based on the elements of the Table 8, where agile values advocate emphasising the interactions of individuals rather than processes, the MBSE adds that these interactions of individuals must be framed in digital repositories and shared models. The safety engineer has ongoing dependencies with each of these businesses and must be able to communicate effectively. The integration of all stakeholders rather than just the client is important, as in the case of nuclear safety demonstration all stakeholders are involved for the protection of people and the environment which is crucial. Finally, the decisions that are taken and resulting from a better understanding of the context inducing changes must be controlled with real impact analyses via the manipulation of models. Indeed, changes that would be induced by performance needs could harm technological choices initiated by fundamental needs for nuclear safety. We thus find the reasons that push towards an appropriation of the MBSE subject for the nuclear industry and a development of work catalysing solutions bringing added value for the industry and all its stakeholders.

The subject of Artificial Intelligence is data. It seems important to us to elaborate the reflections on this subject to identify the elements of the safety demonstration which lend themselves to the exploration of large volumes of data and where learning techniques seem relevant. We are trying to bring a global vision around the work of developing both the right models for nuclear safety project management and an

informed understanding of the possibilities of AI and the topics where AI could have a significant contribution. The multimodality of data is an issue to be considered.

4.6 Expected contributions

In view of the problems listed and the state of the art, our work aims to remove the barriers that are here sorted into four categories. To meet these objectives, we decided to work on a pragmatic method integrating a conceptual reflection through the metamodel that supports it. This will allow us to define the concepts of nuclear safety, their attributes, and the relationship between them. It should be noted that we are not restricting ourselves to a sub-domain of nuclear safety but treating it in a holistic way. This method will be practice-oriented and will allow the integration of safety engineers and the safety domain in the collaboration with the other project stakeholders. Thus, communication will be facilitated to exchange through common models. We will also try to integrate some artificial intelligence techniques through separate contributions, in addition to this method.

Type of barrier	N°	Barrier	Contribution
Conceptual	1	Lack of agreement on common terminology in relation to the demonstration of nuclear safety	Proposal of a metamodel on nuclear safety concepts
	2	Definition of elements strongly present in safety such as: Requirements, Safety argumentation (CAE framework [34])	Proposal of a metamodel on nuclear safety concepts
	3	How to link the nuclear safety demonstration to the design of the installation?	Proposition of a metamodel on including concepts of demonstration with concepts of design.
Methodological	4	How to facilitate communication between teams?	Proposal of a method.
	5	How to facilitate collaboration between different domains?	Proposal of a method.
	6	How to conduct the safety demonstration?	Proposal of a method.
	7	How to integrate nuclear safety into MBSE models as a viewpoint?	Analysis of nuclear safety processes and concepts and integration into a method.
	8	How to have a traceability of safety requirements?	Have a reflection on the traceability integrated in the method.
	9	Lack of clear vision in the standards of the methodology to adopt.	Proposition of AI techniques in phase to irrigate the proposed method with data, information, and knowledge to be considered

	10	Scattered information, fragmented documentation.	AI algorithm to search for certain information.
	11	How can AI help on nuclear safety demonstration?	Elements of reflection on this subject as well as our concrete contributions.
Technical	12	How can the tools/techniques enable the lifting of these barriers?	Elements of reflection on this subject as well as our concrete contributions.
	13	What tools can be used to integrate the approach to both the safety demonstration and the design in order to have an integrated approach to safety in the project.	Proposal of an ecosystem of interoperable tools capable of carrying out these reflections
	14	What type of AI is to be considered for nuclear safety tasks?	Partially through our algorithms, but an in-depth analysis should be undertaken
Human and Organisational	15	Document-oriented work	Proposal of a model-oriented method
	16	Volume of data considered.	Proposal of some AI algorithms
	17	Lack of staff with multi-disciplinary experience and a global vision	Not addressed by these works
	18	Financial: lack of money to make the budgetary drift of projects acceptable.	Not addressed by these works
	19	Psychological: difficulty of cognition of complexity in a "document-oriented" project context.	Method to facilitate the understanding of complexity
	20	Usage: reductionism in engineering which prevents the adoption of the	Holistic approach drawing on the

		understanding postures of other disciplines and which is not facilitated by the document-oriented approach.	strengths of MBSE
	21	Ethics: nuclear demonstration often leads to mistrust by default because of past accident records, leading to increased rigor in this field.	Not addressed by these works

5 Contributions

5.1 Presentation of the contributions

The contributions in this chapter are grouped and presented successively around the three pillars that guided the R&D work. A case study will then illustrate these contributions on data from the nuclear industry before highlighting the limits reached today and thus logically highlighting the perspectives of this work.

5.1.1 The guiding pillars of our R&D work

The contributions of each pillar will be explained in this section:

Figure 19 3 pillars of the thesis

Our work is guided by three "pillars" that reflect R&D objectives considered essential and that have been logically put forward and associated. These pillars have been logically put forward and combined as shown in Figure 19 to remove the barriers presented in the problematic. These barriers have been studied separately, following the logical order of these pillars.

These three objectives are:

- -Objective 1: To be able to make better use of heterogeneous, numerous data that are difficult to master by an isolated human actor. In this context, the solution lies in artificial intelligence techniques.
- Objective 2: Integrate the demonstration of safety as early and as closely as possible in the System Engineering processes and in a model-based engineering approach such as MBSE with its undeniable assets:
    - Easier collaboration made possible by a common vocabulary known by both sides (design engineering and safety actors).
    - Reduction of documents to be delivered as late as possible.
    - Reactivity in exchanges and therefore faster and more reasoned modifications.
    - Global and holistic view of the 'whole' (the system to be delivered as well as its demonstration).
    - Etc.

- -Objective 3: To have support tools that meet the expectations of both engineering and safety.
    - On this objective, the subject of interoperability is not to be considered last. To develop a unique solution that can provide all parts of the method and to integrate the AI contributions seems utopian. However, linking the different elements through an efficient interoperability allowing each part to perform a specific function makes much more sense.

5.1.2 Illustration of the overall contribution in relation to the pillars

To guide the reading of our contributions, we will give first a general vision of the contributions aimed at lifting the barriers mentioned earlier. Taking up the objectives mentioned in the previous section, these contributions should enable (cf.Figure 20):

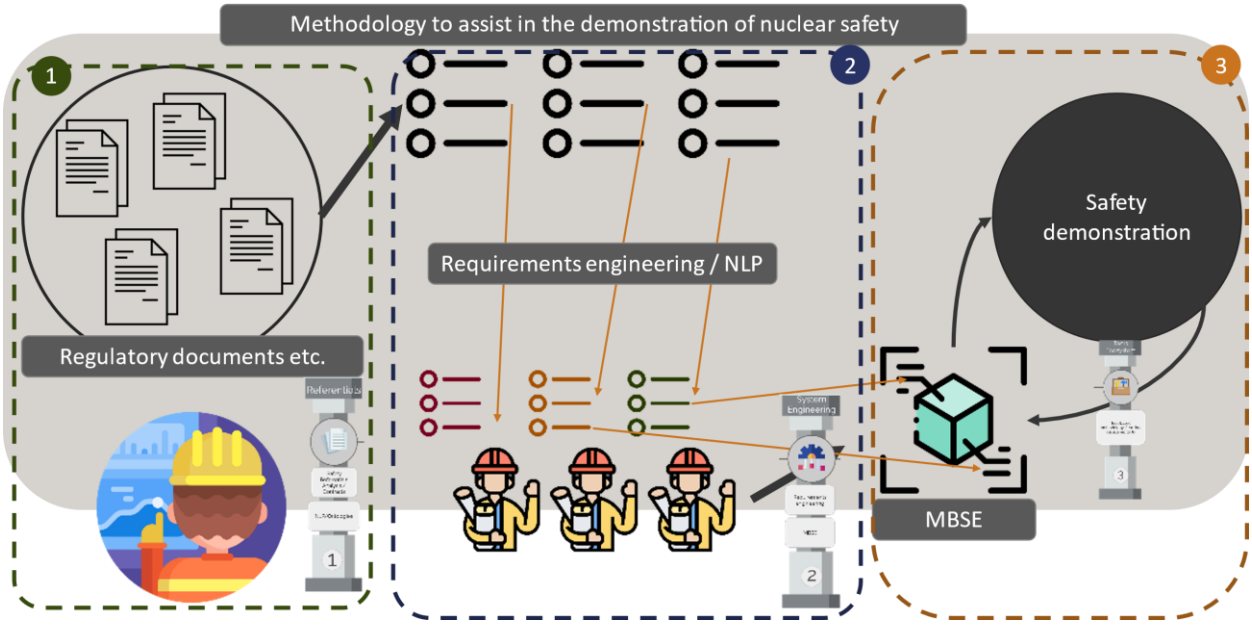


Figure 20 Tooled methodology to assist in nuclear safety demonstration

1. In part 1 of the figure above: Tools that would assist the engineer to facilitate the research work by speeding it up, and by proposing relevant elements for the demonstration of nuclear safety: Tools drawn from the AI domain.
2. Part 2: In the same way, tools would facilitate the navigation within these data allowing to analyse and classify these data: Tools also drawn from AI.
3. Part 3: It should be possible to link these data to models representing the System of Interest (SoI) at a later stage [39] under development. This can be achieved through the development of an appropriate method to better integrate the consideration of nuclear safety into MBSE approaches.

We find our "pillar" objectives mentioned in part 5.1.1 in the Figure 20. The purpose of this figure is to show which contributions are linked to each of these objectives. We have attempted to link the parts of the Figure 20 to the pillars/objectives, to the extent of the contributions of these parts to our three objectives. This will allow the reader to step back and consider the positioning of the contributions in relation to the overall approach of this work.

5.1.3 Pillar 1: Processing of safety references.

In consideration of the 3 pillars presented in section 5.1.1 and 5.1.2, we will start in this section with the presentation of the contributions related to the first

pillar. The elements required for nuclear safety are often found in documents written in natural language.
These documents can have different origins and be of different kinds:

- From the regulations;
    - Decree.
    - Order.
    - Etc.
- From the nuclear safety authority:
    - Guides.
    - Reports.
    - Etc.
- Operators:
    - Safety Report (SR).
    - Guides.
    - General Operating Rules (RGE).
    - Etc.
- Project management:
    - Specification.
    - Applicable documents.
    - Safety studies.
    - Etc.

These documents are not designed to allow for the extraction of information of interest at a later stage. However, this extraction is important because projects linked to the nuclear industry include the safety profession. The latter requires the reading and appropriation by engineers of a large volume of information. In a study analysing the practices of engineers empirically, it was found that 30% of working time is spent on searching for information and 24% on sharing information. Thus, almost half of the engineers' working time is spent on information retrieval and communication. [85] In the case of our safety studies it is important to understand that they are even encapsulated in projects with cost, quality and time constraints [30]. This proportion of working time spent on information gathering is therefore problematic. In our state of the art, we mentioned the interest of artificial intelligence approaches to work on this time saving. The sub-domain of AI which allows the analysis of natural language, NLP (Automatic Natural Language Processing), seems to be able to bring benefits on these subjects. In the following sections, we will present our contributions in relation to NLP for nuclear safety and the purpose of our method. We will describe

our contributions on the training of BERT-type algorithms on the recognition of nuclear safety requirements. These requirements are data of interest in the above-mentioned documents for nuclear safety engineers.

5.1.3.1. Contribution 1.1: Creation of a body of requirements dataset on IAEA documents

In previous work by our team, an API (Application Programming Interface) for OCRisation and recognition of the layout of documents and their constituent elements (table, text, figures etc.) was developed. The output of this document parser becomes the input to our requirements classifier. Inputs recognised as requirements are subsequently extracted. The model provides a reliability score, so that a threshold value can be set for the consideration of requirements. (cf. Figure 21).

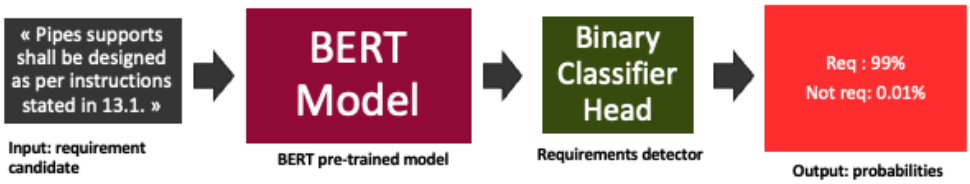


Figure 21 Extraction of a requirement

To train the model we manually prepared a Dataset based on the IAEA documents, mainly about risk characterisation in the context of the choice of nuclear sites for new installations. A total of 1141 requirements were extracted from these documents (cf. Table 9 and Figure 22 The choice of these IAEA documents was motivated by the possible use of this type of standard in several nuclearised or nuclear developing countries. Indeed, these documents can be used by countries that have not yet developed mature nuclear regulations. These documents are therefore an excellent basis for these new safety authorities. They are also considered in more mature nuclear countries as good practices that are appreciated in nuclear safety demonstrations (cf conclusions of section 2.2.1).

Table 9 Documents for requirements dataset constitution.

IAEA Documents	Type
NSG3.2	Geology/Hydrogeological
NSG3.6	Geology/Hydrogeological
SSG9	Geology/Seismic/Bathymetry
SSG35	Seismic
Serie85	Seismic
Serie89	Seismic
SSG21	Volcano
SSG18	Oceanography/Bathymetry/Hydrogeological/Meteorology
NS-R-3 Rev1	Hydrogeological/Meteorology
GSR-Part-7	Meteorology

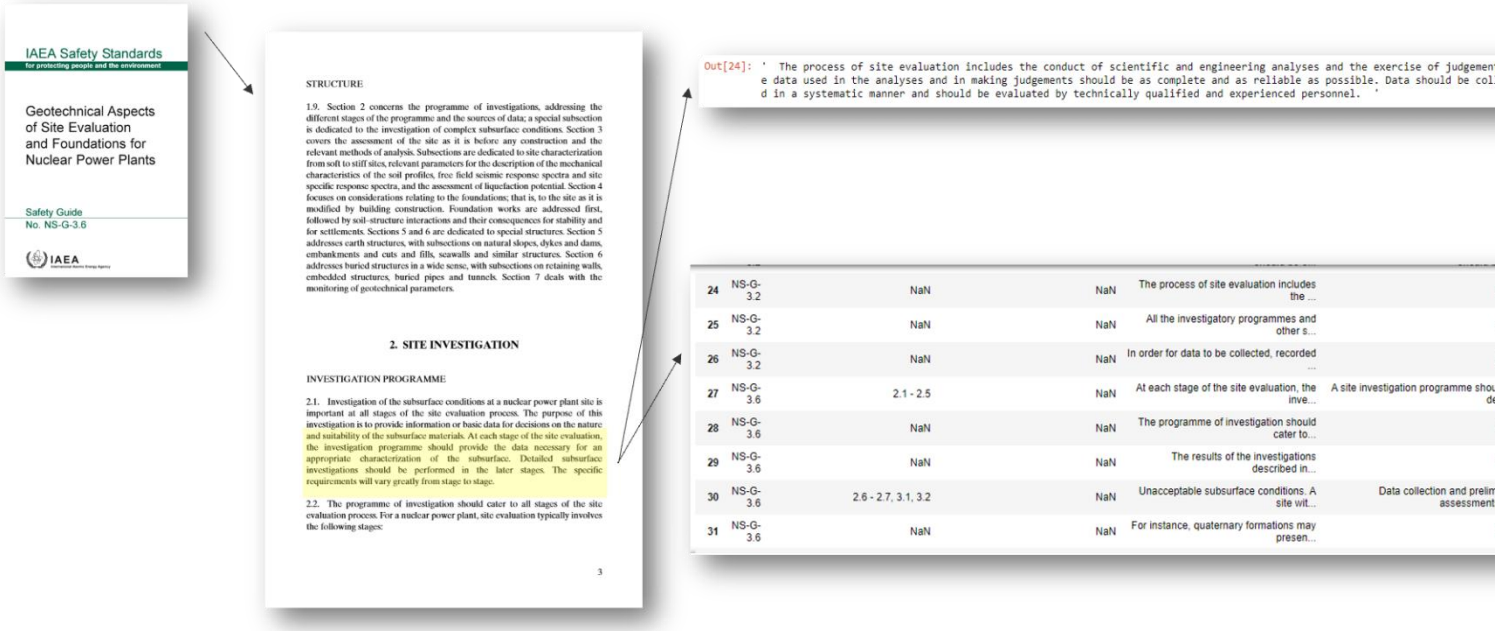


Figure 22 Illustration of the preparation of the IAEA-Requirements dataset

For the constitution of the dataset, the elements of the document labelled "requirement" have been extracted. However, to train the model, it is necessary to have text elements representing what a "non-requirement" is. To do this, we performed a data augmentation by embedding the requirements (represented as a vector via sentence-BERT [86]) and calculating the average vector of the latter, thus representing the "prototype" vector. By taking the opposite of this vector

(prototype of the "non-requirement") and parsing the documents, we extracted the inputs that are close to this opposite vector (cosine distance) and thus represent "non-requirement" texts. Thus, we have artificially increased the number of negative examples ("non-requirement" label) to balance the dataset and thus, the model.

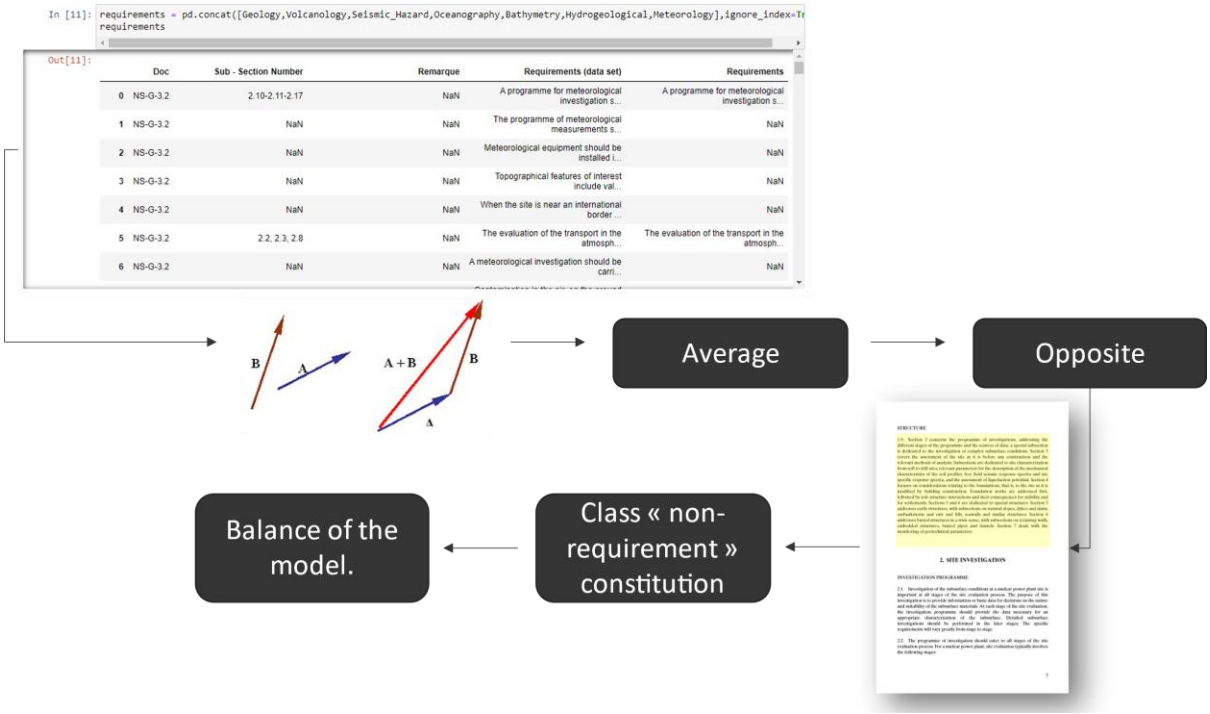


Figure 23 Negative examples augmentation through sentence-BERT

Concerning the training, we have used the model pre-trained by Google teams [74] (requiring huge computing capacities) and "fine-tuned" it on our requirements classification task to extract them afterwards. This consists of a recalculation of the superficial layers of the neural network (cf. section 4.4.1.2) .

When the model is trained, the dataset is divided into 3 parts (cf.Figure 24):

- A set for training the model to recognize the requirements.
- A set for validation used during training to adjust model hyperparameters and thus avoid overfitting of the model. Optimized set of hyperparameters will allow us to perform well on new data.
- A test set. This set constitutes requirements that will never be seen by the model, and it is on this dataset that the model will be checked.

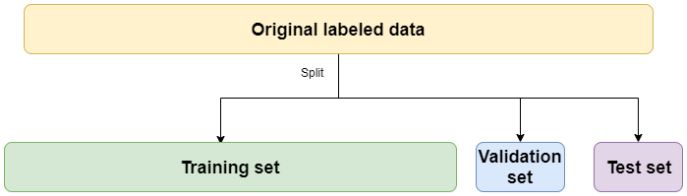


Figure 24 Dataset split

The results will be analysed using a confusion matrix (cf. Figure 25) typically used in classification models. After training the classification algorithm, we present here the results of F1 score on our test dataset (thus never seen by our algorithm). This measure is calculated from the precision and the recall. Precision is the number of correctly identified positive results divided by the number of all positive results, including those not identified correctly. Recall is the number of correctly identified positive results divided by the number of all samples that should have been identified as positive. The product in the numerator directly affects the score if there are extremes.

Classification accuracy using BERT Fine Tuning: 95.63%

	precision	recall	f1-score	support
0	0.99	0.96	0.97	530
1	0.97	0.99	0.98	738
accuracy			0.98	1268
macro avg	0.98	0.98	0.98	1268
weighted avg	0.98	0.98	0.98	1268

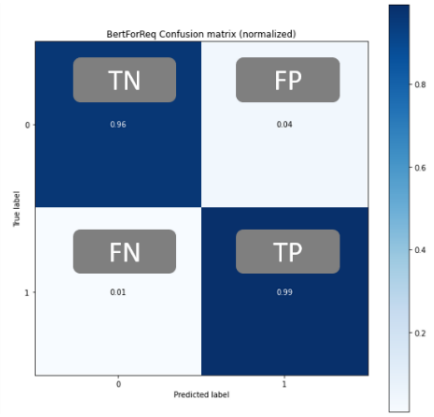
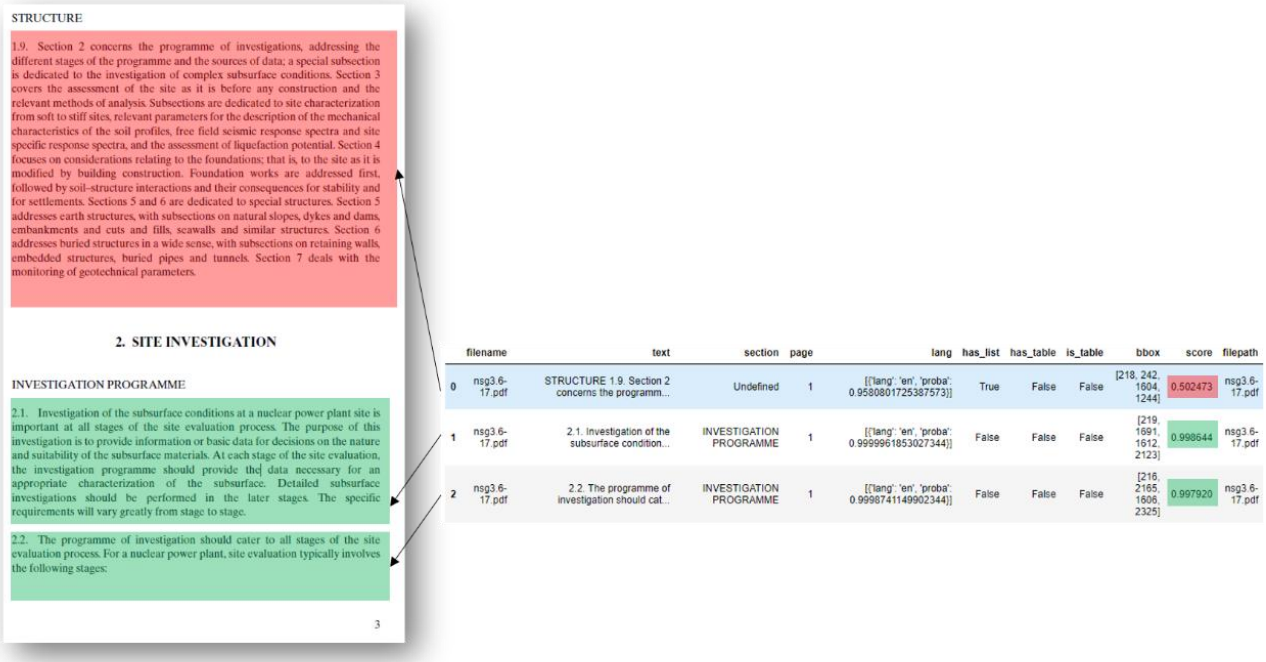


Figure 25 Confusion Matrix and f1 score for requirements Classification on BERT

An example of extraction is shown in Figure 26. The document is a test page that presents specifications for the evaluation of geotechnical aspects in the phase of selection of sites suitable for the construction of nuclear reactors. On this page, points 2.1 and 2.2 are requirements. Point 1.9 is a description of the contents of section 2 of the IAEA report.

The algorithm gives its results for each of these text blocks, we see that point 1.9 obtains a recognition score of about 0.5. Points 2.1 and 2.2 are selected with a



	filename	text	section	page	lang	has_list	has_table	is_table	bbox	score	filepath
0	nsg3.6-17.pdf	STRUCTURE 1.9. Section 2 concerns the programm...	Undefined	1	[{'lang': 'en', 'proba': 0.9580801725387573}]	True	False	False	[218, 242, 1604, 1244]	0.502473	nsg3.6-17.pdf
1	nsg3.6-17.pdf	2.1. Investigation of the subsurface condition...	INVESTIGATION PROGRAMME	1	[{'lang': 'en', 'proba': 0.9999961853027344}]	False	False	False	[219, 1691, 1612, 2123]	0.998644	nsg3.6-17.pdf
2	nsg3.6-17.pdf	2.2. The programme of investigation should cat...	INVESTIGATION PROGRAMME	1	[{'lang': 'en', 'proba': 0.9998741149902344}]	False	False	False	[216, 2165, 1606, 2325]	0.997920	nsg3.6-17.pdf

Figure 26 Example of extraction on a page with requirements and descriptive

reliability of more than 99%. It is then up to us to set our threshold value.

5.1.3.2. Contribution 1.2 : RCC dataset

For this second contribution, we decided to build a dataset on Design and Construction Rules (RCC). This choice was motivated by the understanding of the important elements in our metamodel (explained in section 5.1.5) in terms of repository processing. In the understanding of the methodology in nuclear safety demonstration, the classification of components is fundamental (cf. section 2.2.2.7). This results in the choice of requirements to achieve this safety level for the considered component. Repositories are qualified to achieve these quality levels through binding requirements. The RCCs are published by the French

Association for the rules of design, construction and surveillance in operation of nuclear boiler equipment (AFCEN). This association, created in 1980, brings together more than 800 experts and draws up design rules in several fields:

- Rules for the Design and Construction of Mechanical Equipment PWR (RCC-M) ;
- Rules for the Design and Construction of Electrical Equipment (RCC-E);
- Civil Engineering Design and Construction Rules PWR (RCC-CW) ;
- Rules for the Design and Construction of PWR Fuel Assemblies (RCC-C) ;
- Fire design and construction rules PWR (RCC-F);
- Rules for the Operational Monitoring of EPR Mechanical Equipment (RSE-M) ;
- Rules for the Design and Construction of Mechanical Equipment for Nuclear Installations for High Temperature Structures and the ITER Vacuum Vessel (RCC-MRx).

These standards have been used in the construction of more than 120 reactors, including the 58 in the French nuclear fleet. They are currently used in the construction of EPRs. It therefore seemed appropriate to establish a dataset capable of improving our model for this type of safety requirement with a style and writing characteristics specific to the AFCEN (NLP techniques are sensitive to writing style). This dataset is based on the RCC-M and RCC-E. The case study that we will put forward in the contributions to pillar 3 is based on the RCC-M, to which we added metadata of interest in connection with the safety classification system during extraction. This classification is partly that of the mechanical classification (cf. 2.2.2.7) but adds particularities specific to the RCC-M (cf Figure 27).

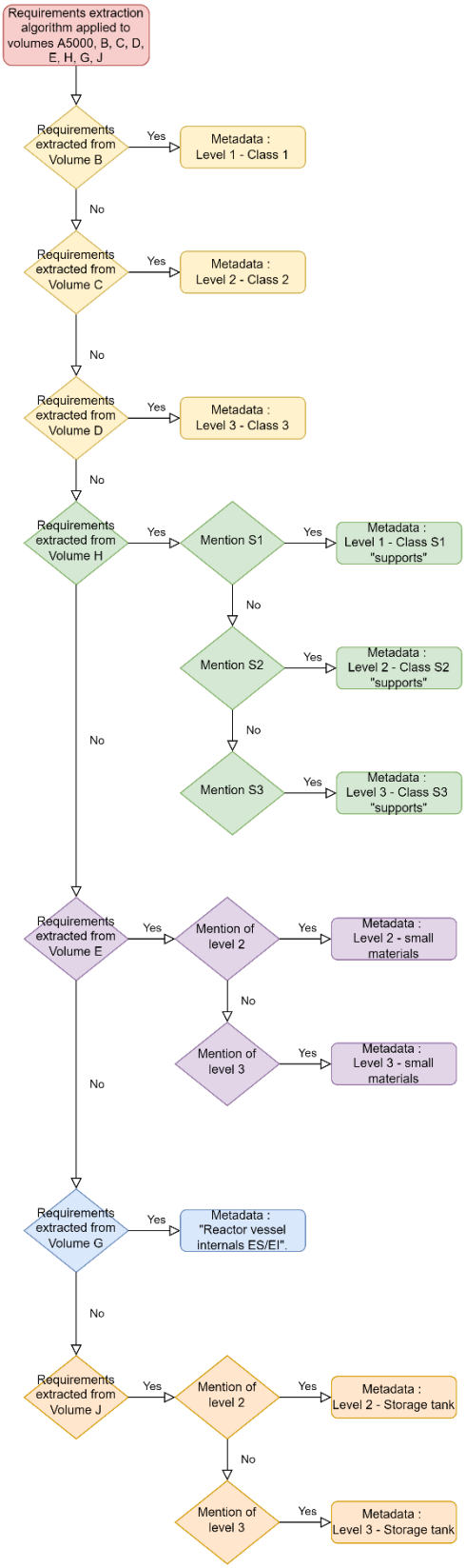


Figure 27 Safety class metadata for RCC -M

RCC-M/RCC-E dataset and camemBERT model drive

The dataset from the RCC-M and RCC-E repositories has the following breakdown:

Table 10 RCC-M/RCC-E dataset broken down by labels/volumes

RCC	Volumes	Label	Number
E	II	Requirements	**156**
	IV	Requirements	**344**
	Total RCC-E	Requirements	**500**
M	A	Requirements	**17**
		Non-requirements	**1**
	B	Requirements	**49**
		Non-requirements	**169**
	C	Requirements	**111**
		Non-requirements	**119**
	D	Requirements	**22**
		Non-requirements	**22**
	E	Requirements	**91**
		Non-requirements	**32**
	G	Requirements	**82**
		Non-requirements	**84**
	H	Requirements	**81**
		Non-requirements	**45**
	J	Requirements	**81**
		Non-requirements	**36**
	Total RCC-M	Requirements	**540**
		Non-requirements	**508**

M + E	Total	Requirements	**1040**
		Non-requirements	**508**

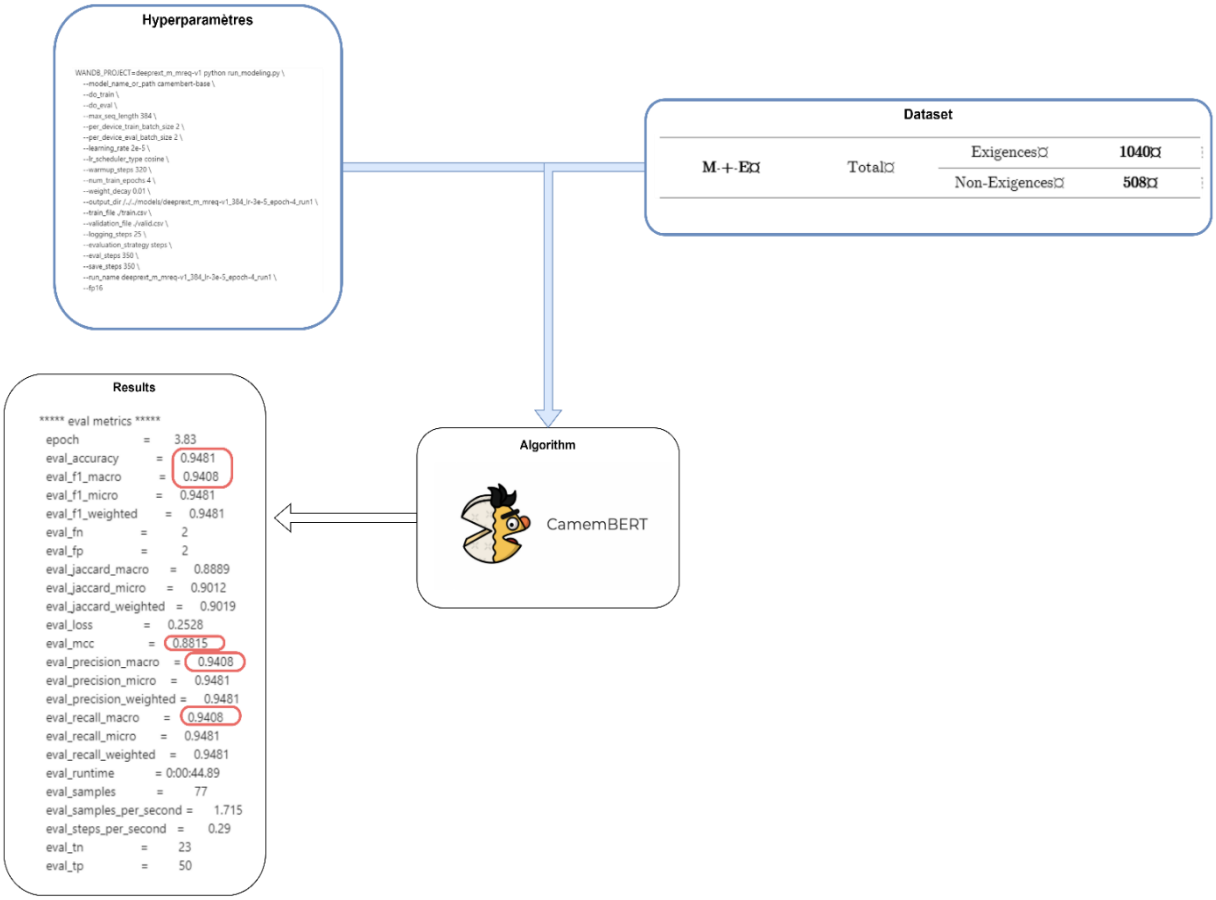


Figure 28 Hyperparameters, dataset and training results of CamemBERT on our RCC dataset

The trained model is an instance of BERT whose weights have been pre-trained on a large amount of French language data (CamemBERT [87]). The Figure 28 summarises the results as well as the hyperparameters of the training (refer to the training modalities of the BERT type language models in section 4.4.1.2).

The evaluation values (surrounded in red in Figure 28) are the same as for previous model training in section 5.1.3.1. There is also the MCC (Matthews Correlation Coefficient Formula cf. Figure 29) evaluation [88], [89] :

$$MCC = \frac{TN \times TP - FN \times FP}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

Figure 29 MCC Calculation

"The coefficient takes into account true negatives, true positives, false negatives and false positives. This reliable measure produces high scores only if the prediction returns good rates for all four of these categories [90].

As a conclusion to the contributions on pillar 1, the work carried out was mainly focused on the identification of high value-added data for the nuclear safety domain: safety requirements. The field of AI and the adapted algorithms were selected. A dataset of about 3000 requirement/non-requirement units was annotated. These datasets were used to train two NLP (Natural Language Processing) algorithms of the BERT type.

5.1.4 Pillar 2: Requirements Engineering

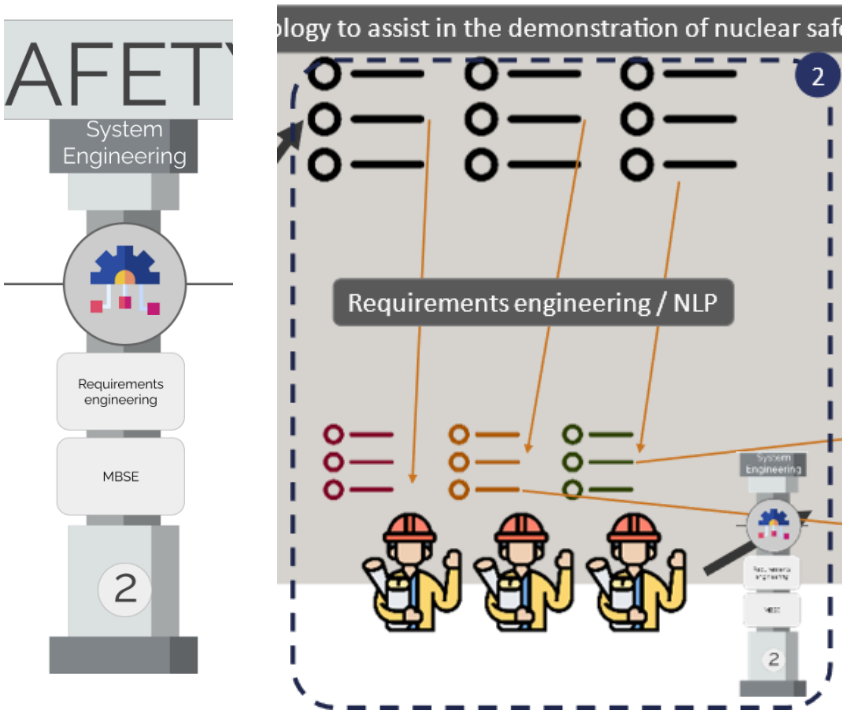


Figure 30 Pillar 2: System Engineering and requirements engineering

In part 2 (Figure 30), the contributions focus on the use of NLP approaches to facilitate the navigation, analysis and classification of requirements.

5.1.4.1. Use of unsupervised algorithms in the processing of a large number of requirements.

Requirements engineering is a broad field that deals with requirements-related activities in the context of a project. Activities included in requirements engineering [91] are:

1. Collecting the requirements from all stakeholders [92] and regulatory prescriptions.
2. Compiling and collating the requirements.
3. Establishment of the requirements.
4. Ensuring the expected qualities of the requirements (e.g., SMART).
5. Tracing, tracking, and reporting the progress of requirements.

These activities become complex as soon as the volume of requirements increases. They seem to us to be facilitated by an artificial intelligence approach. Among the techniques put forward, the representation of requirements in the form of vectors (embedding) and the representation of the latter in a vector space is an interesting process which has been put forward in certain recent works [93] [94]. The meta-analysis of these works in [95] show that the field is not as simple as simply training the latest algorithms on our requirements. The choice of the linguistic encoding of embedding is important (syntactic, semantic etc.).
Work within our team aims to improve the use of these techniques in order to:

- Classify;
- Streamline;
- Analyse quality;
- Detecting links;
- Detecting contradictions.

In the Figure 31 is presented an example of requirements classification, requirements clustering and a 2D representation to facilitate the visualisation of clusters. These embeddings can also be used to facilitate information retrieval. The cosine distances compared are then those of the query with the requirements of the vector space created. This proximity can be semantic, syntactic, etc. depending on the linguistic encoding chosen for the embedding.

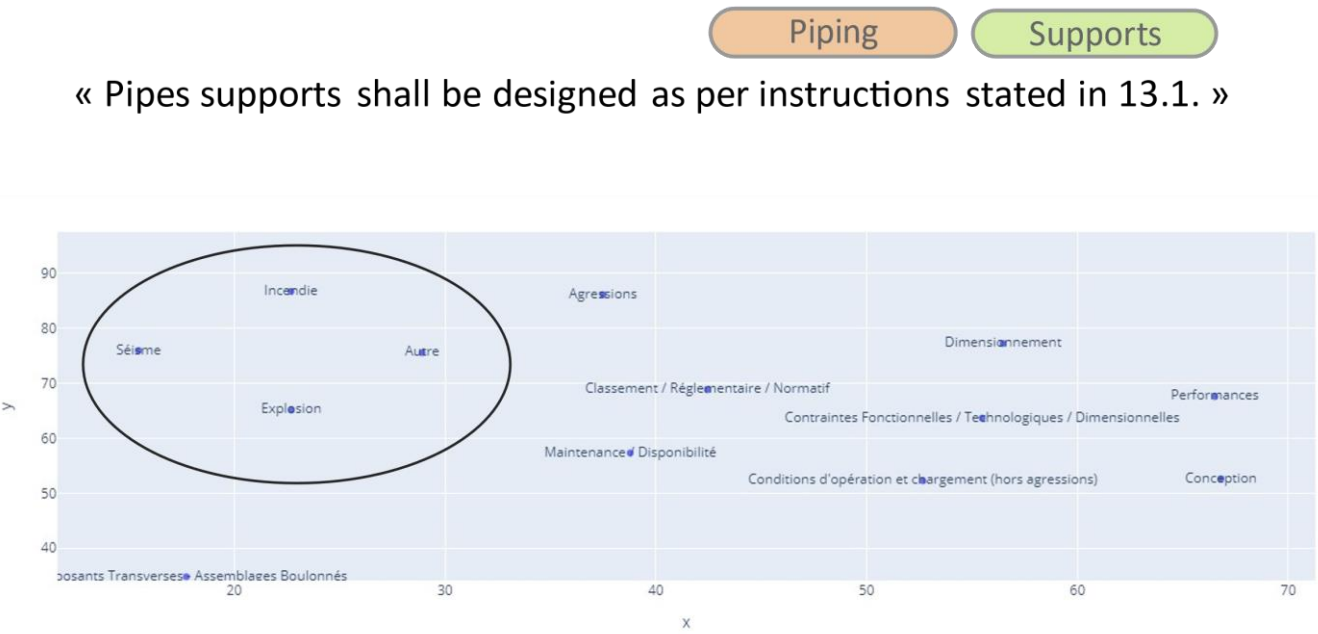


Figure 31 2D vector projection of cluster of requirements

In the presentation of the contributions of pillar 3 (section 5.1.6) a practical use of these techniques for the search for requirements that may be applicable to a component from a model.

5.1.5 Pillar 2: MBSE

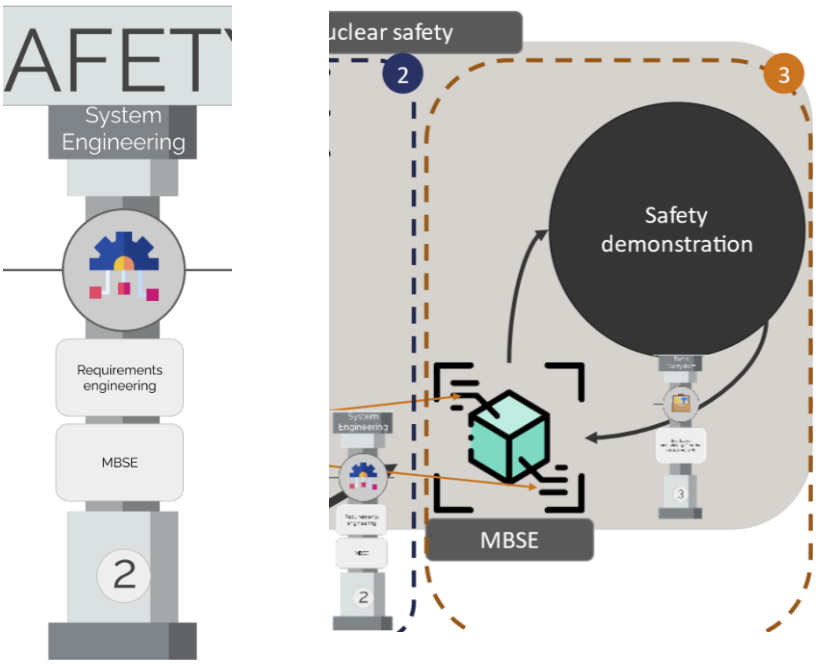


Figure 32 Pillar 2 and MBSE

In the following contributions, we will focus on those related to the modelling part (MBSE). In this context, our method is a global approach aimed at integrating the elements related to the demonstration of nuclear safety into the modelling of the target installation on which the various engineers are working (cf.Figure 32).

Figure 33 Framework of the method followed

This method (cf. Figure 33) is composed of:

- Concepts: Ontology/Metamodel in which we describe the concepts of our method (described in section 5.1.5.1):
    - Their definitions.
    - Their attributes.
    - The relations between these concepts and their constraints to model the relationships to be considered, for instance, between a proof and the activity that provides it.
- Languages: DSML (Domain Specific Modelling Languages) establishes the rules for handling concepts (described in section 5.1.5.2) promoting then modelling activities to progress together with an holistic and globalized view of both the system of interest to be studied (INB) and the safety demonstrations to be performed and justified.
- Processes: The steps to carry out the method (described in section 5.1.5.3). These processes can be expressed in several ways, for example in the form of a BPMN (Business Process Modeling Notation [96])
- Tools: Tools that will allow us to implement the method, this may require interoperability between several tools (described in section 5.1.6).
- REK (Repository of Expertise and Knowledge): Repository of expertise, best practices, REX or more simplest experiments (described in section 05.1.6.2) In the context of models, this concerns knowledge elements that have been approved, verified, validated, and can be generalised and reused in other projects.

5.1.5.1. Contribution 2.1: Nuclear safety concepts and metamodel

The various concepts specific to the demonstration of safety have been modelled in our metamodel in ecore format, considered as the reference [97] for the implementation of the Meta-Object Facility (MOF) standard [98] [99] of the Object Management Group (OMG). This format is an integral part of the Eclipse Modeling Framework [100] which is mainly aimed at programming through modelling. This approach will be mentioned in the section 5.1.6, on the tooling of the methodology.
The reflection around this meta-modelling was done through an analysis of the literature on the demonstration of safety, the main documents used are those from the pyramid of regulatory texts (cf.Figure 34).

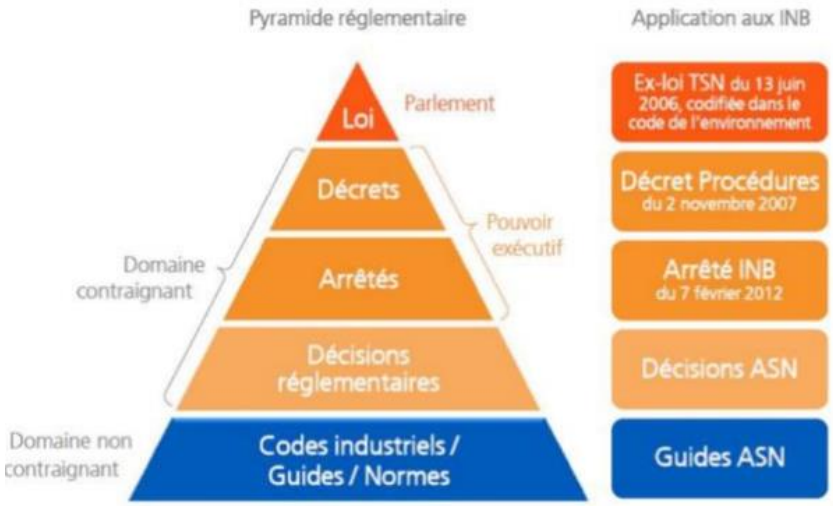


Figure 34 Nuclear industry regulatory pyramid

This analysis was carried out according to the following methodology:

- Identification of concepts of importance for the nuclear safety demonstration;
- List of important attributes for the engineers in charge of future modelling;
- Linkage of these concepts with other concepts already reported (intra-safety);
- Linkage of these concepts with concepts specific to the System of Interest (SoI i.e. the installation to be designed and realized) and the System Used To Do (SUTD) i.e. the project and the requested organization that focus on the system of interest design and realization. Particularly here requesting the safety demonstration as a particular set of tasks to be done in

collaboration and synchronization with all other tasks requested for design and realization.
- Iteration on new documents or in the context of exchanges with experts on the subject to focus on the genericity of the method.

To facilitate the work, the general metamodel has been divided into three views [60] :

- Scenario view,
- Safety specification view,
- Safety demonstration specification view.

These views are consistent with the processes which will be explained in more detail in the section 5.1.5.3. In the different figures, the concepts in blue are those that will be found in system engineering processes, even under different denomination that are here semantically unified in order to reach a compromise. These are the cross-cutting concepts that allow the safety demonstration method to be linked to the general modelling of the installation's design (requirements, functions etc.). We will develop the integration of this safety method into an existing methodology in Pillar 3 section 05.1.6. The elements explained in section 2.2.2 section will be useful for the understanding of the following parts. The summary of the metamodel and the description of the different concepts can be found in the Appendix 9.1.

Scenario view

In the scenario view, the main objective is to model incident and accident scenarios. These scenarios will then be used to specify nuclear safety features such as safety classifications, requirements etc. (Safety specification view).

These scenarios are part of installation situations:

- Normal ;
- Incidental :
- Design basis accidental ;
- Accidental beyond design basis.

For each of these situations, the operator sets Global Safety Objectives (radioactive dose objectives etc.). (cf.Figure 35)

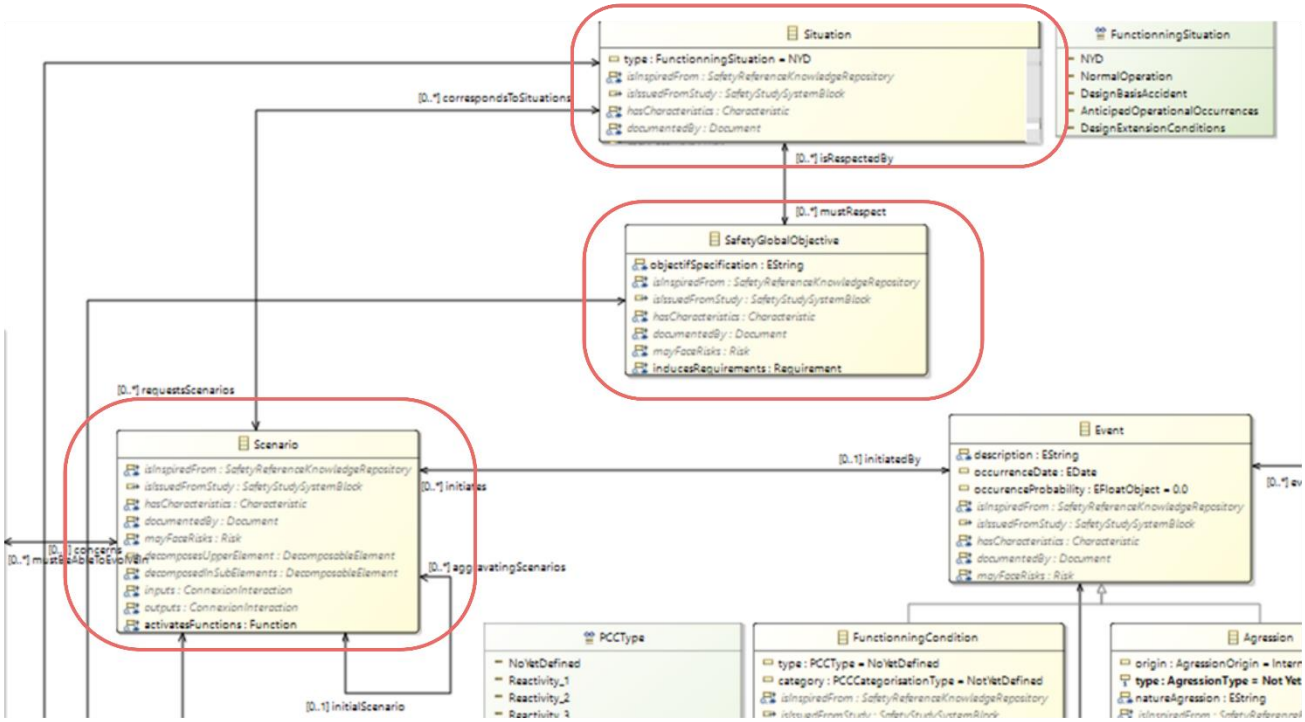


Figure 35 Concepts of situation, scenarios, and Safety Global Objectives in the scenario view

These scenarios concern components and are triggered by initiating events (cf. Figure 36).

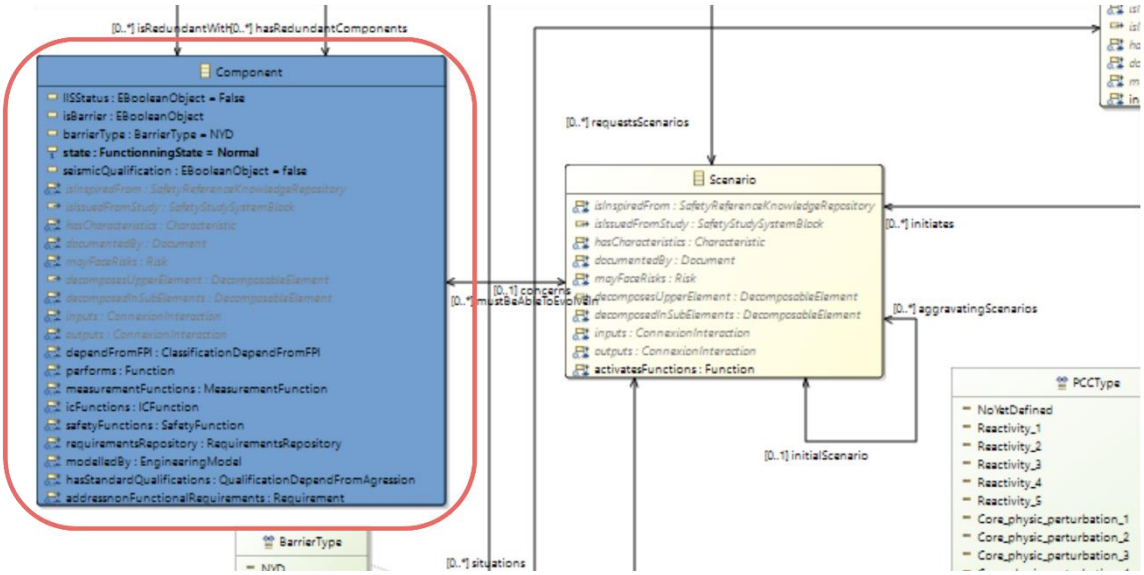


Figure 36 Concepts of component in the scenario view

The latter, within the scope of our study, are triggered by internal events (functioning condition) or by aggressions. These events lead to risks (cf. Figure 37). Finally, the concept of risk will be used later to trace the sources of requirements.

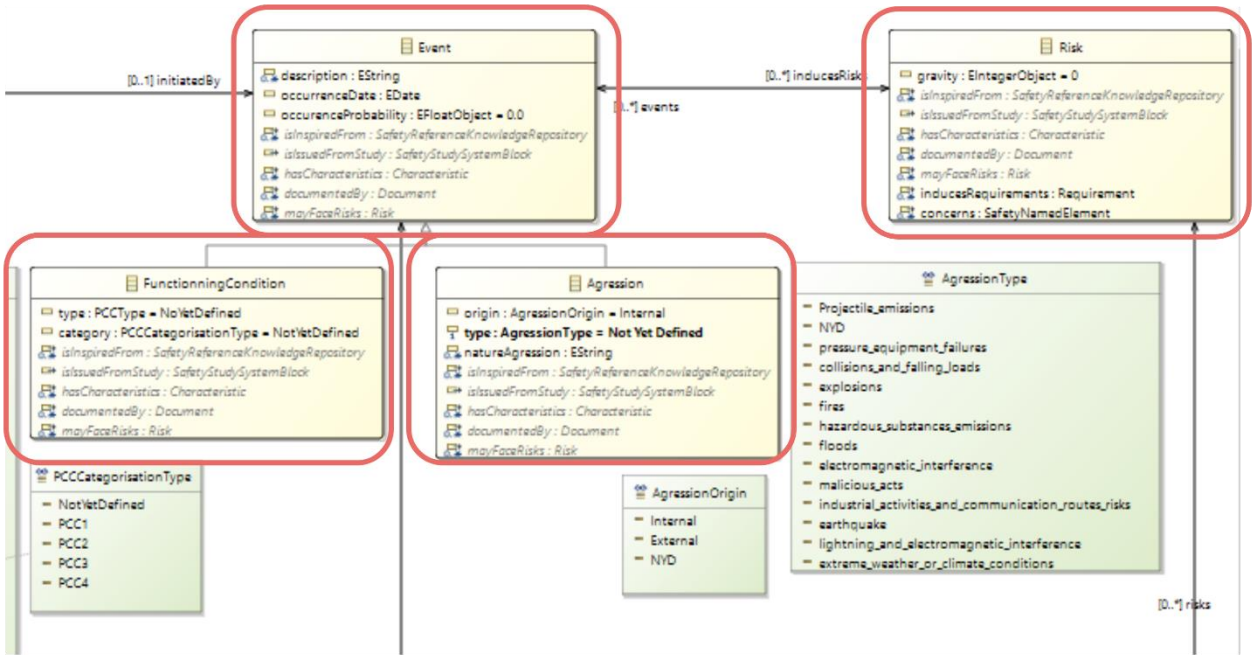


Figure 37 Concepts of events (functionning condition and agression events) and risk in the scenario view

Safety specification view

This view establishes the roles of the components with respect to the risks induced by initiating events. Similarly, this view highlights classifications and qualifications in relation to the role that each component plays in preventing and/or mitigating incidents/accidents. The classifications will also be linked to the FPIs (interest protection functions) to be performed by the component (see section 2.2.2.2). These qualifications will be related to the considered aggressions (earthquake qualification etc.) (cf. Figure 38, Figure 39).

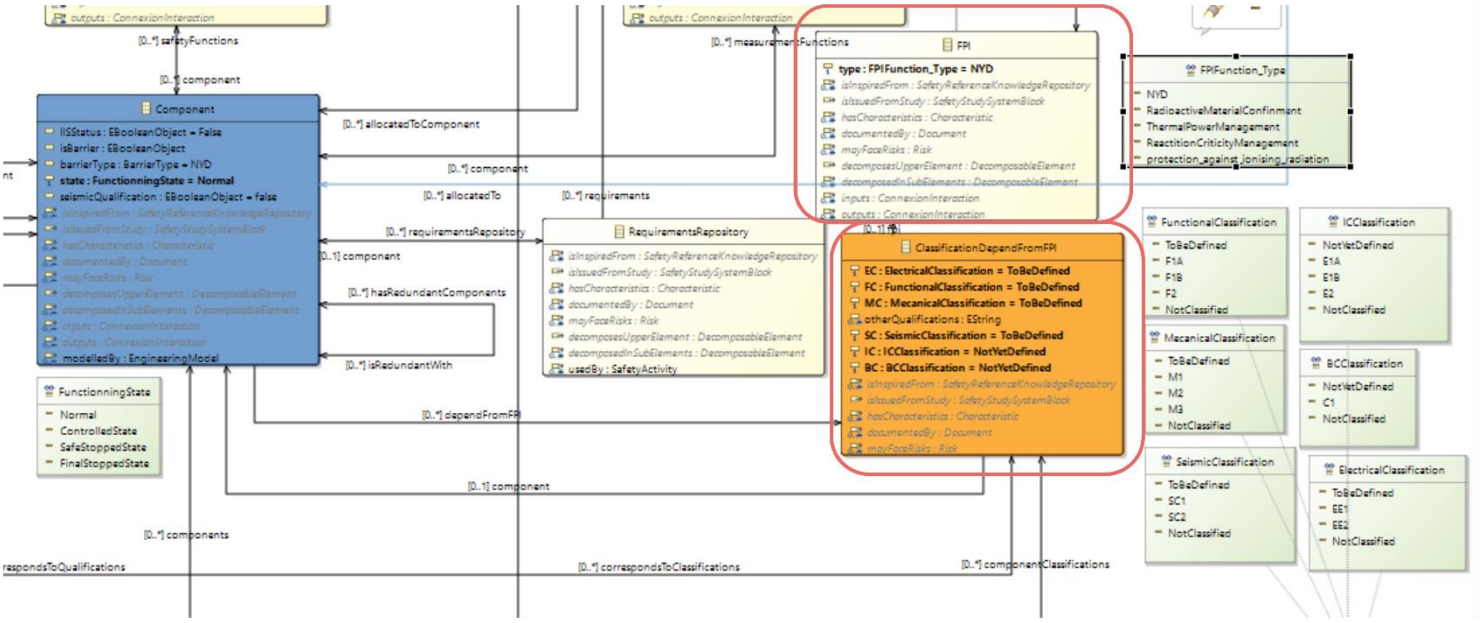


Figure 38 Classification and FPI concepts in the safety specification view

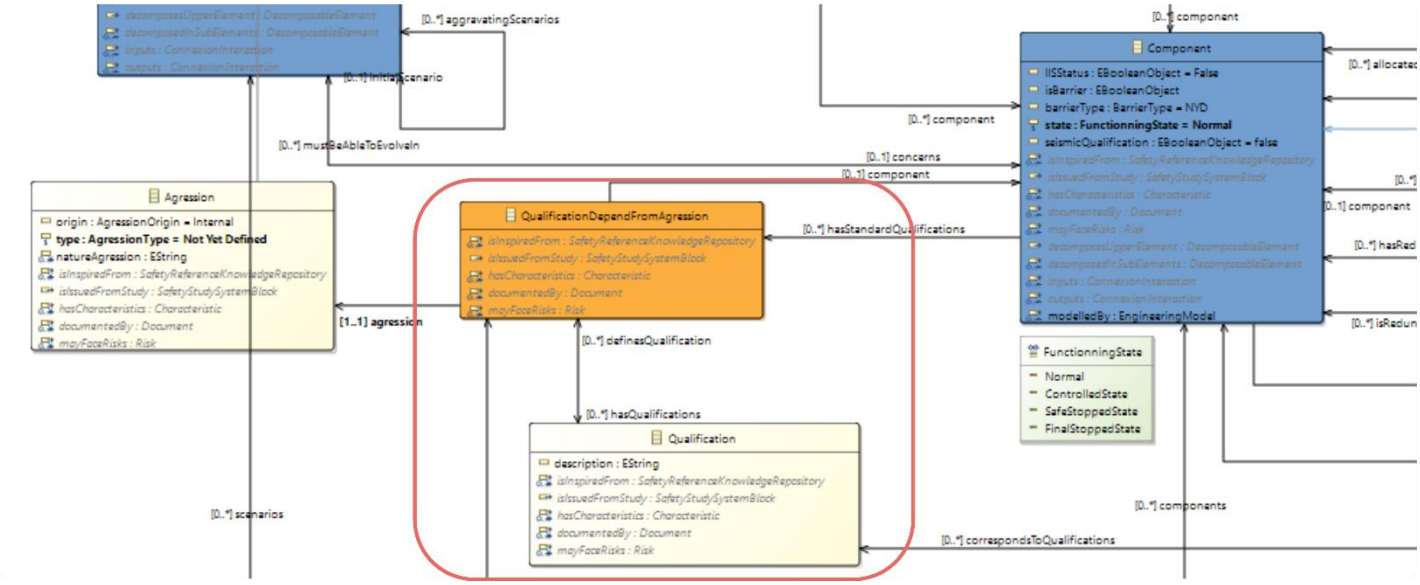


Figure 39 Concepts of qualification depending from Agression considered

These qualifications, as well as these classes, lead to requirements. In the case of nuclear safety, the typology of requirements is important. We find :

- IPFs: express functional requirements. They are functions to be provided by the components, but they can also be seen as higher level requirements.
    - Example: "Control of reactivity".
- EXs (requirements): These are high-level requirements found in the regulations. It is known that a certain number of systems will have to comply with them, but no means are given.
    - Example: "The release of radioactive material must be prevented"
- CAs (Expected Characteristics): These are proposals for the characteristics expected of a component to comply with the EXs and thus the FPIs.
    - Example: "The component must be sealed"
- The ED (Defined Requirements): These are proposed technical requirements (often proposed by the component's domain expert) to enable the expected characteristic of the component to be achieved.
    - Example: "A seal will be placed ...".

In our metamodel, these types of requirements all inherit from the general concept of requirements, which is therefore one of the abstract concepts used to structure the metamodel as a whole and to ensure the sharing of common attributes and relationships (cf.Figure 40).

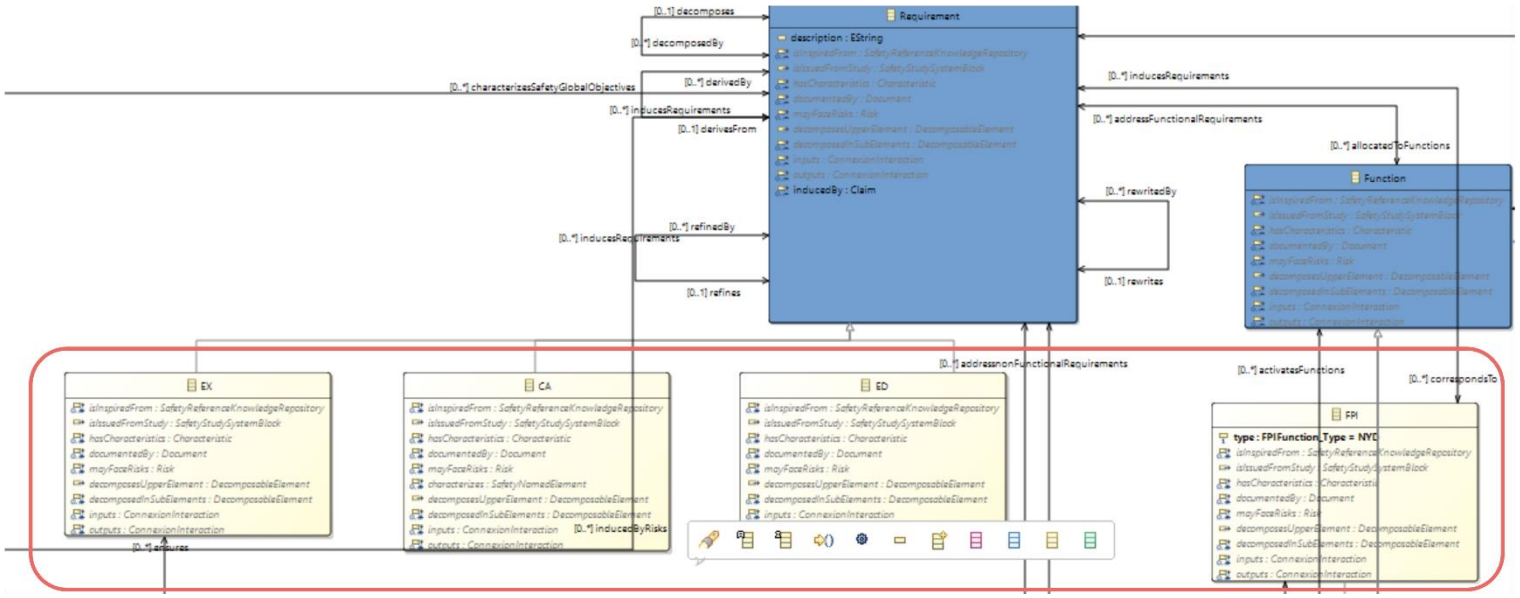


Figure 40 FPI, EX, CA, ED concepts in Safety Specification View

Safety demonstration specification view.

The classifications and qualifications as well as the safety analyses shall be used to derive the safety requirements to be met by the systems in the installation. It is then required to demonstrate the safety of the proposed design, including compliance with these safety requirements, the relevance of these requirements, etc. We decided to implement the CAE (Claim-Argument-Evidence) framework [34], [50] and therefore to describe the different concepts of the latter in our metamodel.

The CAE framework consists of the demonstration of "Claim" (Assertion) and "Sub-claim":

"Claims, which are assertions put forward for general acceptance. These are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims." [34].

The transition from one Claim to the other is done through blocks of argumentation:

"Arguments, which link the evidence to the claim. These are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established" [28], together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit " [34].

An empirical analysis of the safety cases led to the consideration of five blocks of arguments:

- Concretion block: "*This block is used when a claim needs to be given a more precise definition or interpretation. This is often the case of top-level claims, which generally need to be expressed in more measurable, less abstract, terms."*
- Substitution block: *"Another common type of claim expansion involves transforming a claim about an object (or property) into a claim about an equivalent object (or property), which can be viewed as a form of substitution."*
- Decomposition block: *"This block is concerned with structure. Many claim decompositions are about partitioning some aspect of the claim, for example, according to the functions of the system, the architecture, the properties being considered or with respect to some sequence such as life cycle phases or modes of operation."*
- Calculation block*: "Calculation blocks This block is used to claim that the value of a property of a system can be computed from the values of related properties of other objects (e.g., its subsystems).*
- Evidence incorporation block: *"This block is used at the edge of the CAE structure to incorporate evidence into the assessment. It is used to demonstrate that a subclaim is directly satisfied by its supporting evidence."*

The arguments are finally supported by evidence: *"Evidence, which is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis."*

To support the use of the CAE framework, a graphical notation describes the relationships between the different elements. (cf.Figure 41).

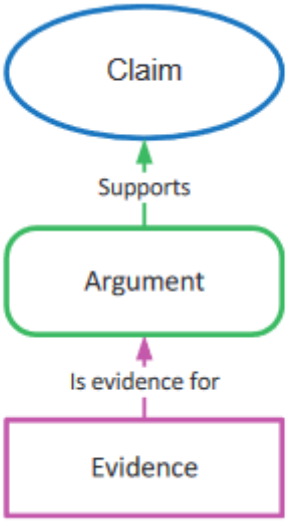


Figure 41 CAE framework

This graphic notation will be used in our safety demonstration specification diagrams. In our method, the link between the claims and the safety requirements is added, thus representing the keystone of the link between the design (requirements) and the demonstration (claims) (cf. Figure 42).

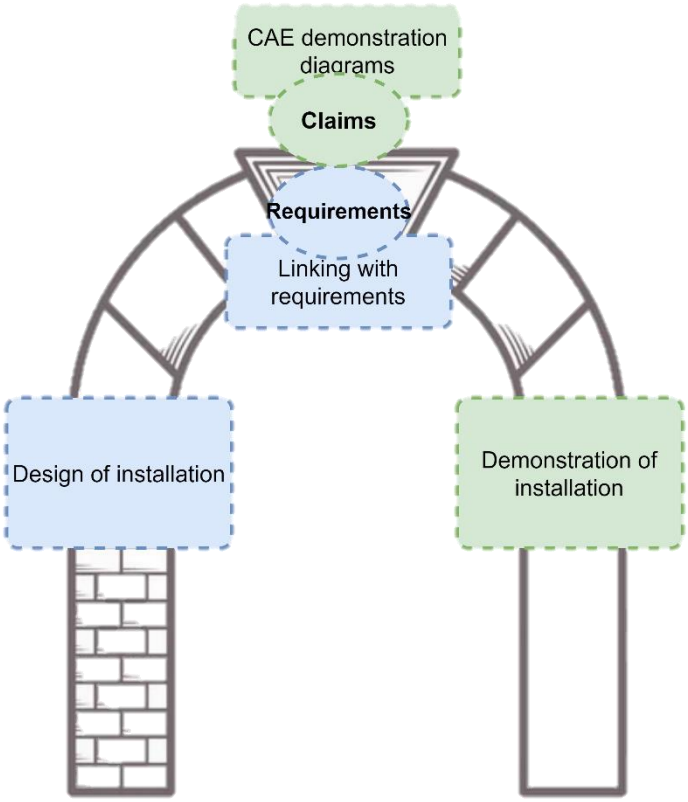


Figure 42 Link between design and safety demonstration

This link is established in our metamodel (cf. Figure 43).

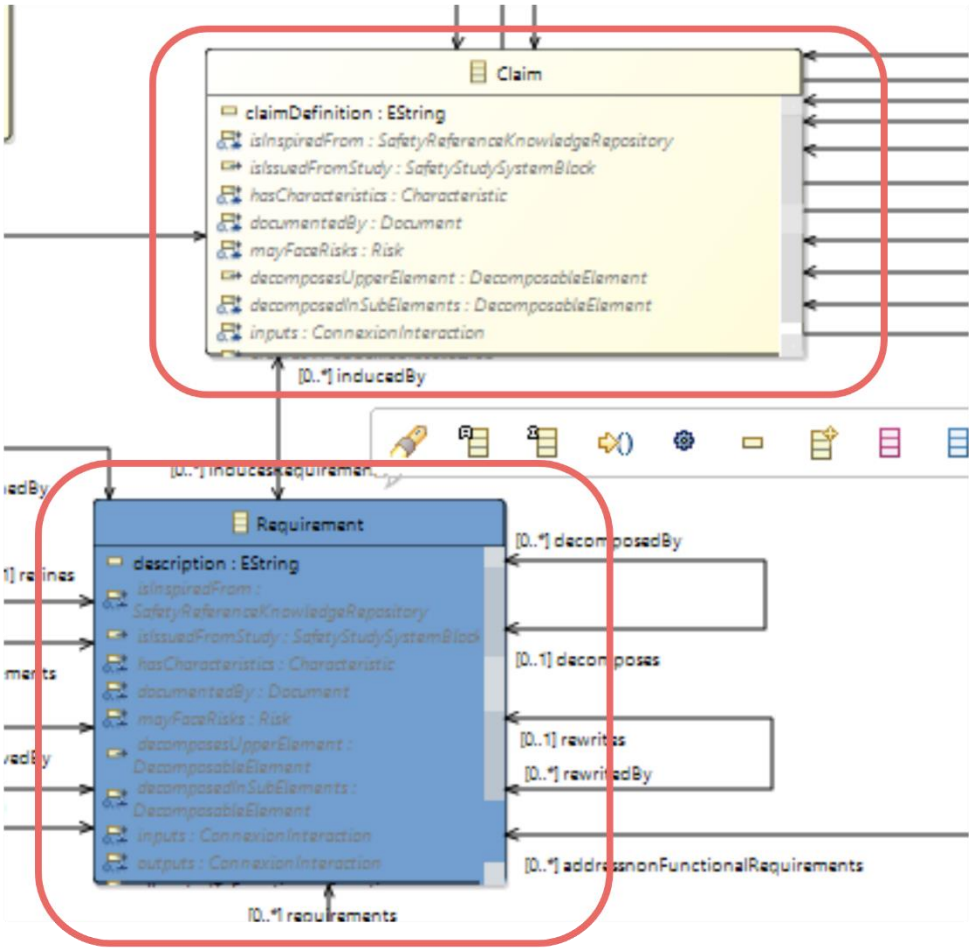


Figure 43 Concepts of claims and requirements in Safety Demonstration Specification View

Also, we can find in the metamodel the argument blocks.

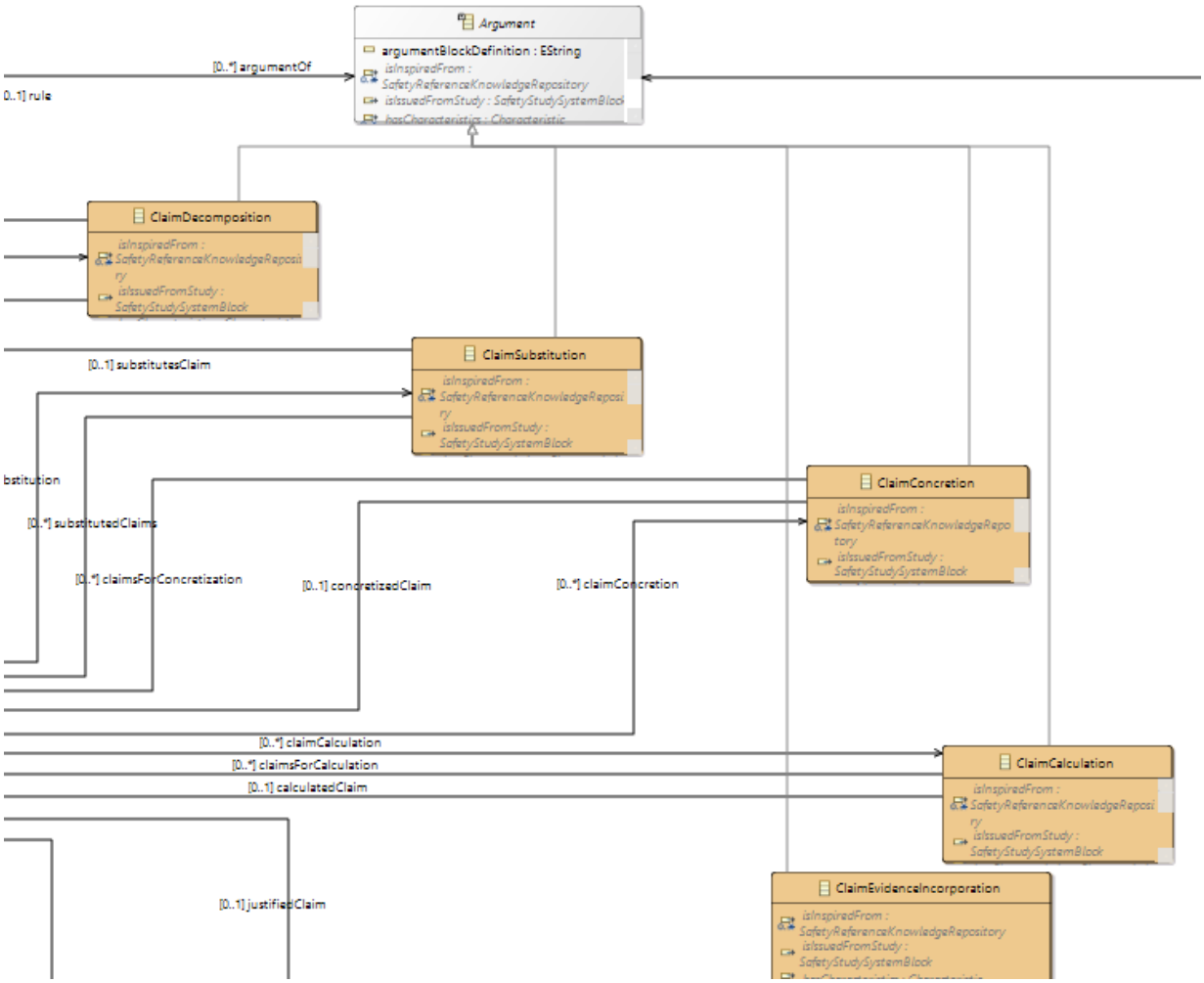


Figure 44 Concepts of CAE arguments in Safety Demonstration Specification View

The argument block "Incorporation of evidence" is related to the concept of evidence:

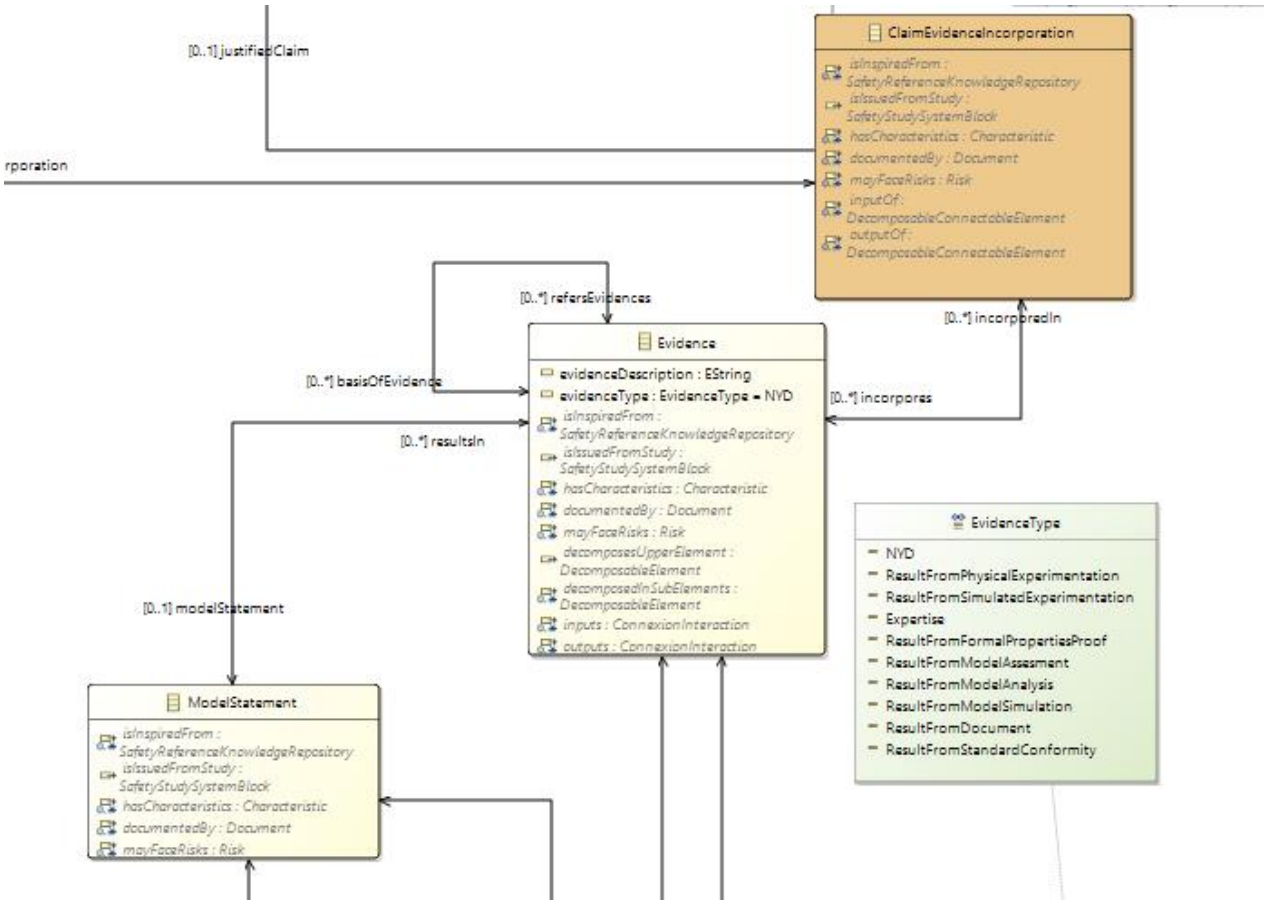


Figure 45 Concepts of EvidenceIncorporation and Evidences in Safety Demonstration Specification View

5.1.5.2. Contribution 2.2: Concrete syntaxes (graphical and textual/tables) and semantics

We use meta-model compliant languages that allow us to build models. These models have a graphical representation which itself conforms to the concrete graphical syntax of the language. Different concepts representing a subset of our complete metamodel are mapped onto graphical elements that will have rules for manipulation, binding etc.

In our case, we decided to extend an existing methodology to include these new concepts, diagrams, and processes, some diagrams are new, and others are extensions of pre-existing diagrams (such as functional or physical architecture diagrams). In general, these diagrams, tables/matrices are concrete graphical or

textual syntaxes based on our metamodel (abstract syntax). The concepts manipulated are a subset of the general metamodel.

Figure 46 Different diagrams of the safety method divided into our three views

After having introduced the concepts of our metamodel in each of the three views, we will explain here the three languages developed in these three views. Each of these languages has one or more concrete graphical or textual syntaxes (in the form of matrices) which allow the concepts of the language to be manipulated (cf. Figure 47). In the same logic of presentation for each of the views of their concepts in the previous section (section 5.1.5.1), we will describe here the use of languages through their graphical representation or in the form of tables/matrices.

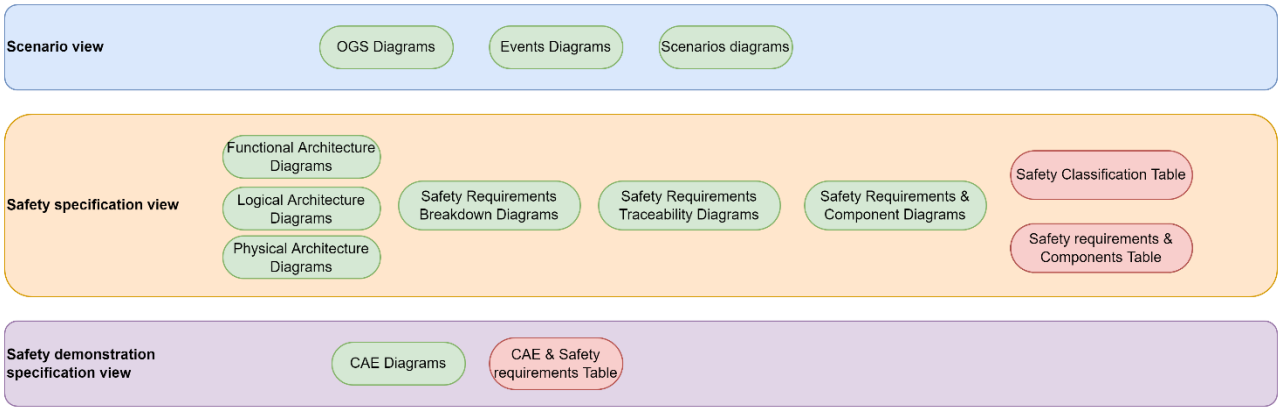


Figure 47 3 method views and its diagrams and tables

Scenario view:

Figure 48 Scenario view and its diagrams

To enable the general safety objectives to be set, to relate them to the various situations in the installation and to relate these to incident/accident scenarios, the safety engineer has the OGS diagrams at his disposal. (cf. Figure 49)

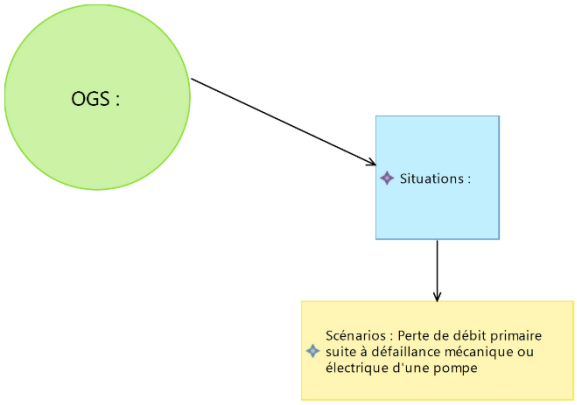


Figure 49 OGS Diagram in Scenario View

The initiating events are found in the event diagram (cf. Figure 50) classified by accident frequency group (PCC2, PCC3, PCC4, (Operating Conditions Sutdies) see Section 2.2.2.5).

Figure 50 Events diagram in Scenario View

Each of these events initiates one or more scenarios. In these scenarios, the components perform safety functions that are involved in the control or mitigation of the incident/accident.

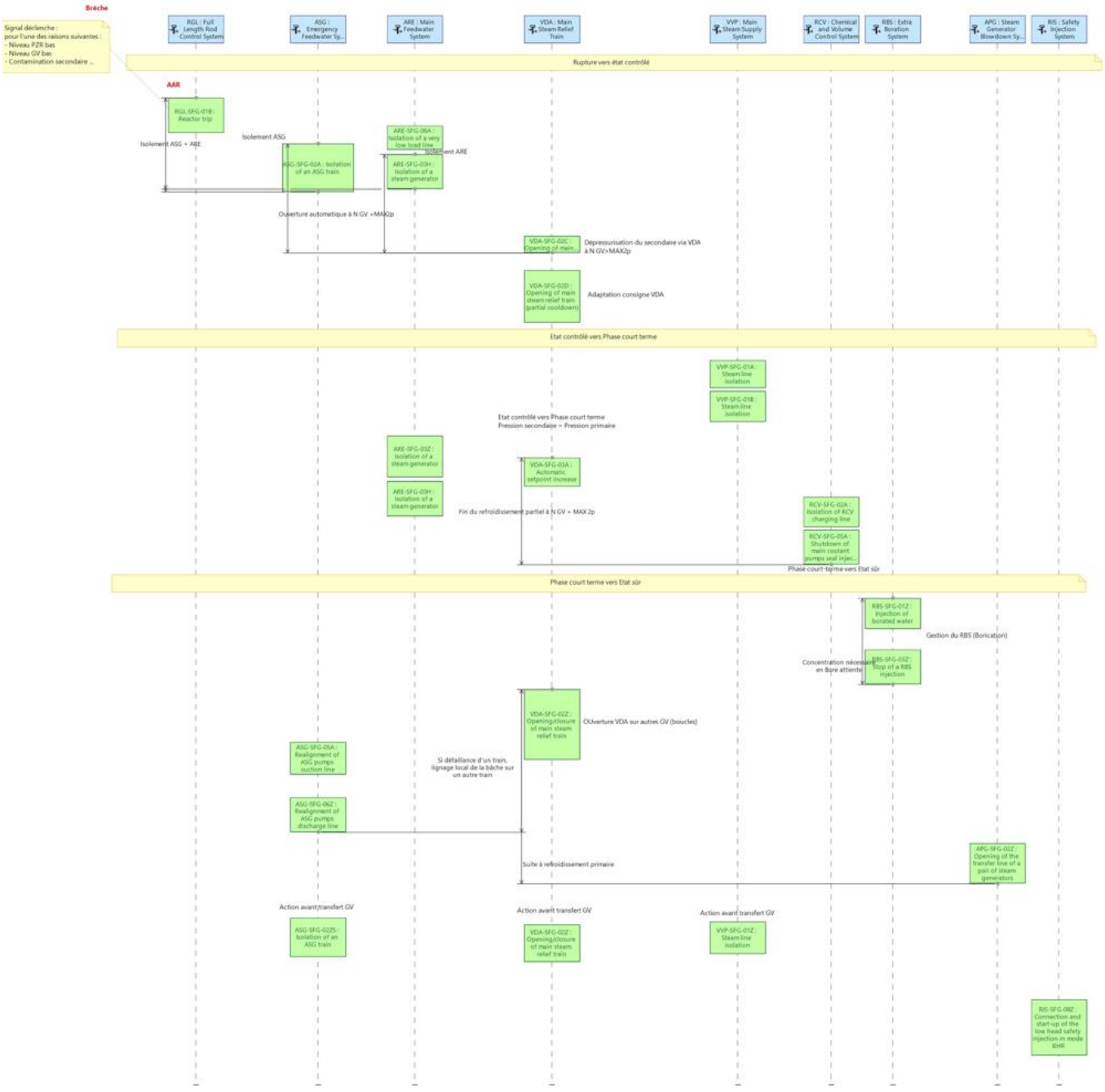


Figure 51 Scenario diagram in Scenario View

Safety requirements specification view:

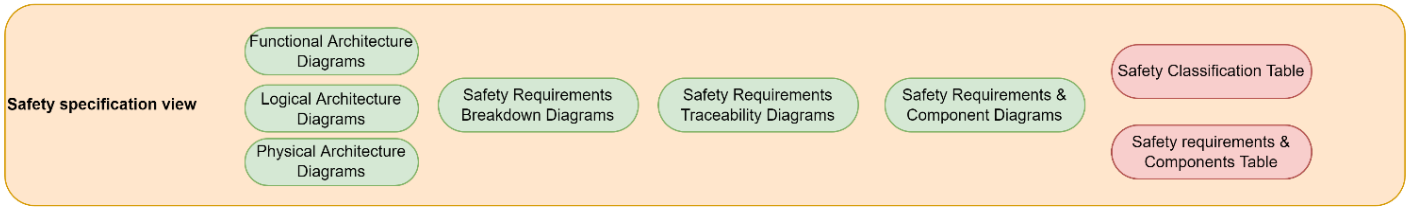


Figure 52 Safety specification view and its diagrams/matrices

In this view, engineers should be able to fill in safety classifications and qualifications as attributes of components (or on functions at a lower design maturity). The architecture diagrams, which we extend with the concepts of our metamodel, thus allow the addition of the requirement types introduced in the previous section.

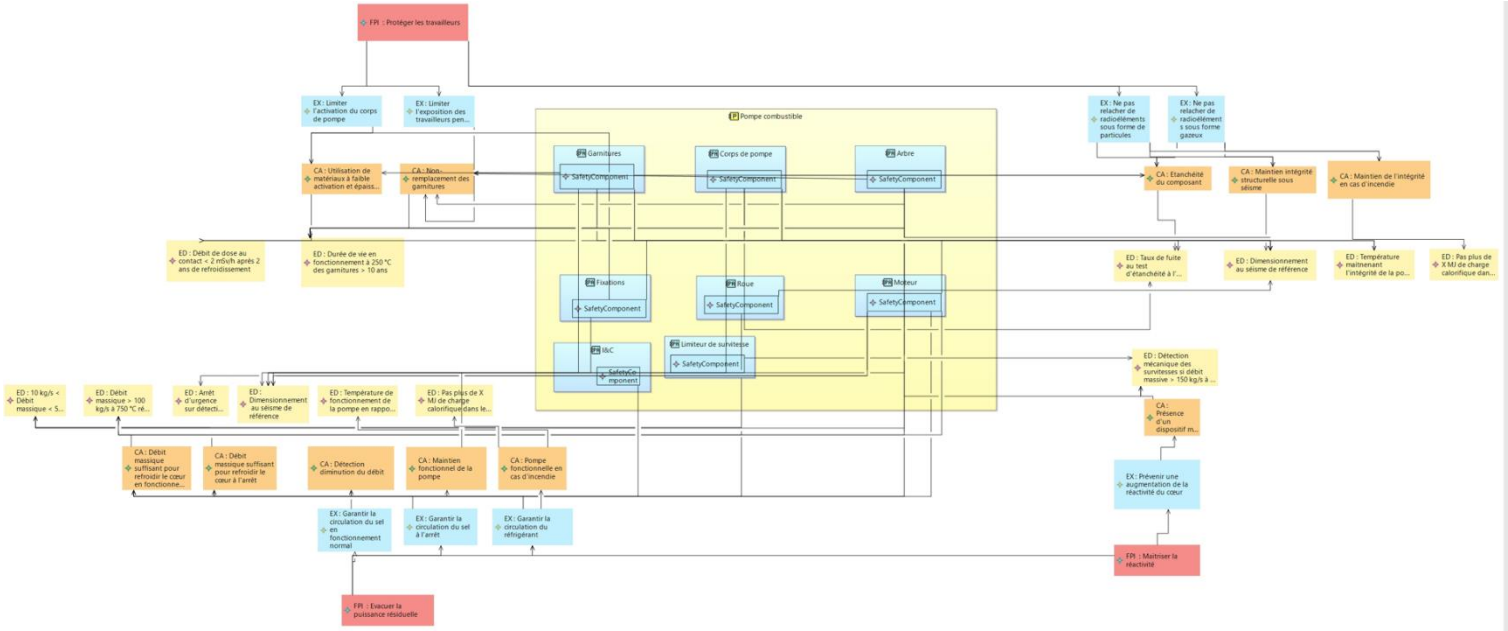


Figure 53 Extended architecture diagram for Safety Specification View

Concrete graphical syntaxes (diagrams) have been developed. These represent the elements of our abstract syntax (metamodel) to graphically visualise the traceability of requirements. These diagrams can be created or generated from other diagrams (cf. Figure 54) :

- Hierarchy and linkage diagram of safety requirements and traceability of their origins (SRBS to FPI, EX, CA, ED) :

    - This makes it possible to know, for example, from which FPI or EX, a CA is derived.
- Diagram of traceability of requirements to their source (scenario or risk analysis).
    - This diagram shows whether a requirement is the result of a scenario analysis or a risk analysis, e.g. in relation to an aggression.
- Diagram of requirements linked to a component.
    - This diagram shows all the safety requirements attached to a component.

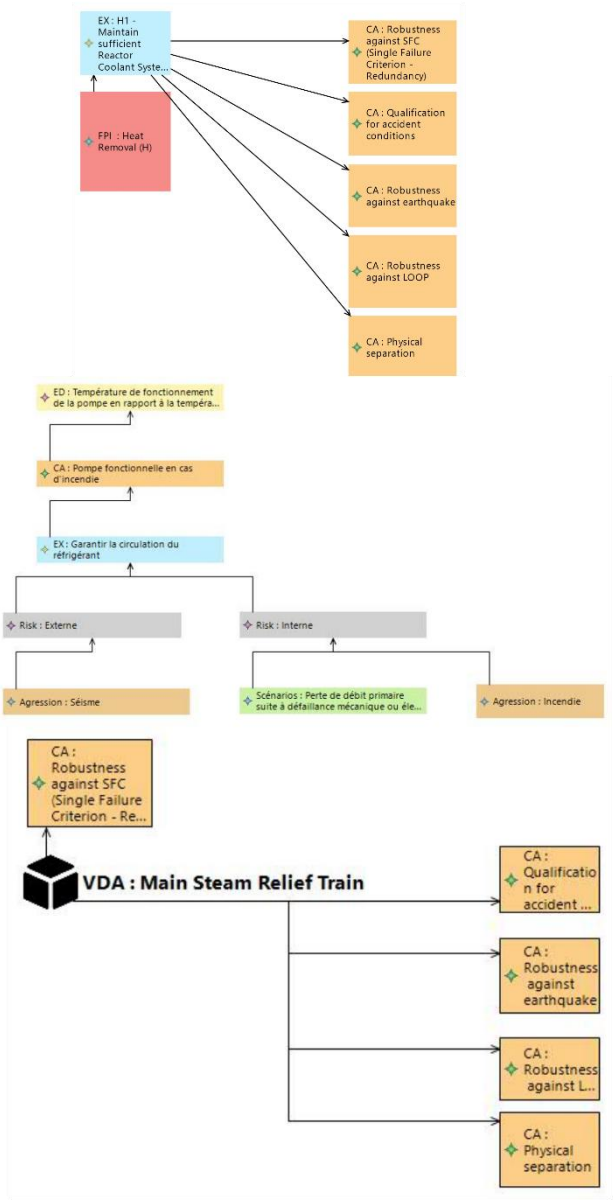


Figure 54 Diagrams of requirements for traceability and visualisation in Safety Specification View

- Allocation matrix of components and their respective safety requirements.
    - Matrix to visualise the requirements allocated to the components.
- Allocation matrix of components and their respective safety classifications.
    - Matrix to visualise the safety classes of components.

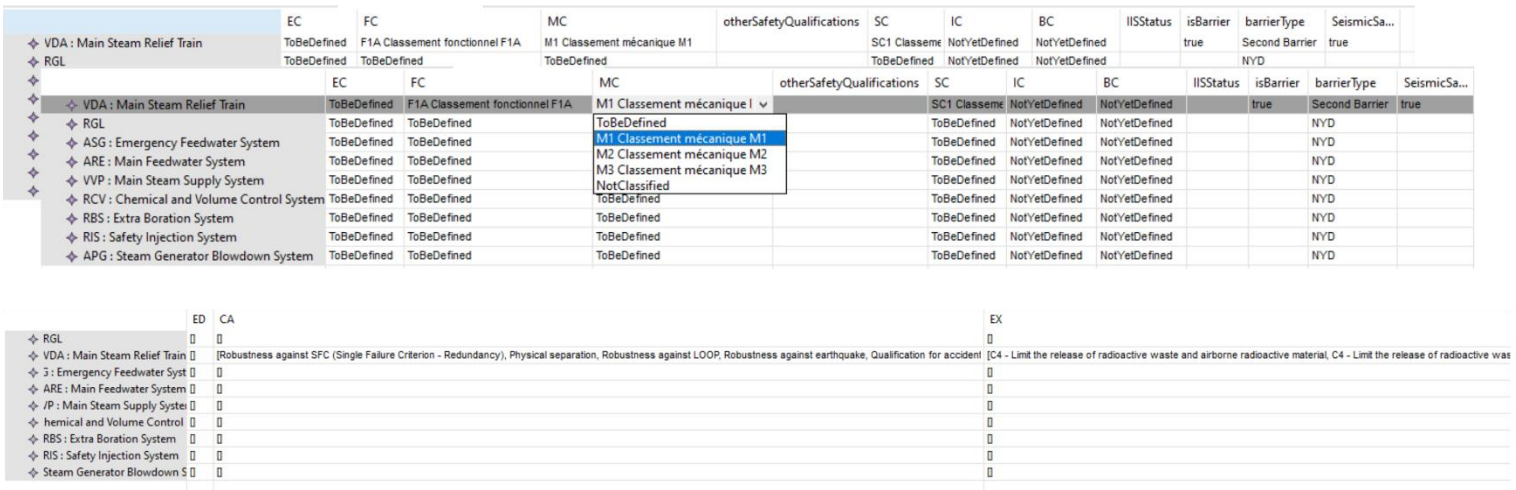


Figure 55 Component-based requirement and safety class matrices for the Safety Specification view

Demonstration specification view

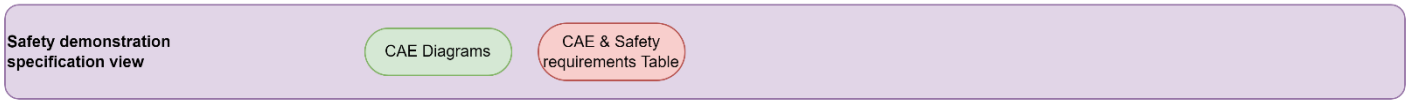


Figure 56 Safety demonstration specification view and its diagrams/matrices

In the demonstration specification view, the language essentially manipulates the concepts of the CAE framework. The diagrams and matrices used in this language are :

- Demonstration specification diagram (CAE framework and claims allocation to requirements [34], [50]).
- Development of an allocation matrix of requirements and their respective safety demonstration diagram.

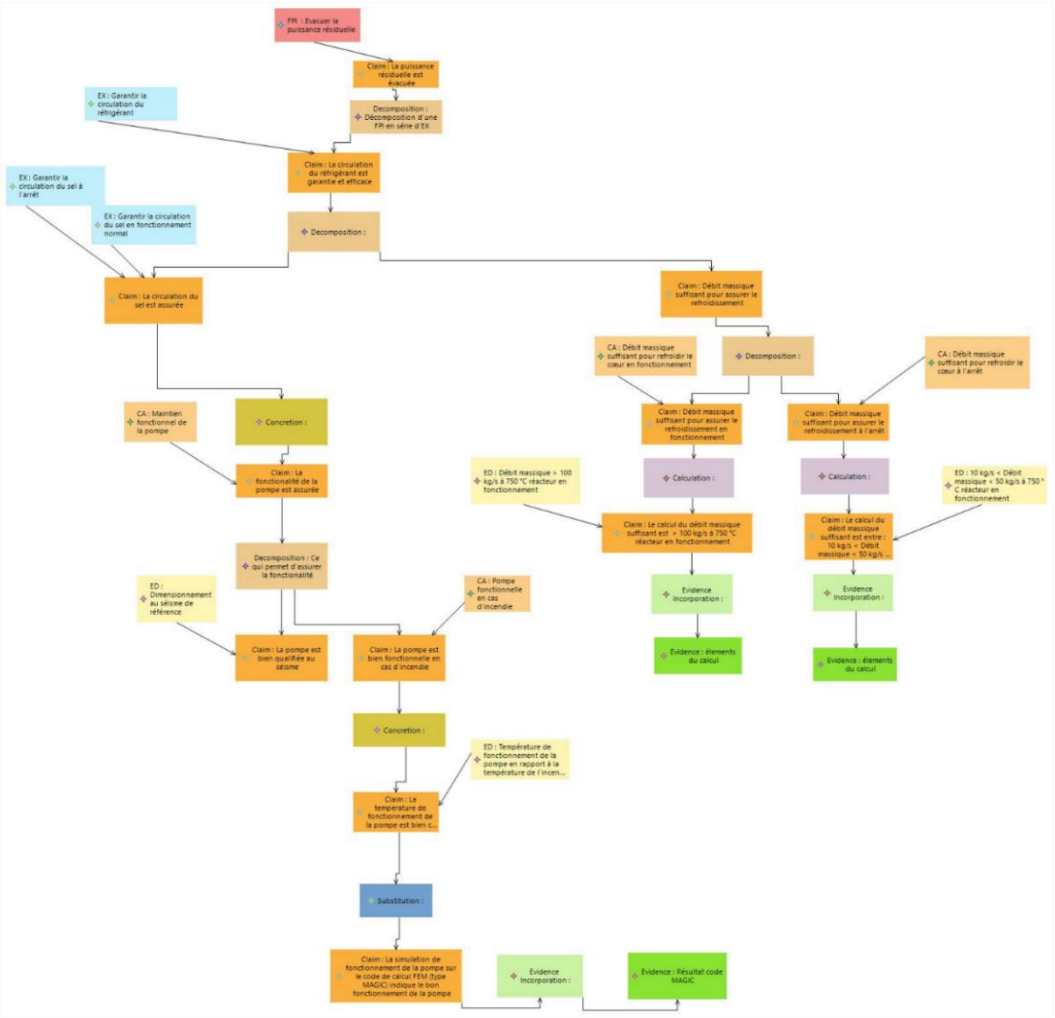
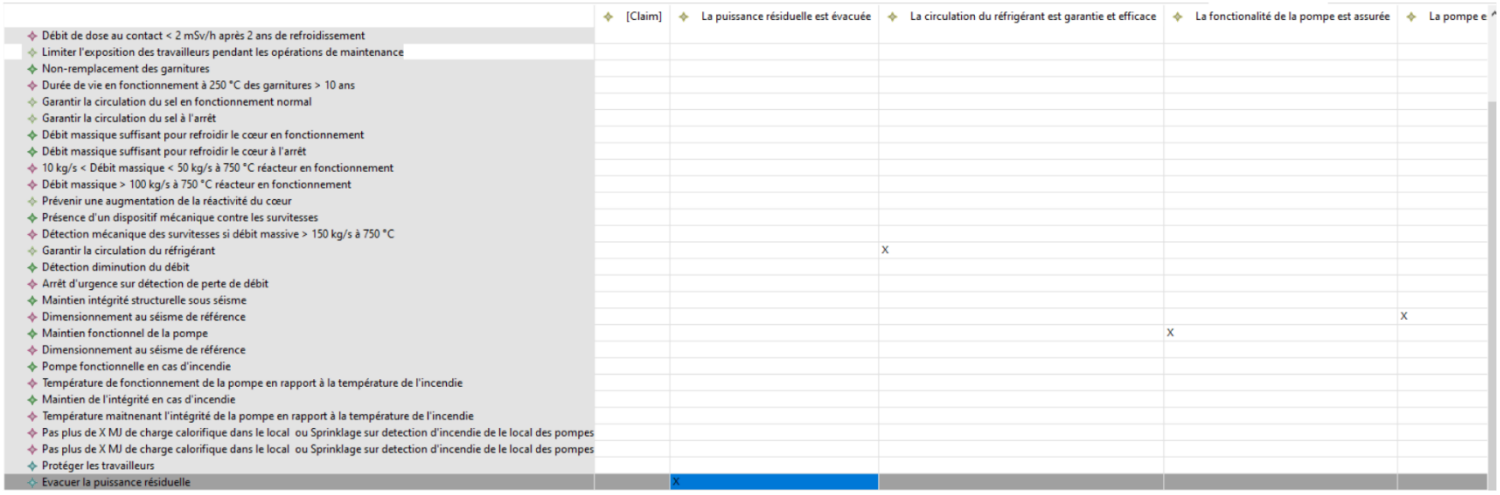


Figure 57 CAE Diagram in Safety Demonstration Specification View



	[Claim]	La puissance résiduelle est évacuée	La circulation du réfrigérant est garantie et efficace	La fonctionalité de la pompe est assurée	La pompe e
Débit de dose au contact < 2 mSv/h après 2 ans de refroidissement					
Limiter l'exposition des travailleurs pendant les opérations de maintenance					
Non-remplacement des garnitures					
Durée de vie en fonctionnement à 250 °C des garnitures > 10 ans					
Garantir la circulation du sel en fonctionnement normal					
Garantir la circulation du sel à l'arrêt					
Débit massique suffisant pour refroidir le cœur en fonctionnement					
Débit massique suffisant pour refroidir le cœur à l'arrêt					
10 kg/s < Débit massique < 50 kg/s à 750 °C réacteur en fonctionnement					
Débit massique > 100 kg/s à 750 °C réacteur en fonctionnement					
Prévenir une augmentation de la réactivité du cœur					
Présence d'un dispositif mécanique contre les survitesses					
Détection mécanique des survitesses si débit massive > 150 kg/s à 750 °C					
Garantir la circulation du réfrigérant			X		
Détection diminution du débit					
Arrêt d'urgence sur détection de perte de débit					
Maintien intégrité structurelle sous séisme					
Dimensionnement au séisme de référence					X
Maintien fonctionnel de la pompe				X	
Dimensionnement au séisme de référence					
Pompe fonctionnelle en cas d'incendie					
Température de fonctionnement de la pompe en rapport à la température de l'incendie					
Maintien de l'intégrité en cas d'incendie					
Température maitnenant l'intégrité de la pompe en rapport à la température de l'incendie					
Pas plus de X MJ de charge calorifique dans le local ou Sprinklage sur detection d'incendie de le local des pompes					
Pas plus de X MJ de charge calorifique dans le local ou Sprinklage sur detection d'incendie de le local des pompes					
Protéger les travailleurs					
Evacuer la puissance résiduelle		X			

Figure 58 Allocation matrix of requirements and their respective safety demonstration diagram in Safety Demosntration Specification View

5.1.5.3. Contribution 2.3: operational approach

Analysis of the literature of good practices in the conduct of nuclear safety demonstration found in the regulations, in the guides of the safety authorities (ASN, ONR etc.) and international authorities (IAEA) as well as in the guides of the operators (EDF, CEA etc.), has made it possible to extract a set of process that compose the expected usages and activities that are described in this section.
As mentioned in the previous sections, this method is divided into 3 views:

Scenario view (cf. 5.1.5.1, Figure 59) in which are set:

- Safety Global Objectives (OGS);
- The allocation of these objectives to functioning situations of the installation.
- The description of events and incidental/accidental scenarios.

In this scenario section, the safety engineer will use the developed OGS diagram, event and scenario diagrams to describe the different incident and accident scenarios triggered by various initiating events. The functions performed by the components in these scenarios will be useful in the safety specification view.

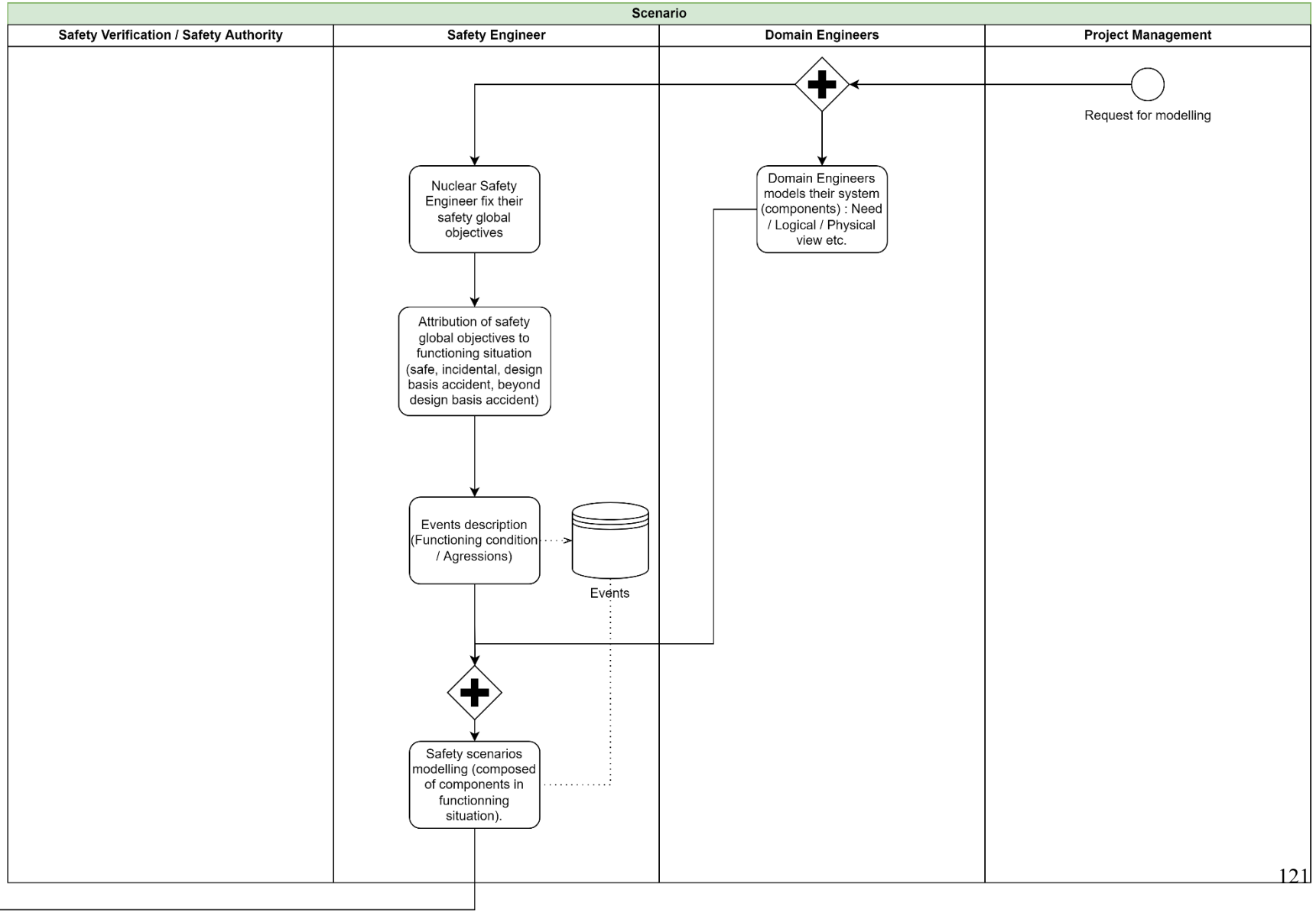


Figure 59 Safety Scenario BPMN

Safety requirements specification view (cf. 5.1.5.1, Figure 60**),** in which are set:

- Items important for protection (IIP).
- IIP classifications and qualifications.
- Safety requirements and their allocation to components

With the analysis of the various scenarios, the equipment important for protection is identified. Depending on the role performed, safety classes as well as qualifications to the aggression are specified. Based on this and various risk analyses and applicable regulations, multi-level requirements are specified for each component and equipment. This work is based on collaboration between the safety engineers and the various other project areas. In this context, the sharing of architecture diagrams with our safety extensions, classes, and qualification attributes as well as requirements related diagrams and matrices (RPBS, Traceability, Component Requirements) facilitate information sharing, communication and understanding.

.

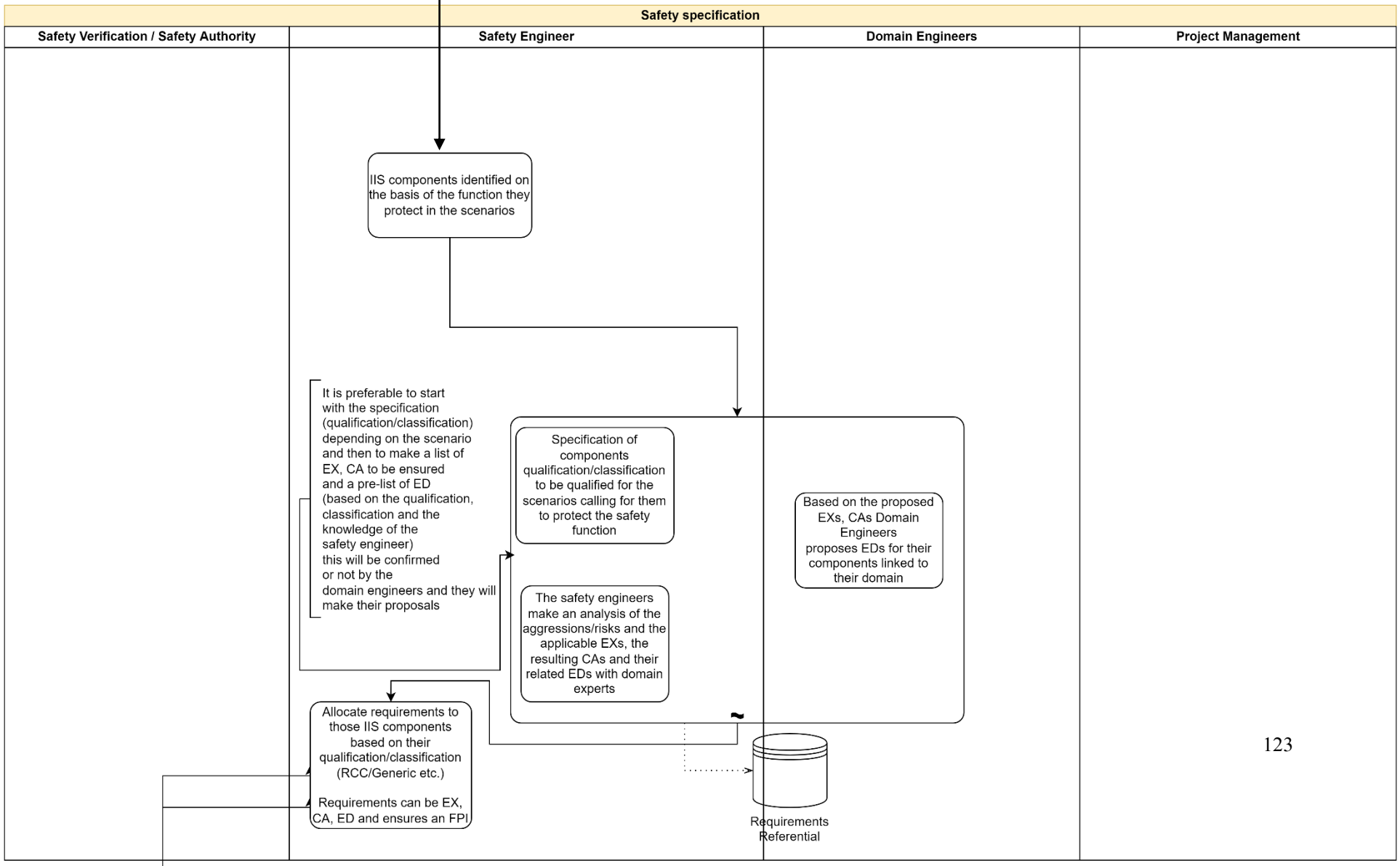


Figure 60 Safety Specification BPMN

Demonstration specification view (cf. 5.1.5.1, Figure 61**),** in which are set:

- Allocation of requirements to claims (enabling the design/demonstration link).
- The CAE framework [50] [34].

As the design progresses, the specification of the desired demonstration is carried out using the CAE framework and the matrices for allocating requirements to the claims to be demonstrated.

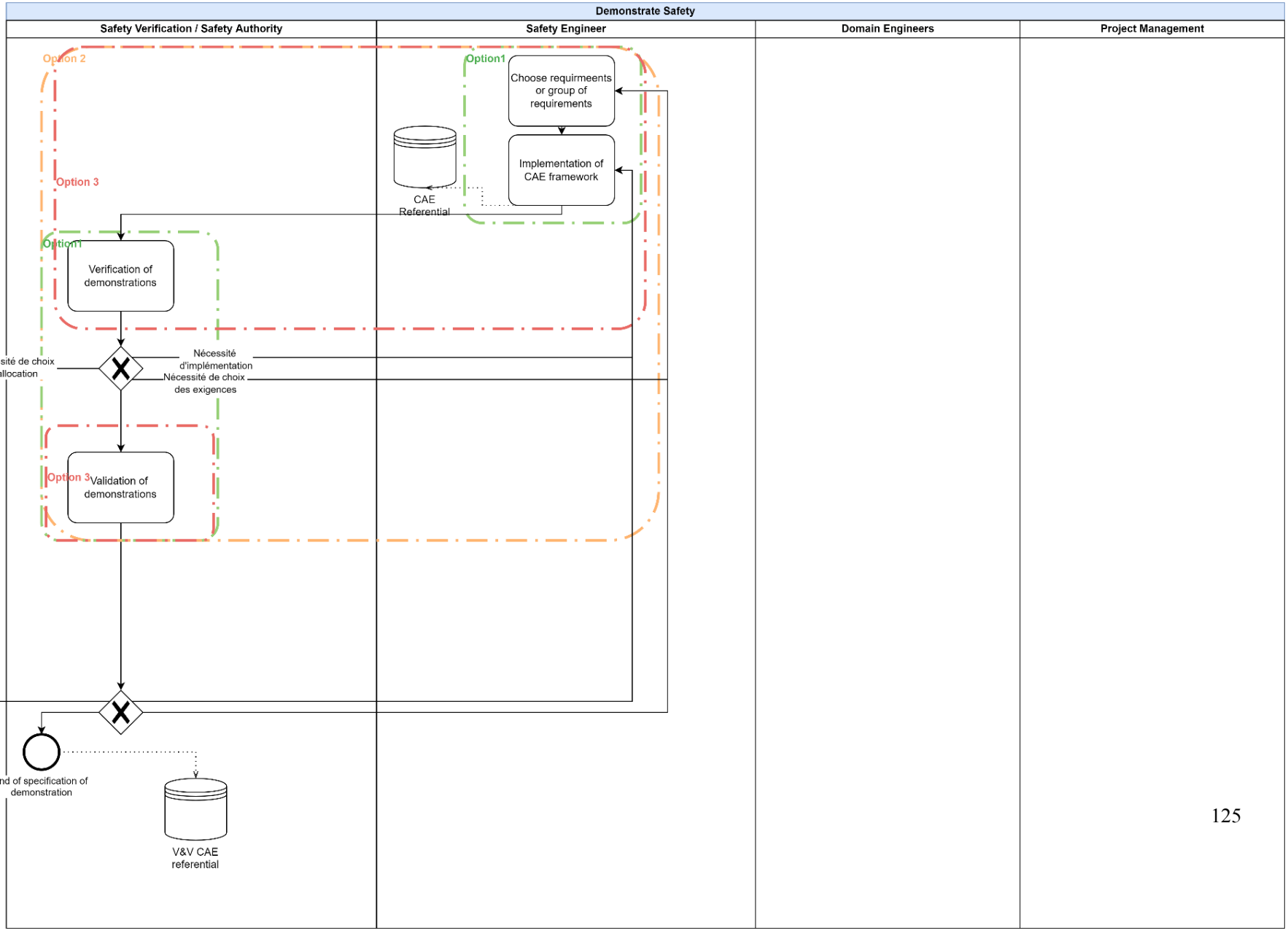


Figure 61 Safety Demonstration BPMN

We have thus seen in the previous sections the first three elements of the expected approach to Pillar 2:

- The development of a meta-model highlighting three complementary and interrelated views on important safety concepts.
- The proposal of languages allowing to establish models, with the more usual graphical concrete syntax in MBSE, but also matrices linked to these languages.
- An operational approach that fits into the system engineering approach and indeed into an MBSE framework.

In the following part, and to respond to pillar n°3, we develop the tooling phase aiming at an ecosystem of supporting IT tools. It covers both the AI tools implementing the AI techniques (pillar 1) and the actual tooling of the method introduced above (pillar 2).

5.1.6 Pillar 3: Ecosystem of tools

Figure 62 Pillar 3 and tooling

We will therefore introduce this part by separating the tools specific to pillar 1 and those of pillar 2 and then integrating them into a coherent and interoperable ecosystem of tools. It is indeed necessary to link the contributions in AI and MBSE by considering the question of interoperability (tools, languages, models) and by proceeding by means of adapted HMI (Human Machine Interface).

5.1.6.1. Deployment of AI tools

The first version of the algorithm was made available to engineers through, initially, APIs (cf.Figure 63), which notably allow calls to functionalities and work on interoperability through scripts:

- Reader API:
  - Document Layout Detection
  - Text, tables, figures extraction
  - OCR, table structure recognition
- Extractor API (the classification algorithm trained on our requirements which takes as input the output of the API reader):
  - Automated requirements extraction using transformers models
- Analyzer API (with some ongoing work on requirements engineering):
  - Semantic duplicates detection, automatic clustering
  - [WIP] Quality analysis
  - [WIP] Contradiction detection
  - Requirements comparison

The finalisation of the webapp is still a work in progress (cf. Figure 64):

- [WIP] Python backend (REST API with FastAPI) + Angular frontend

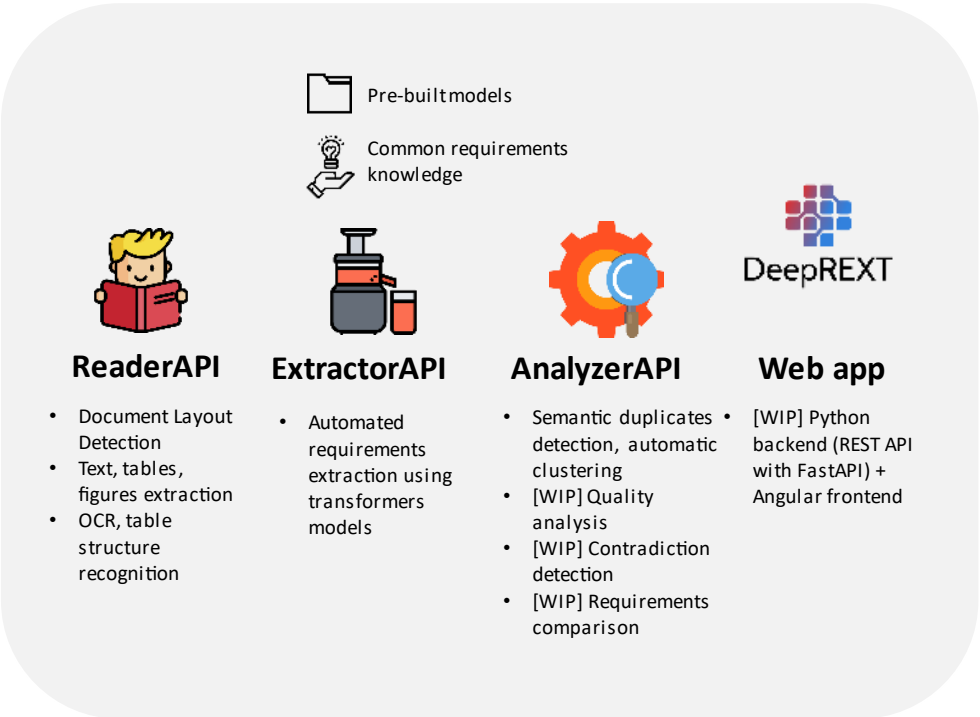


Figure 63 APIs and webapps for algorithms

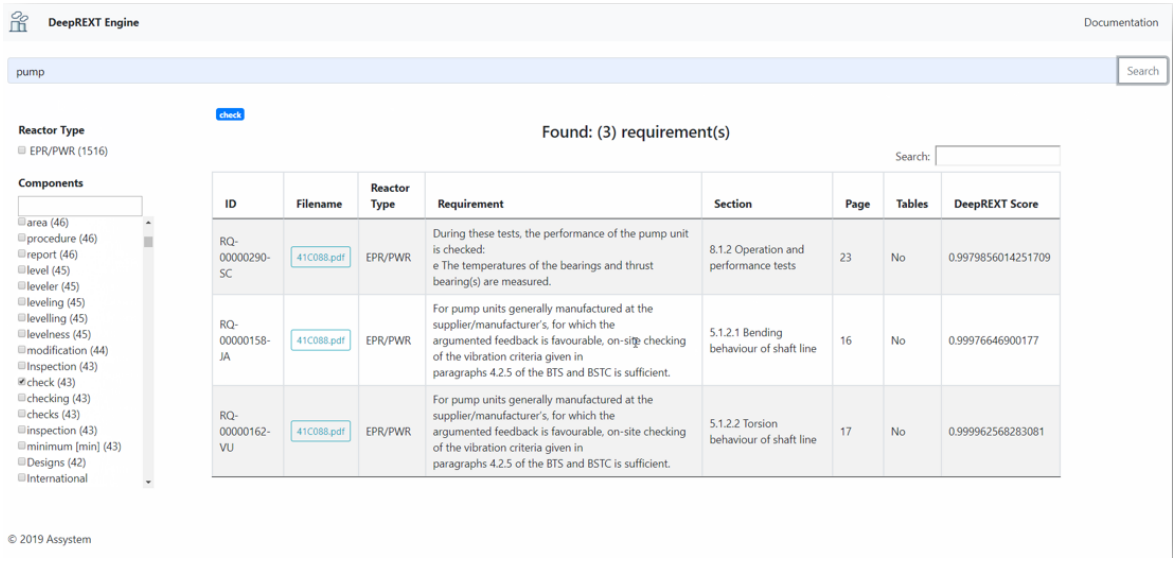


Figure 64 Webapp deploying requirements extraction algorithm

5.1.6.2. Contribution 3.1: Deployment of the work through the Capella software

The Capella tool [101] was chosen because of its extensive use in the company's projects. Also, the open-source aspect of the tool as well as the development possibilities are interesting for our work. Efforts have been made to integrate this method into an add-on for this software. It is therefore around this software, the Arcadia method [102] (Figure 65) and the Arcadia DSML language [101] [102] that we are integrating our current research to integrate our concepts and methods specific to safety demonstration.

Development is done under the Capella Studio platform which provides a fully integrated development environment that aims to facilitate the development of extensions for Capella.

It provides developers with a platform containing both:

- Kitalpha and Eclipse modelling frameworks and tools
  - Eclipse [103] *a project, broken down and organised into a set of software development sub-projects, of the Eclipse Foundation aiming to develop an open source software production environment that is extensible, universal and versatile, based primarily on Java. Eclipse is both a Development Environment, a framework, and a platform".*
  - Kitalpha [104] *an environment for developing and executing Model-Based Engineering (MBE) work for system, software and*

hardware engineering, it makes eclipse integrate the System Engineering ISO/IEC/IEEE 42010:2011 standard [60]"

— Libraries of the Capella modelling software for engineering.

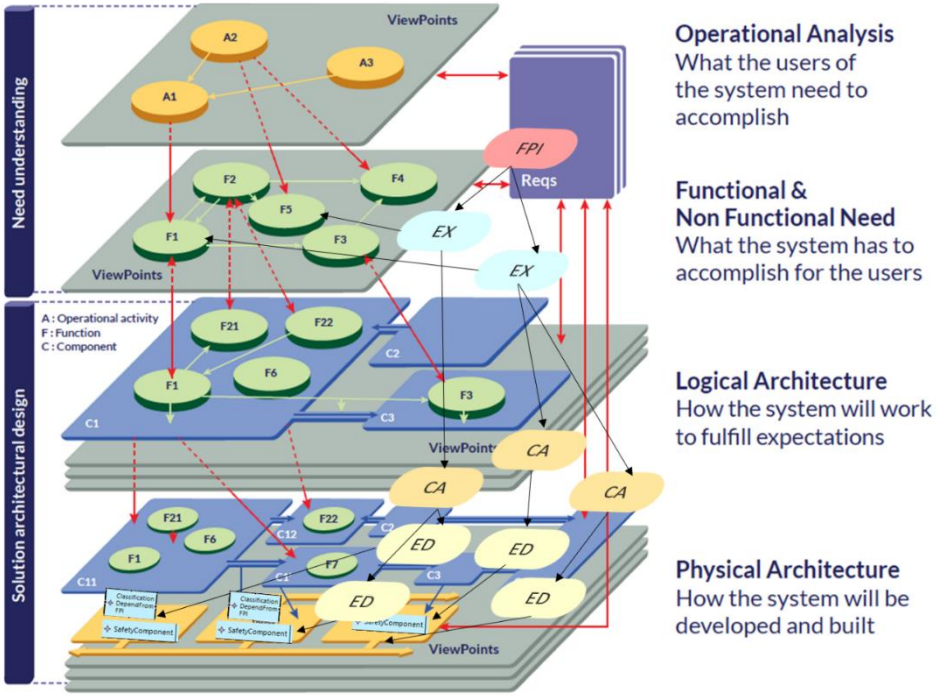


Figure 65 Arcadia method with the addition of the safety add-on

Integration of the metamodel with the Capella metamodel

As explained in section 5.1.5.1, elements of the metamodel have been identified as pivots between the metamodel present in Capella and the concepts of our metamodel. These pivots elements are those identified and formalised in various normative documents such as ISO 15288 [39] or the ARCADIA method of Thales, which the CAPELLA tool allows to apply. Also, the highest level element of our metamodel from which each class inherits "SafetyStudySystemBlock" extends the highest level class of Capella "capellamodeller.SystemEngineering". Further extensions through class associations have been established between the elements of our metamodel and the Capella metamodel (cf.Figure 66))

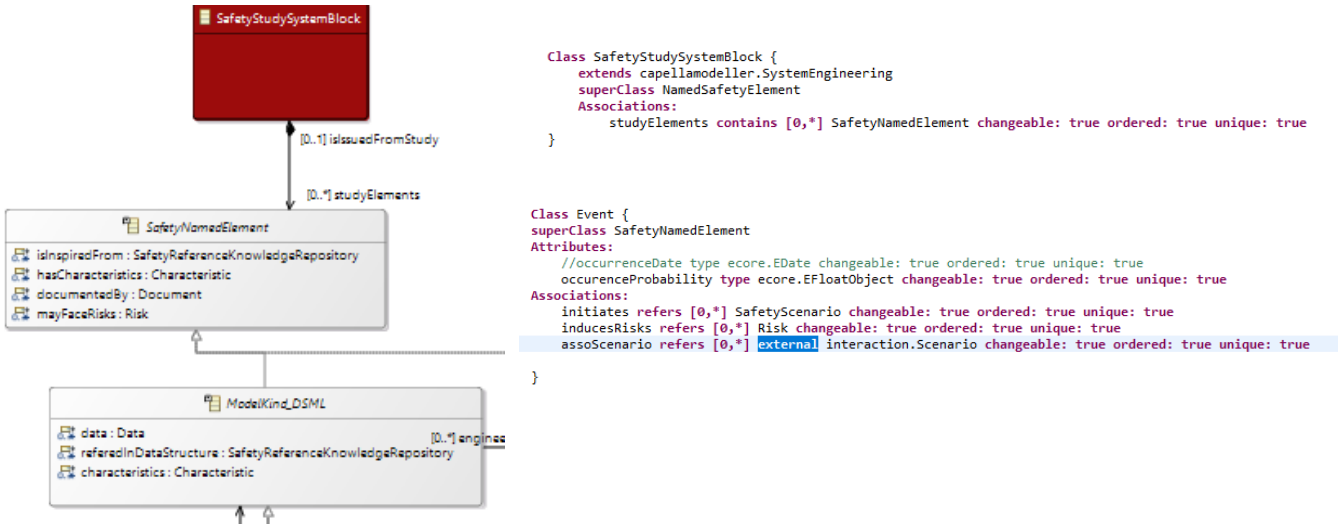


Figure 66 Integration of our metamodel to Capella's metamodel

Development of diagrams in Capella

The diagrams mentioned in section 5.1.5.2, were developed in Capella. A total of 12 diagrams/matrices were either created or extended from existing diagrams. (cf.Figure 67)

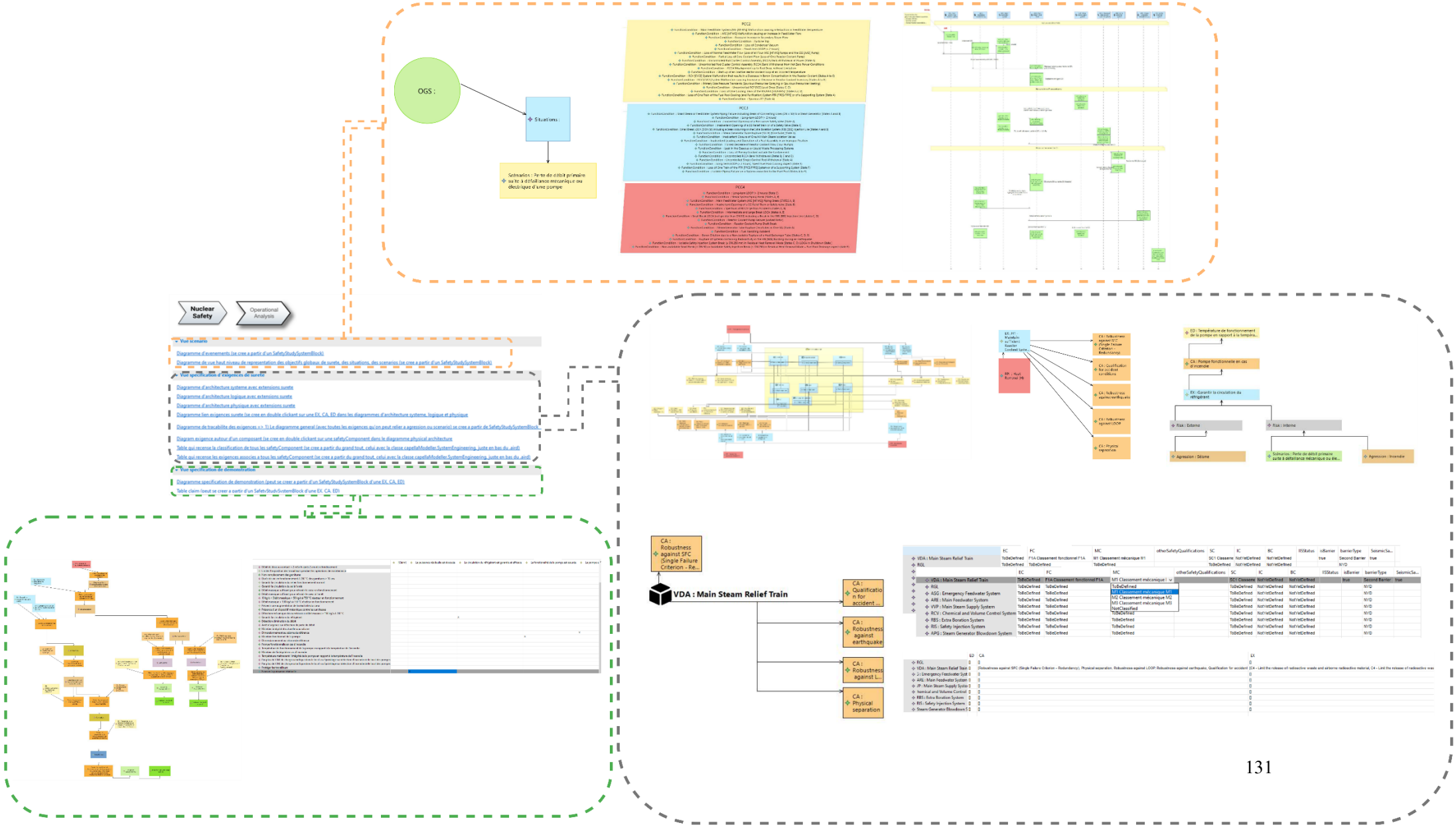


Figure 67 Linking of modelling views and modelling diagrams

Adding the different activities to the Capella activity diagram

The future objectives of this work will be to integrate these modelling practices into projects with a nuclear safety dimension. To do this, we have begun by integrating our safety diagram creation activities into the Capella activity diagram (called "workflow" in the software cf. Figure 68). The objective will be to take advantage of feedback on the evaluation of the method to identify possible improvements to the diagrams and matrices. We could also consider the possibility of adding new diagrams. Also, more precise processes could be described on the use of such or such activities (in relation to the method's diagrams) to be used according to the project's progress phases.

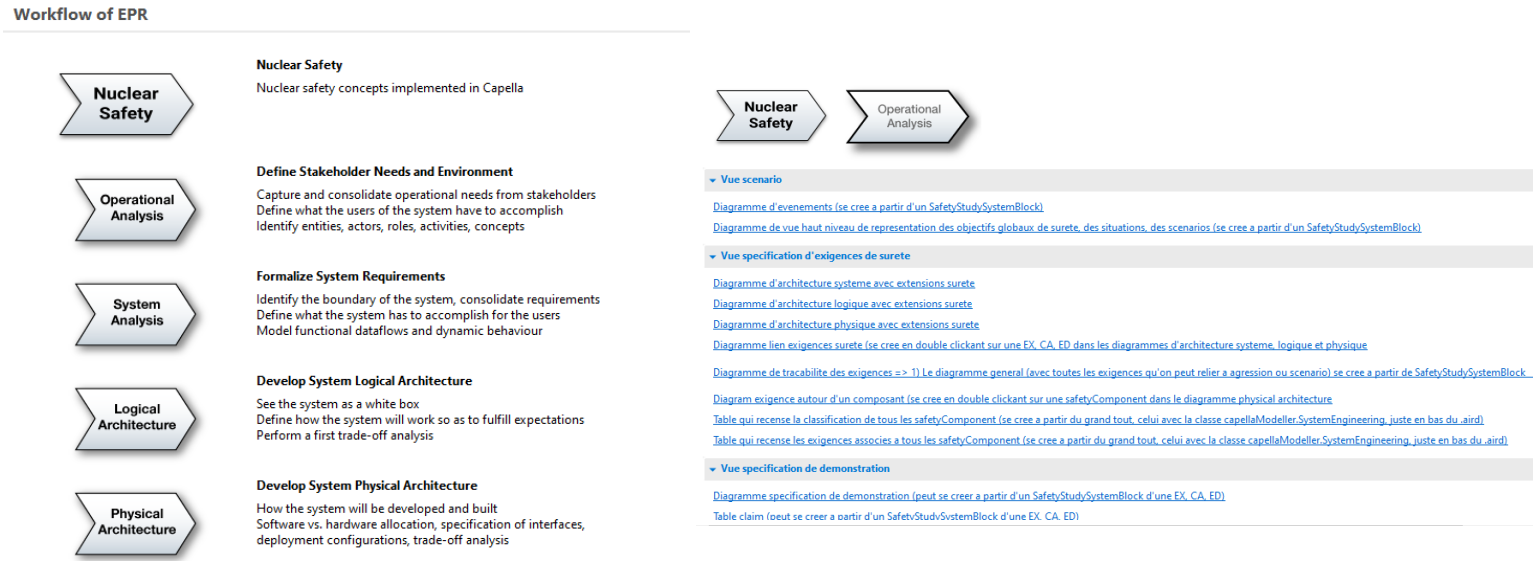


Figure 68 Adding method activities to the Capella workflow

Capella features for the REK (Repository of Expertise and Knowledge)

The Capella software offers tools to move towards the concept of "Repository of Knowledge and Expertise" described in section 5.1.5. Although the solution is not optimal, we can save parts of models that can be reused in other diagrams, projects, etc. This functionality described in [101] is called "REC/RPL" in Capella (Replicable Element / Replicable Pattern). We demonstrate this in the Figure 69, through the reuse of a part of a demonstration specification model around a fire case.

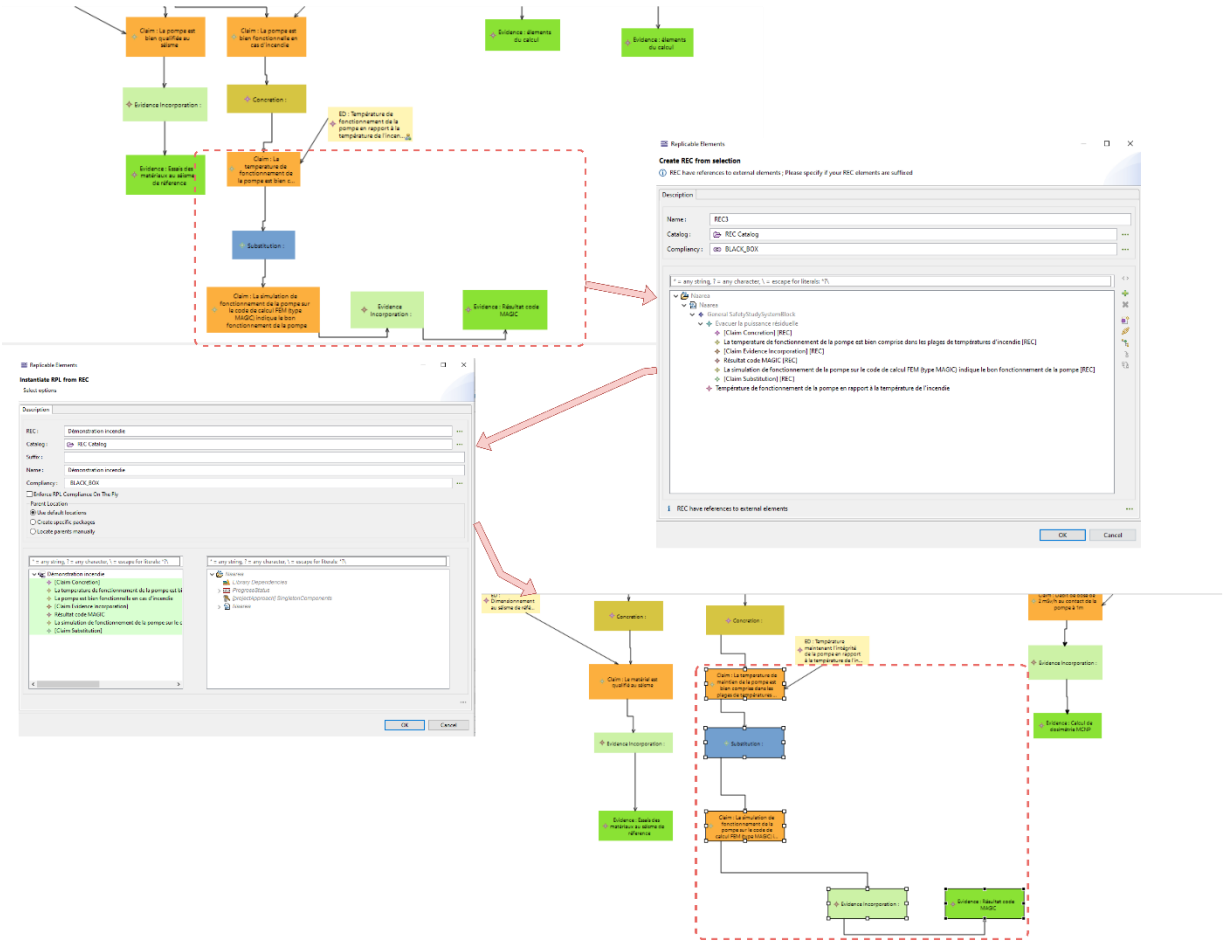


Figure 69 Use of Capella's REC/RPL function for the Repository of Expertise and Knowledge

5.1.6.3. Contribution 3.2: Extension of a Python library for interoperability via API between software and AI algorithms

In this part we will present the means used to integrate the use of the AI algorithms presented in section 5.1.3 to the modelling activities on the Capella software. To do so, we have worked on the interoperability of AI algorithms in the use of models. We will present the results in more detail in the case study.

Adaptation of Python4Capella to our metamodel concepts

In a first step it was necessary to adapt the Python4Capella library [105] which allows to interact with Capella models through the use of Python. This offers many possibilities of interoperability; however, it was necessary in a first step to adapt the library to our add-on (cf.Figure 70).
To do this, the following steps were taken:

- Addition of the "get_safet_study_system_block" function in the modules of the "SystemEngineering" class through the "ownedExtensions" module. As a reminder, the element containing our metamodel (cf.Figure 66) extends the highest-level element of Capella. Through this extension, we recover our safetystudysystemblock.
- Definition of the SafetyStudySystemBlock class by making it inherit from SystemEngineering. Thus, we get all the modules of this inherited class. In the initiation of this class, the path to the metamodel has been modified by ours as well as by the metamodel element concerned (here SafetyStudySystemBlock and then the "self" element in each of the classes described).
- The classes FPI, EX, CA, ED, Classification as well as Safetycomponent were in turn described by making them inherit from the created class "SafetyStudySystemBlock".
- Finally, scripts have been written to perform functions to achieve the interoperability objectives:
    - Adding and associating safety requirements to safety components.
    - Import of safety requirements (FPI, EX, CA, ED).
    - Extraction of information from the metamodel for querying AI APIs.
    - AI API call.

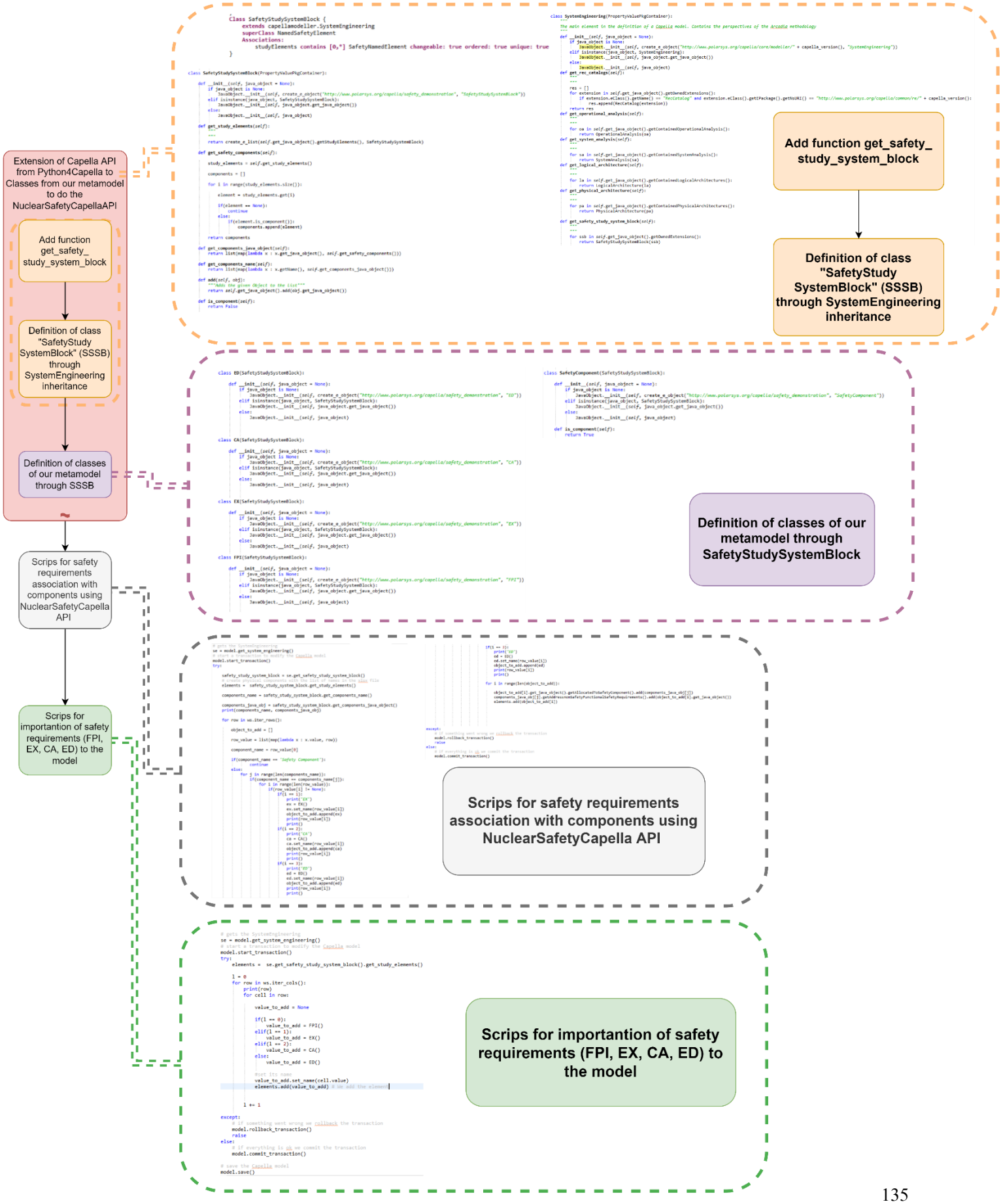


Figure 70 NuclearSafetyCapellaAPI and scripts

Script for AI interoperability with MBSE

As described in the principal script (previous section), it is through the API call that we query our algorithms. We first extract the information from the model through the Python4Capella modification, and then run the queries. The retrieved information is then fed back into the model if it satisfies the user concerned (cf.Figure 71, Figure 72). This choice is made via a graphical interface for selecting the applicable requirement and its type (FPI, EX, CA, ED). Through this interface, the user is also able to consult the origin of the requirement in the context of the document in PDF format.

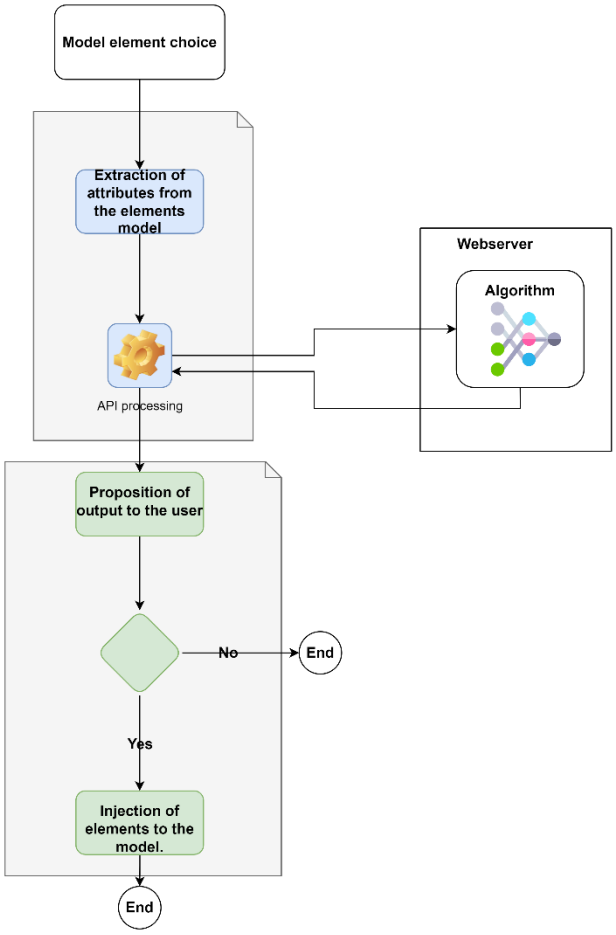


Figure 71 Generic Interoperability between AI and MBSE

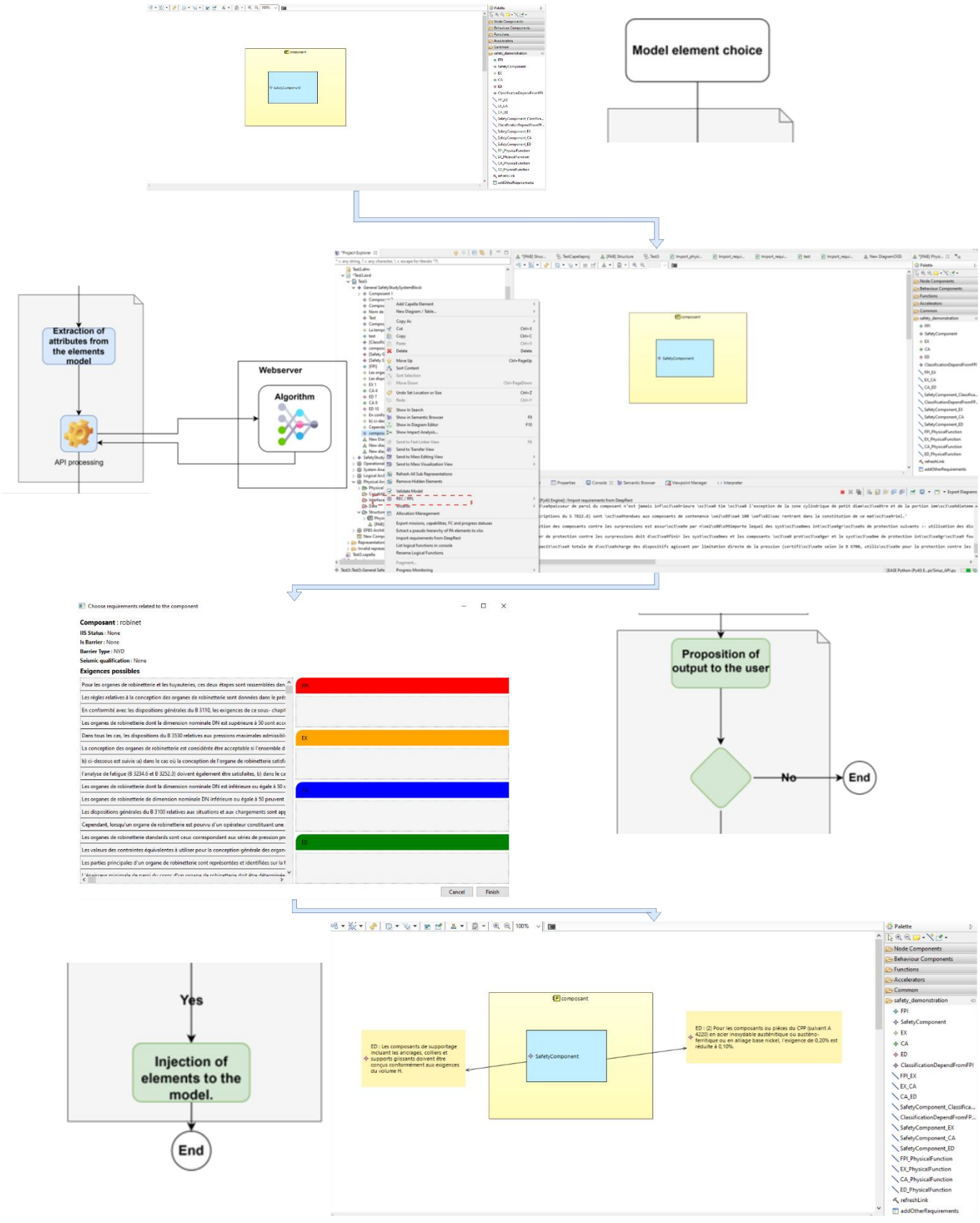


Figure 72 Integration of AI to requirements modelling step

Several user scenarios have been set up, which we will not detail because they approach the case illustrated in the Figure 71. What really differs is the type of research performed on the requirements. In the first case (cf Figure 73), the user uses a simple search engine (weighting methods type [106]). In a second case, the one illustrated in the Figure 72 , the search first uses an augmentation of the search terms through synonyms of the selected component (via the WordNet library [107]). This is then coupled with domain rules linked to metadata (cf 5.1.3.2) which filters the requirement proposal space to the user. In a third case (cf Figure 75)., The search is called "semantic" because it is the linguistic hint used to generate a vector space from all the requirements in the project. Once this space has been generated, the selected requirement is compared (in terms of cosine distance) with the other requirements.

Figure 73 Requirements search engine

Figure 74 Requirements search with term expansion by synonym and filtering by domain metadata

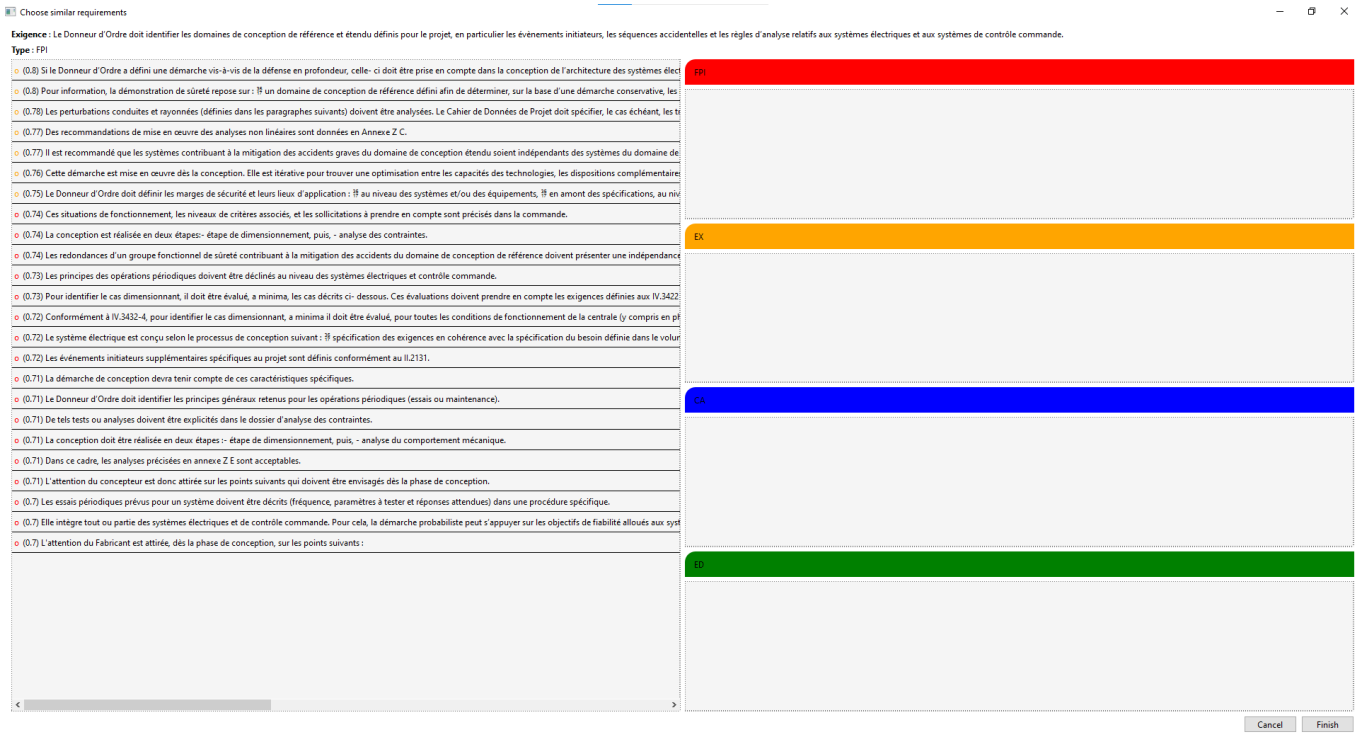


Figure 75 Search for semantically similar requirements

5.2 Summary of contributions

We summarise in Figure 79 the contributions according to each of the pillars. These works propose seven main contributions around artificial intelligence (pillar 1) and MBSE (pillar 2) for nuclear safety and their tooling and interoperability (pillar 3). In the following section, we will present an application of these contributions on two nuclear installation systems.

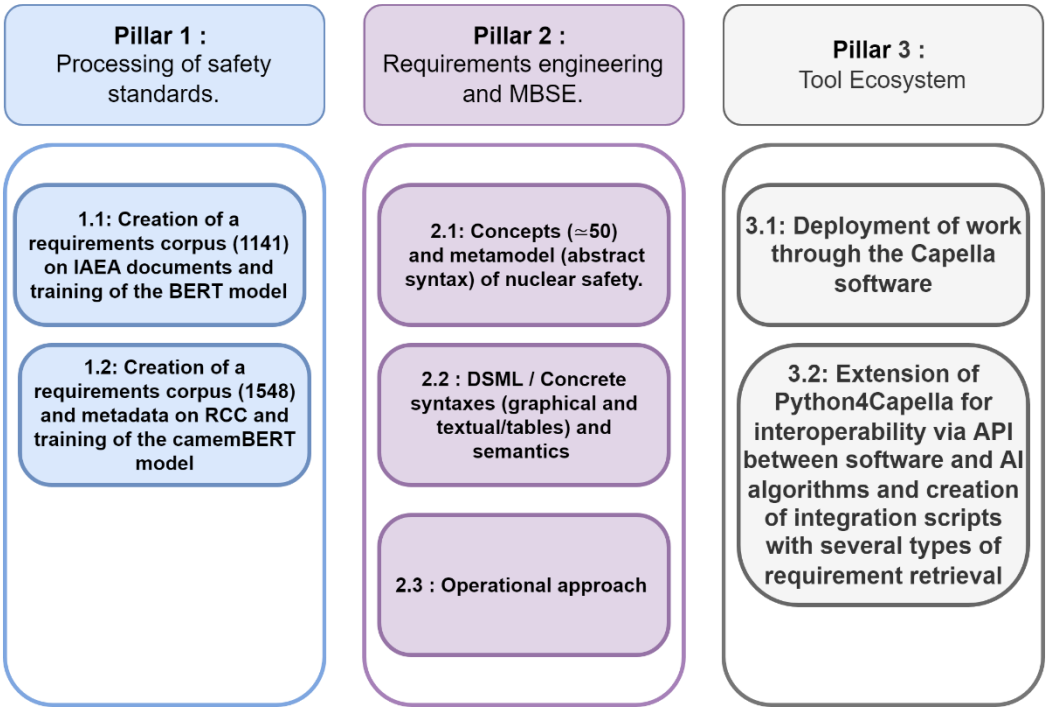


Figure 76 Summary of contributions

6 Application and discussion (use case)

In the remainder of this manuscript, we will apply this methodology to two case studies which will allow us to cover most of the diagrams and tables developed. The diagrams not used in these case studies are those of the General Safety Objectives (OGS) as well as the functional and physical architectures. The input data did not allow the coverage of the OGS (high level diagram). For the functional and logical architectures, our method provides the same functionality as for the physical architecture diagrams. The add-on developed allows the transition of requirements between each of these levels to be managed. This makes it possible to respect the recommended stages of modelling via the ARCADIA method in Capella (cf.Figure 65).

These safety studies are related to two very different systems of installations:

- The Main Steam Relief Train (VDA) system of the EPR under construction.
- A pump system for a cooling circuit of an XSMR (Extra Small Modular Reactor) [108].

6.1.1 VDA System

The VDA system is a discharge valve to the atmosphere (see Figure 78).**Figure 77** [21]) in the secondary circuit of the European pressurised reactor (EPR).

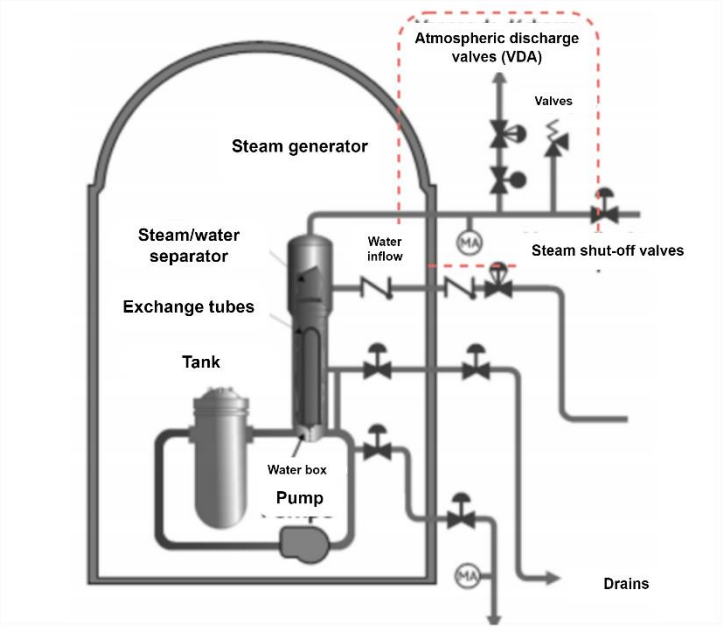


Figure 77 Relief valves and steam line valves (MA refers to radioactive activity measurements of the fluid)

With the primary circuit at 155 bar pressure under normal operating conditions, if a sufficiently large breach occurs in one of the steam generator tubes, the water and pressure transfers will cause the relief valves and safety valves in the affected secondary line to open. There is then no longer a 'barrier' between the primary fluid and the environment. It is this GV tube rupture that we will consider in the scenario analysed in this case study.

6.1.1.1. Steam Generator Tube Rupture Scenario - 1 Tube

This case study deals with a Steam Generating Tube Rupture (SGTR), with 1 tube damaged. The main consequence of this failure is the loss of the second barrier and contamination of the secondary water. This can lead to the release of radioactive products into the atmosphere if the VDA is used. Consequently, it is necessary to act as quickly as possible to limit the release of radioactive materials. For this purpose, the study will be carried out in two phases:

- Short-term phase: stopping the leak
- Long-term phase: reaching the safe state, with possible release of radioactivity due to the use of the VDA train associated with the affected SG

State Controlled Breakdown

Initial State: For this transient the unit is in State A: Reactor on power. There is a breach in a SG tube resulting in a loss of primary coolant. As the pressure in the primary is higher than in the secondary, water from the primary enters the secondary.

Sequence of events: The loss of primary coolant leads to a pressure drop in the primary and contamination of the secondary due to primary water leaking into the secondary. In response, an AAR (Automatic Reactor Shutdown) occurs. This can come from different sources:

- The evacuation of water in the radioactive SG (SG affected by the SGTR) leads to a drop in the level in the primary and in particular in the PZR (Pressurizer) If N PZR < MIN2p + P2 this will trigger an AAR: **RGL-SFG-01G** (nomenclature of the safety functions [27])

- The discharge of primary water into the radioactive SG leads to an increase in the SG level. If N GV > MAX2p, this triggers an AAR: **RGL-SFG-01B**.

- The water from the primary that arrives in the secondary is radioactive. Therefore, the radioactivity sensors in the secondary will indicate to the operators a significant radioactivity **KRT-SFG-01aA**. The operators then manually activate the AAR. **RGL-SFG-01Z**.

What determines which of the three elements triggers the AAR is the initial state of the slice:

- Full power operation: the radioactive SG level will not increase significantly. The AAR will therefore have been triggered on low PZR pressure.

- Zero power operation: in hot shutdown the heat from the primary transferred to the secondary is insufficient to vaporise the flow at the breach. The level of the radioactive GV therefore increases until an AAR is triggered. The radioactive SG is isolated on the water side: ASG (Auxiliary power supply to the SG) isolation: **ASG-SFG-02A** and ARE (Normal power supply to the SG) isolation: **ARE-SFG-06A, ARE-SFG-03H**.

In this study, the AAR will be triggered automatically before manual intervention by the operators.
The VDA will open automatically when N GV > MAX2p **VDA-SFG-02C is** reached.

The continuous loss of coolant causes the PZR to drain. The pressure in the primary circuit drops and the RCV (Chemical and Volumetric Control of the primary circuit) is not sufficient to compensate for the loss of water. An IS (Safety Injection) signal is quickly triggered on the criterion of P PZR < MIN3p, the RCV will no longer be used to compensate.

There is also partial cooling following the triggering of the IS signal initiated by P PZR< MIN3p or N GV > MAX1p in the radioactive GV. This partial cooling allows the temperature and thus the pressure in the SG to decrease by reducing the set pressures of the VDAs **VDA- SFG-02D**.

The IS signal will start the ISMP (Safety Medium Pressure Injection) trains to compensate for the loss of primary refrigerant. However, the ISMP pumps cannot inject water because the primary pressure is initially above their operating range.

The controlled state is reached when the ISMP trains, and possibly the RCV, can compensate for the loss of primary water. However, since the leak has not yet been treated, water from the primary continues to flow into the affected SG through the breach.

State Controlled -> Short-term phase

The SG affected by the SGTR (Steam Generator Tube Rupture) is identified and isolated as a result of the combination of the two signals:

- NGV > MAX2p
- End of partial cooling

The SG affected by the SGTR is identified and automatically or manually isolated. To perform this isolation, the VDA set pressure will be automatically raised above the ISMP injection point but below the opening point of the VVP (Main steam circuit) protection valves , taking care to close the **steam** isolation valves **VVP-SFG-01A / VVP-SFG-01B**. Thus, if the previous openings of the VDA are not considered, no release of radioactivity into the atmosphere takes place **VDA-SFG-03A**.

The RCV charge line will also be automatically isolated at the end of partial cooling when N GV > MAX2p **RCV-SFG-02A** as well as the injection at the GMPP (Primary Motor Pump Unit) seals **RCV-SFG-05A**.

Following the isolation of the affected SG, the flow from the breach increases the pressure in that SG. The pressure in the SG will increase until it becomes equal to that of the primary. The flow rate at the breach then becomes zero: the end of the short-term phase is reached, where the water in the primary no longer drains into the secondary. The isolation of the GV means that no more radioactive material is released into the atmosphere. Indeed, as the GCT (Global Turbine Bypass) was unusable and the VDA was favoured, all the steam leaving the VDA was contaminated.

Short-term phase -> Safe state

Safe state: The safe state is reached when the SG is isolated and at least one RIS-RA train in RA mode (Reactor Off mode, cooling SGs cannot be connected with these physical parameters) is connected to the primary.

To do this, operators need to carry out various actions:

- Boron injection: During cooling, the RBS (Safety Borication Circuit) will inject boron into the **RBS-SFG-01Z** primary. Once the desired boron concentration is reached,
- The operator stops the **RBS RBS-SFG-03Z**.

- Primary cooling: Cooling is carried out from the three remaining operating SGs, which are associated with the ISMP to avoid disturbing the pressure balance between the primary and the affected SG. Once the radioactive SG level drops below MAX2p, the operator opens the VDA on the other SGs **VDA-SFG-02Z** to depressurise to 30 bar. It is possible to feed the SGs with ASG (Auxiliary water supply to the SG). The ASG tanks are large enough to reach RIS-RA conditions in RA (Reactor Shutdown) mode before the tanks are empty. In the event of a ASG train failure, the tank of the failed train can be locally connected to another train by opening the ASG barrel upstream of the **DSC-SFG-05A** pumps or downstream of the **DSC-SFG-06Z** pumps.

- Primary depressurisation: At the end of the previous cooling stage, the primary pressure is higher than the connection pressure of the RIS in RA mode. At this point, if the level of the affected SG is too high, the operator opens the transfer valve to the adjacent SG (SGs work in pairs) **APG-SFG-02Z**. The aim is to avoid the risk of water hammer on the failed SG. This also prevents the overfilling of the faulty SG, as the more it is filled the greater the potential for release to the atmosphere. Consequently, the second GV must be prepared to receive water from the radioactive SG. To do this, it is necessary to:

- Lower the level control value of the second GV slightly above the MIN2p setpoint.
- Stop the ASG **ASG-SFG-02ZS**, close the VIV (Steam Isolation Valve) **VVP-SFG-01Z** and increase the pressure setpoint in the SGs via VDA **VDA-SFG-02Z**.

As soon as pressure and temperature allow, the operator switches the RIS trains to RA mode RIS-SFG-08Z. The safe state is reached (described in Figure 78).

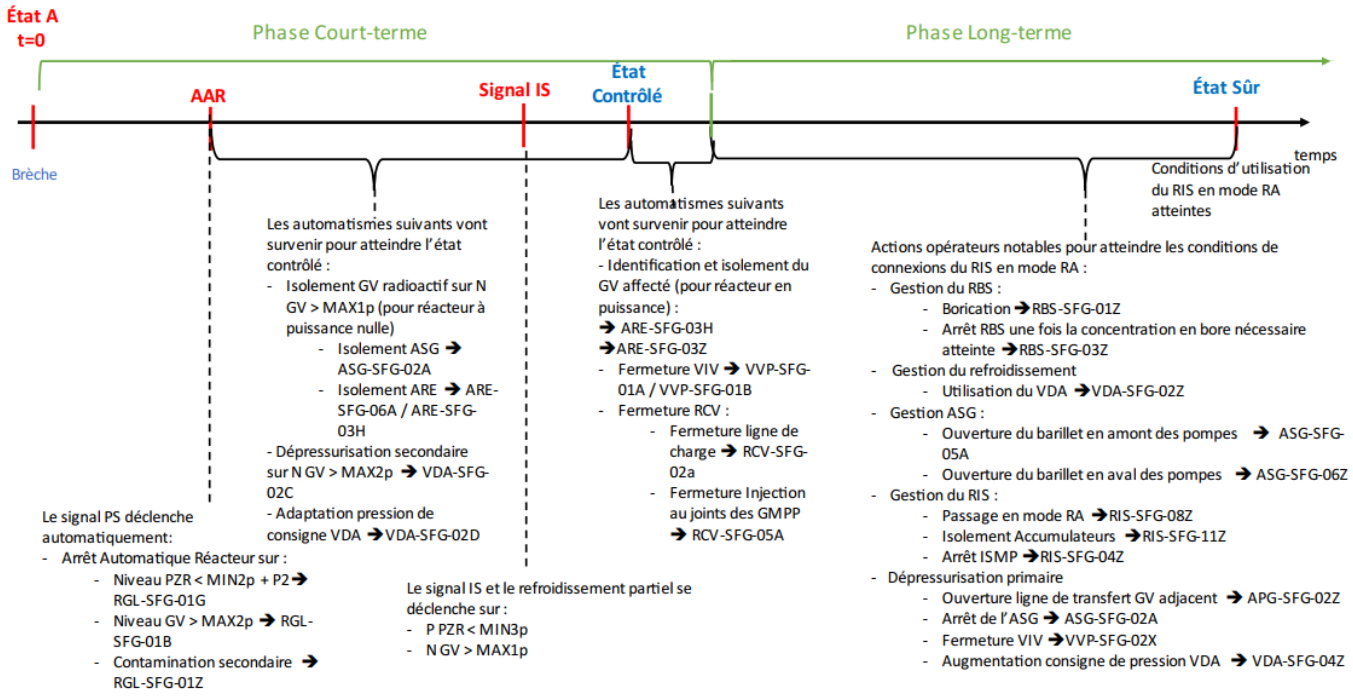


Figure 78 SGTR Timeline - 1 Tube

6.1.1.2. Classification and requirements

The scenario described in the previous section is detailed in terms of functions in the tables in Chapter 15 of the HPC EPR safety report [27]. The functions performed by the components are linked to safety classes (see section 2.2.2.7) which are themselves linked to certain types of requirements. These elements have been used to model the following diagrams (in green and red in the Figure 79).

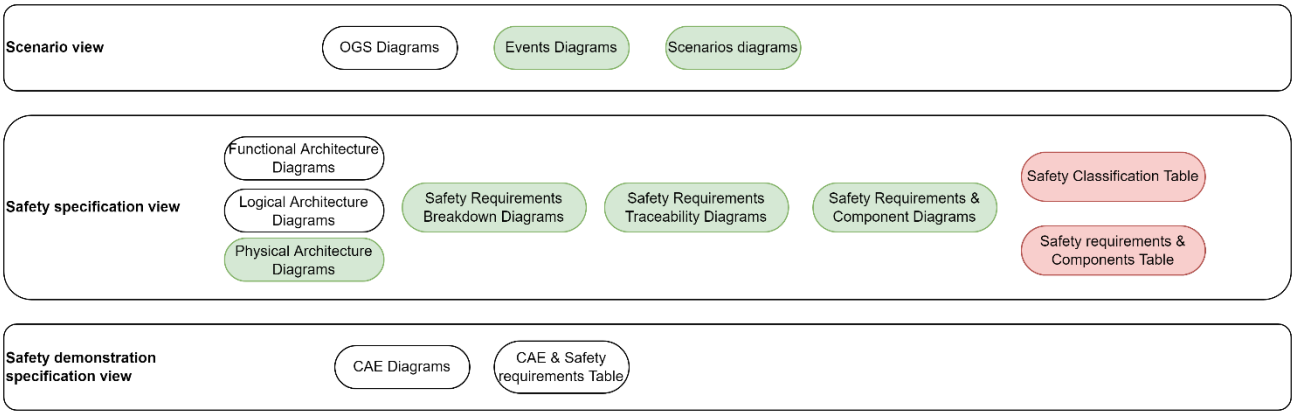


Figure 79 Diagrams and tables of the VDA case study

6.1.1.3. Modelling the case study

Events Diagram/Scenario Diagram

As explained in section 2.2.2.5, initiating events are important in the conduct of the safety demonstration of an installation. Depending on the type of installation, a more or less complete formalisation of these events is carried out. In the case of EDF reactors, this work has been carried out on all levels to establish families of accidents that are conservative in their consequences. The study of the scenarios makes it possible to make design choices according to the roles played by the components with respect to the accident. In the event diagram modelled in this way (cf. Figure 80) are listed the initiating events of type PCC (Operating Conditions) and categorised in probability of occurrence (PCC 2, 3, 4, cf

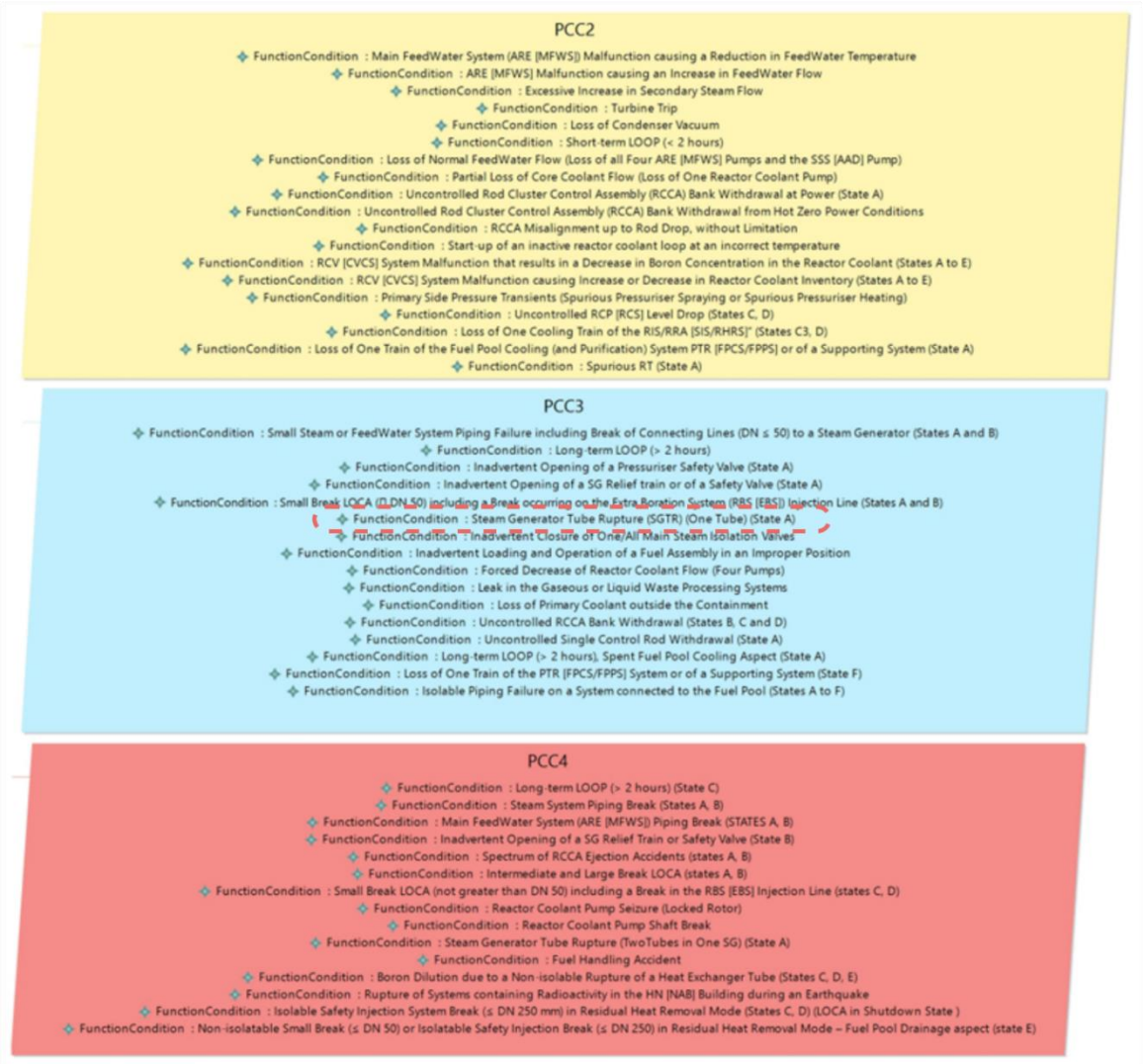


Figure 80 Event diagrams for EPR and PCC events

section 2.2.2.5).

Each of these events is linked to one or more scenarios. In this case study the scenario (cf. Figure 81) described above "Steam Generator Tube Rupture (SGTR) (One tube)

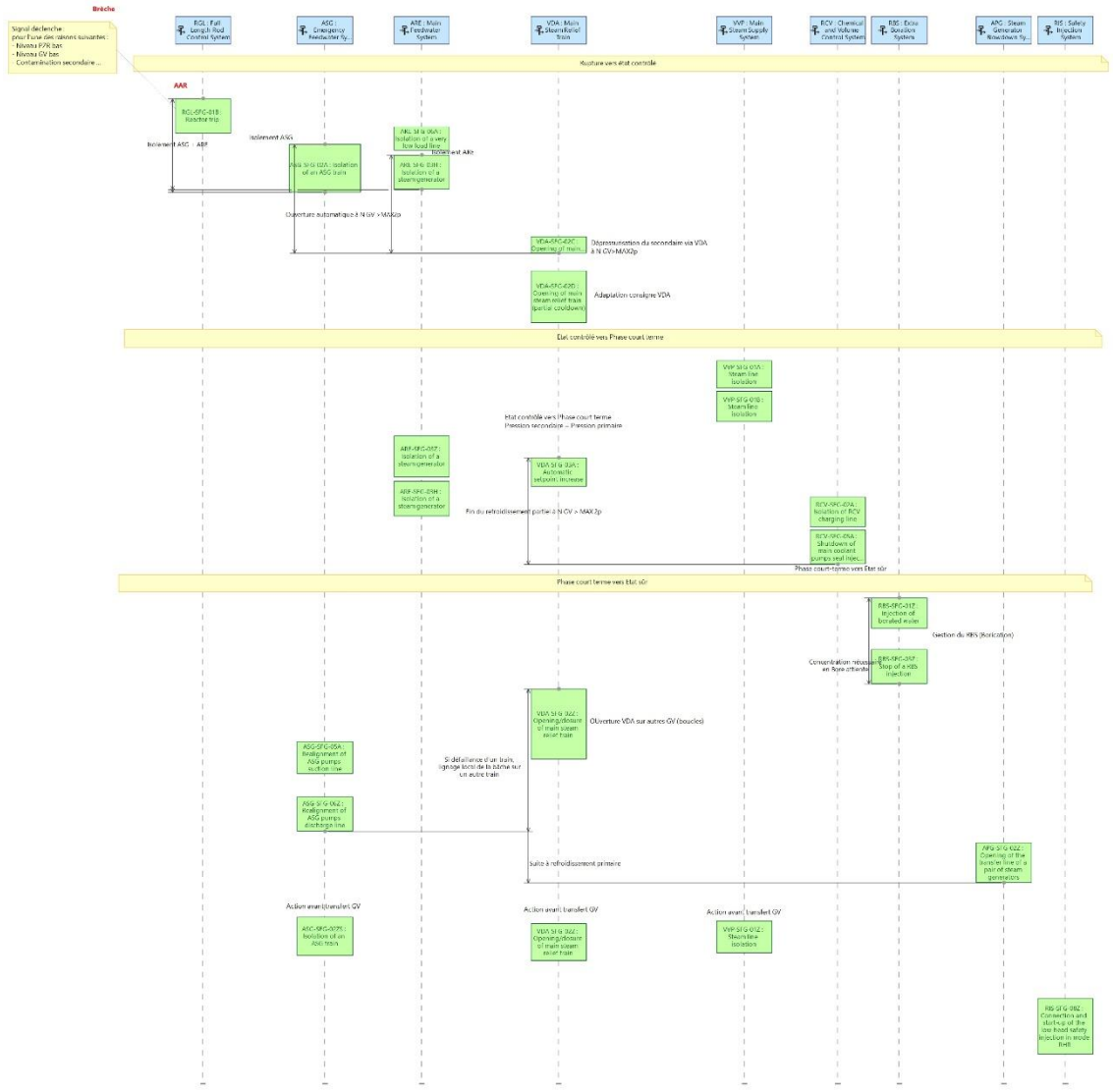


Figure 81 Steam Generator Tube Rupture (SGTR) (One tube) scenario

Physical Architecture Diagram

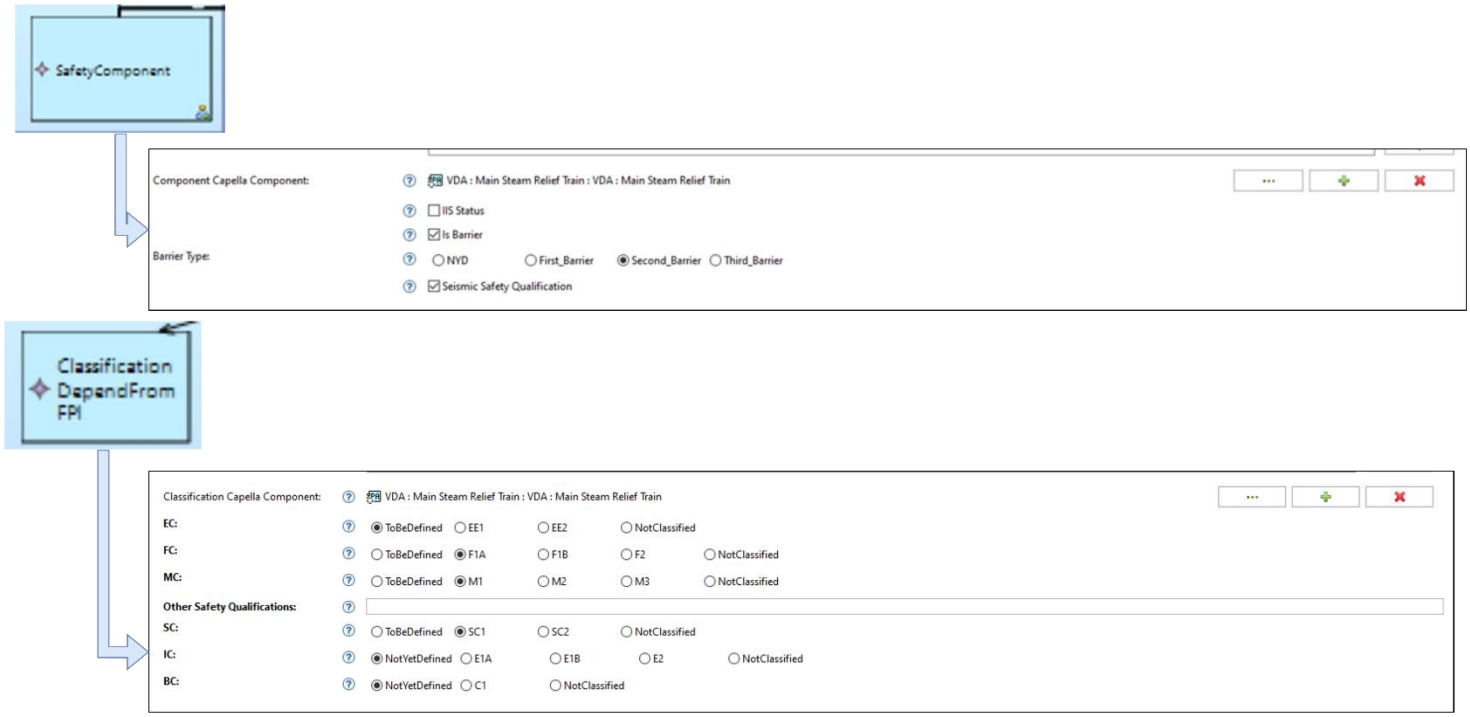


Figure 82 Part of "Safety Component" and "Classification" classes properties

The analysis of these scenarios allows the addition of safety attributes in terms of classes and requirements (according to its typology (FPI, EX, CA, ED)). This addition of attributes is done in the model through the properties of the instantiation of the "Safety Component" class extending the "Component" class of Capella, as well as the instantiation of the "Classification" class (cf.Figure 82).
The latter is added to and linked to the "Component" element. In our case study, the other elements appear with their safety functions involved in the scenario (Figure 81) but are not detailed in terms of classifications and requirements, as the case study is about the VDA system.

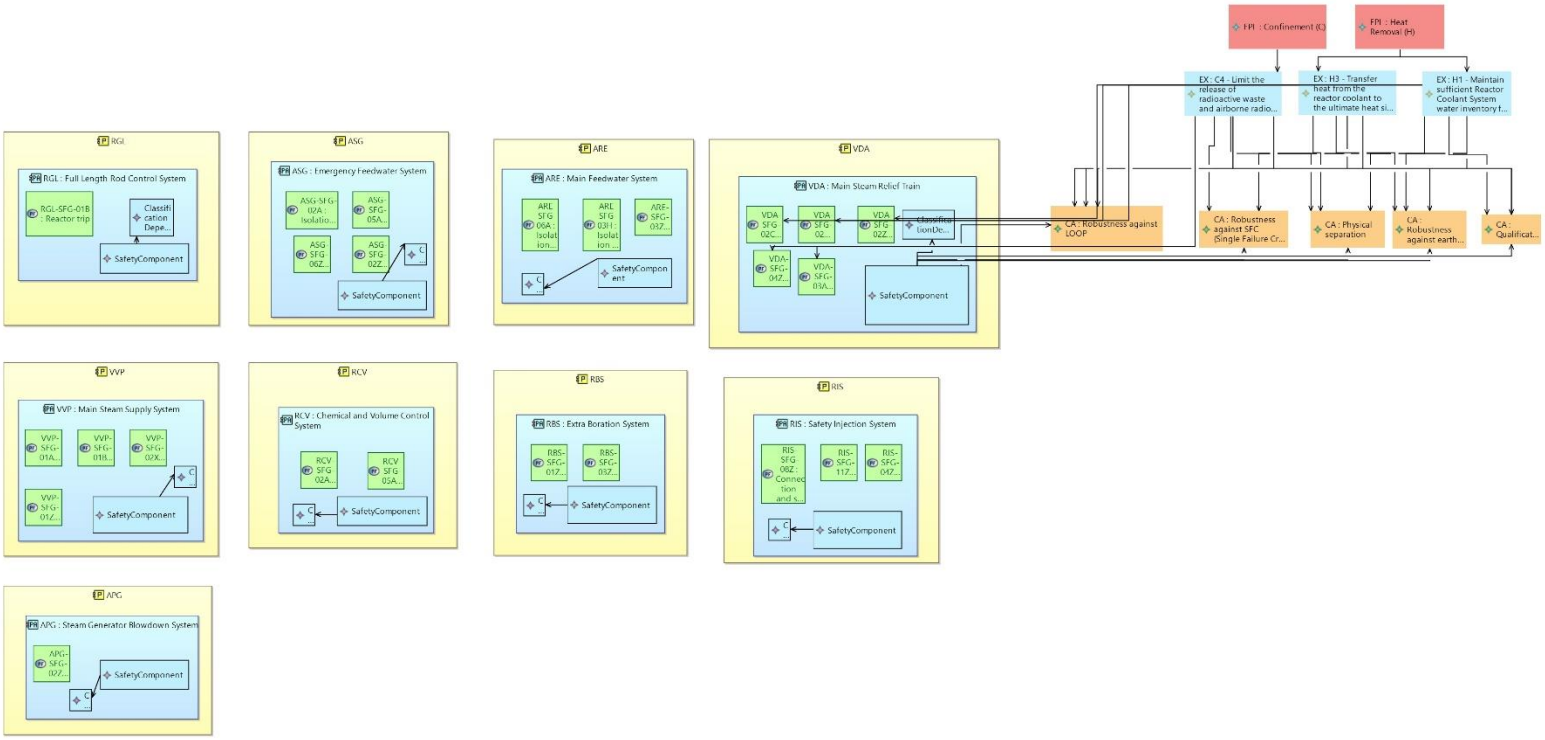


Figure 83 Physical architecture diagram for systems in relation with scenario concerned

Safety Requirements Breakdown Diagram

When requirements increase, it is important to be able to trace them back to their hierarchy as well as their sources. The issue of traceability of requirements has already been mentioned through the concept of the "Golden Thread" in the British nuclear industry. Several diagrams could be used to illustrate this part of the case study since each requirement can be selected to automatically generate its SRBS (Safety Requirements Breakdown Structure). The Figure 84 illustrates the traceability diagram generated from an EX-level requirement, "Maintain sufficient Reactor Coolant System water inventory for core cooling".

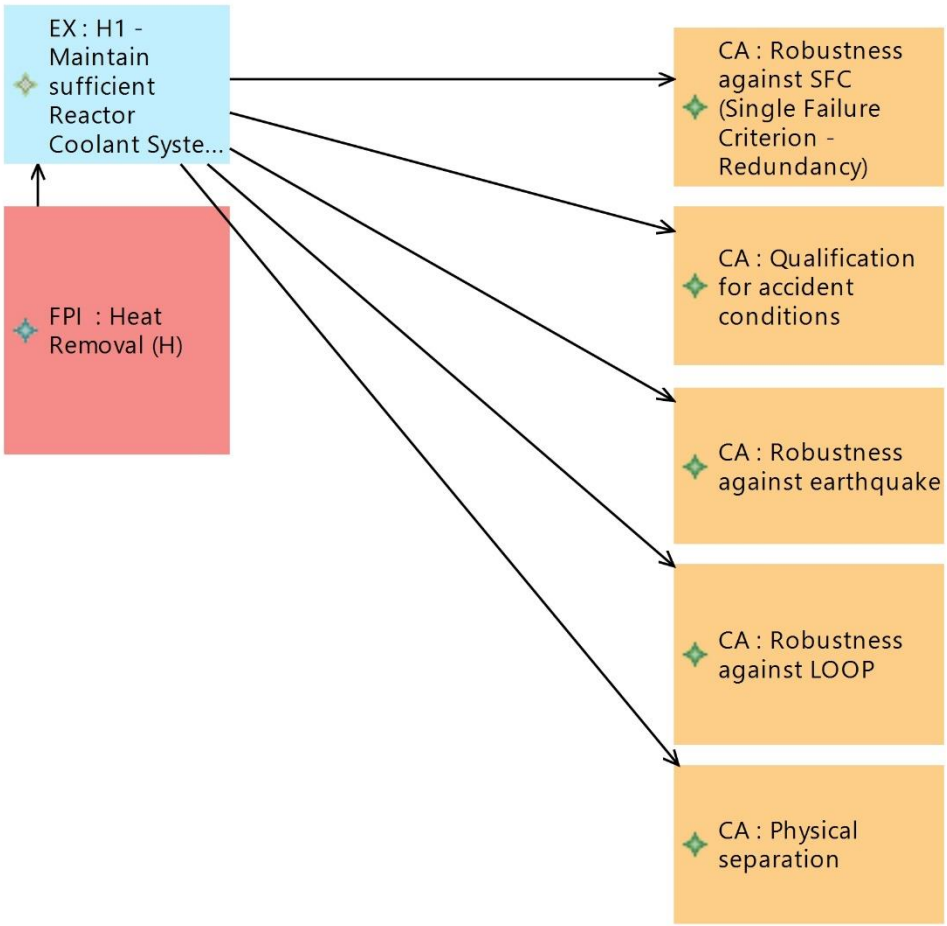


Figure 84 Safety Requirements Breakdown from FPI of Heat Removal Type to the level of CA requirements

Safety Requirements Traceability Diagram

The traceability of requirements is also necessary with respect to their sources. In our metamodel, we consider two types of sources:

- The safety requirement is defined following a scenario analysis, in this case the source will be the scenario in question.
- A risk analysis is carried out by safety engineers and generates requirements. The source is then the relevant analysis of the risk typology considered.

In the same way as the SRBS diagram, the traceability diagram is generated automatically from the attributes of the requirements (cf. Figure 85)

In our case study, the traceability of the requirements related to the circulation of the cooling fluid is linked to the scenario considered in our study through the concept of risk.

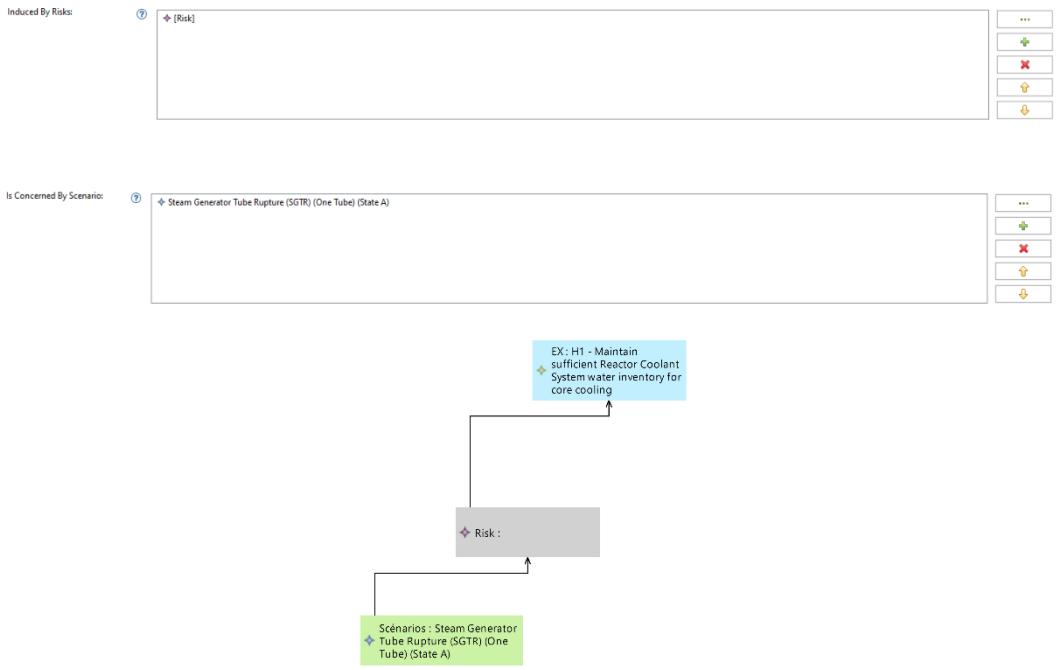


Figure 85 Diagrams and properties related to traceability to the source of safety requirements

Safety Requirements & Component Diagram with classes and requirements tables and extension of component properties

The possibility of isolating components and their safety requirements in specific diagrams is made possible through an automatic creation of the latter. We illustrate this here through a Components-Safety Requirements diagram for the case of the VDA system (cf Figure 86.).

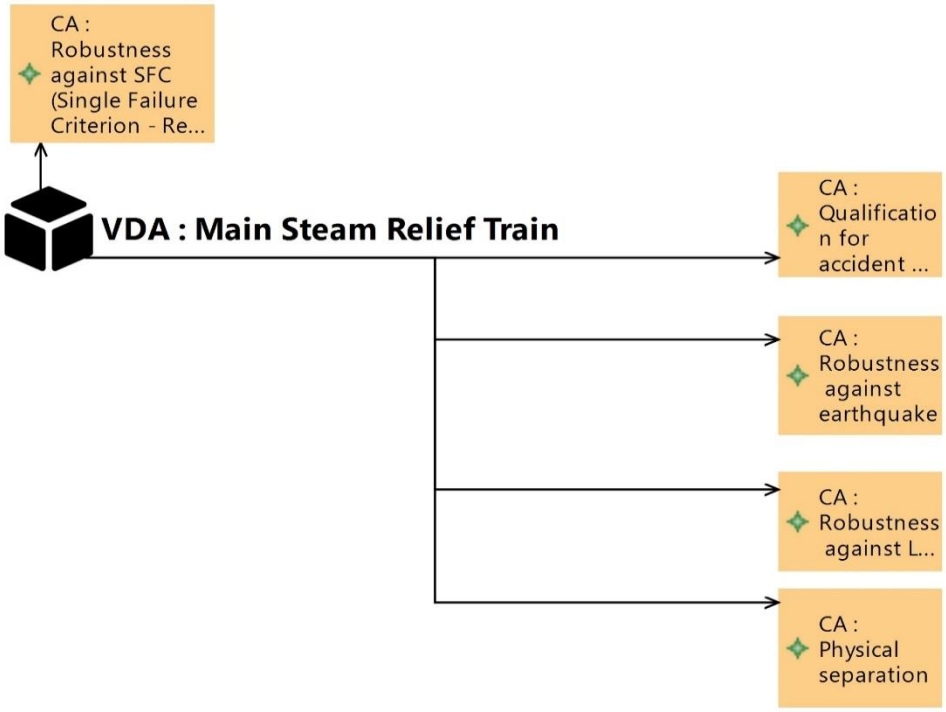


Figure 86 VDA Component-Safety Requirements diagram

It is also possible to generate summary tables from the attributes filled in during modelling (cf. .)which inform about:

- The components and their related requirements with a columnar separation of the safety requirement typologies.
- The components and their safety classes.

These tables can also be used to fill in these same attributes in a way that is more convenient for engineers than the graphical view provided by diagrams.

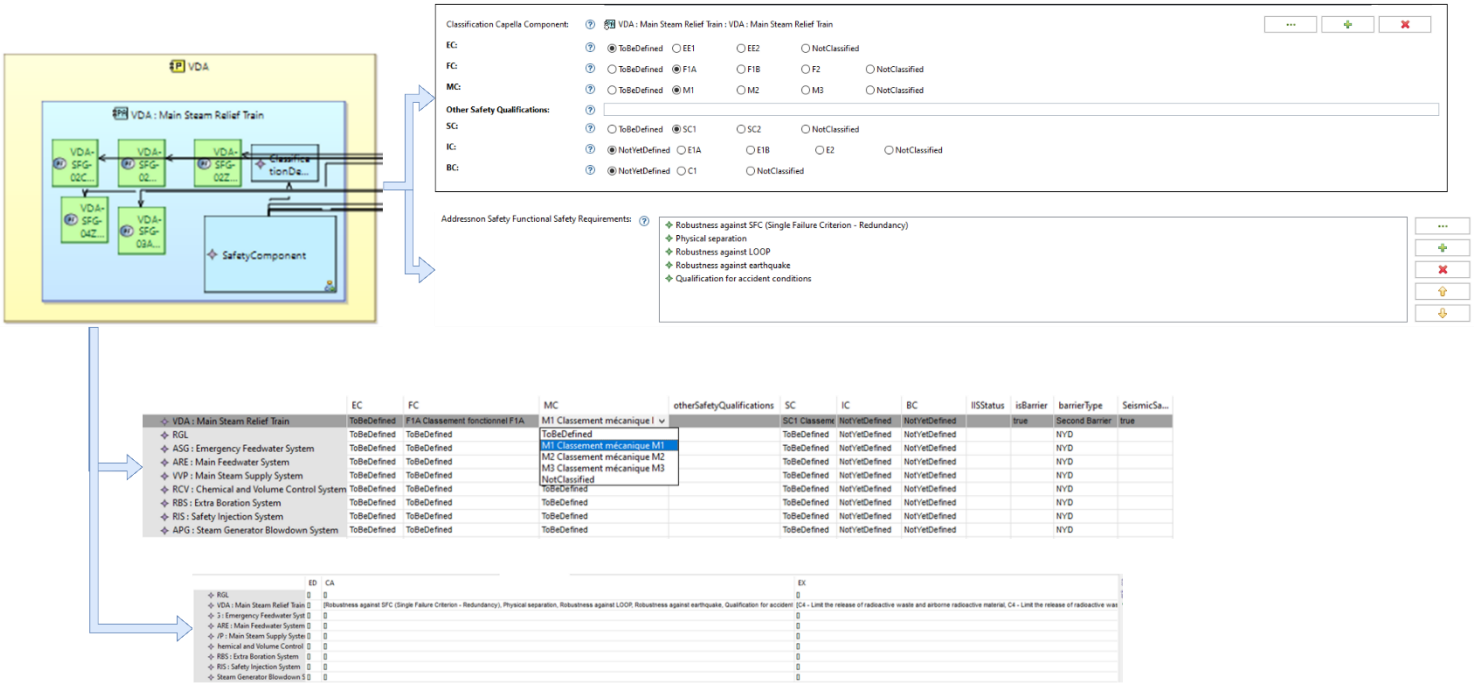


Figure 87 Tables summarising safety classes and requirements

6.1.2 XSMR Pump

6.1.2.1. Introduction to the system

This safety case study focuses on the fuel pump (equivalent to the GMPP of a PWR) of the coolant on an XSMR (Extra Small Modular Reactor) [109].
Safety requirements have been specified for the pump components consisting of:

- Pump packing.
- Pump body.
- Pump shaft.
- Wheel.
- Engine.
- Fixings.
- I&C aspects.
- Overspeed limiter.

These requirements (cf.Table 11) are not exhaustive and are intended to illustrate the elements of the diagrams. The case study on the pump of an XSMR will allow us to put an important element of the method at the heart of this thesis: the link between the design and the safety demonstration which is particularly complicated to follow in projects. The latter requires a good number of iterations and generates a good number of documents, exchanges, and meetings. These models provide a visual dimension that facilitates this work at the centre of an extensive collaboration between the design engineers and those responsible for ensuring the safety demonstration of the installation.

Table 11 Safety requirements of the XSMR fuel pump

Interest protection function	Requirement	Subsystems	Expected characteristics	Requirements defined
Protection of the environment and workers	Do not release gaseous radioelements	Seal + pump body	Sealing of the component	Overall helium leakage rate less than 6.69.10-9 Pa.m3/s
Protection of the environment and workers	Do not release radioelements in the form of particles	Seals + pump body	Sealing of the component	Overall helium leakage rate less than 6.69.10-9 Pa.m3/s
Protection of the environment and workers	Limit the activation of the pump body	Pump body	Use of low activation materials	Contact dose rate < 2 mSv/h after 2 years cooling
Protection of the environment and workers	Limiting worker exposure during maintenance operations	Seals + pump mounting + motor + shaft	Non-replacement of gaskets	Operating life at 250°C of seals > 10 years
Protection of the environment and workers	Do not release radioelements (gaseous/particulate)	Seal + pump body	Maintaining structural integrity under earthquakes	Design for the reference earthquake
Protection of the environment and workers	Do not release radioelements (gaseous/particulate)	Seal + pump body	Maintaining integrity in the event of fire	Pump operating temperature VS fire temperature (see fire curve or simulation)
Protection of the environment and workers	Do not release radioelements (gaseous/particulate)	Seal + pump body	Maintaining integrity in the event of fire	Not more than X MJ of heat load in the room or Sprinkler on fire detection in the pump room
Evacuate residual power	Ensuring the circulation of salt in normal operation	Pump motor + impeller + shaft	Mass flow rate sufficient to cool the core during operation	Mass flow rate > 100 kg/s at 750 °C reactor in operation
Evacuate residual power	Ensuring the circulation of salt at standstill	Impeller + shaft	Mass flow rate sufficient to cool the core at standstill	10 kg/s < Mass flow rate < 50 kg/s at 750 °C reactor in operation
Residual power removal	Ensuring refrigerant circulation	I&C System	Detection of reduced flow	Emergency stop on loss of flow detection
Residual power removal	Ensuring refrigerant circulation	All SS	Functional maintenance of the pump	Design for the reference earthquake
Residual power removal	Ensuring refrigerant circulation	Functional assembly of the pump	Functional pump in case of fire	Pump operating temperature VS fire temperature (see fire curve or simulation)
Residual power removal	Ensuring refrigerant circulation	Functional assembly of the pump	Functional pump in case of fire	Not more than X MJ of heat load in the room or Sprinkler on fire

				detection in the pump room
Controlling responsiveness	Preventing an increase in the reactivity of the heart	Overspeed governor, shaft	Presence of a mechanical overspeed device	Mechanical overspeed detection if mass flow > 150 kg/s at 750°C

These are the elements that have been used to model the following different diagrams (in green and red in the Figure 88).

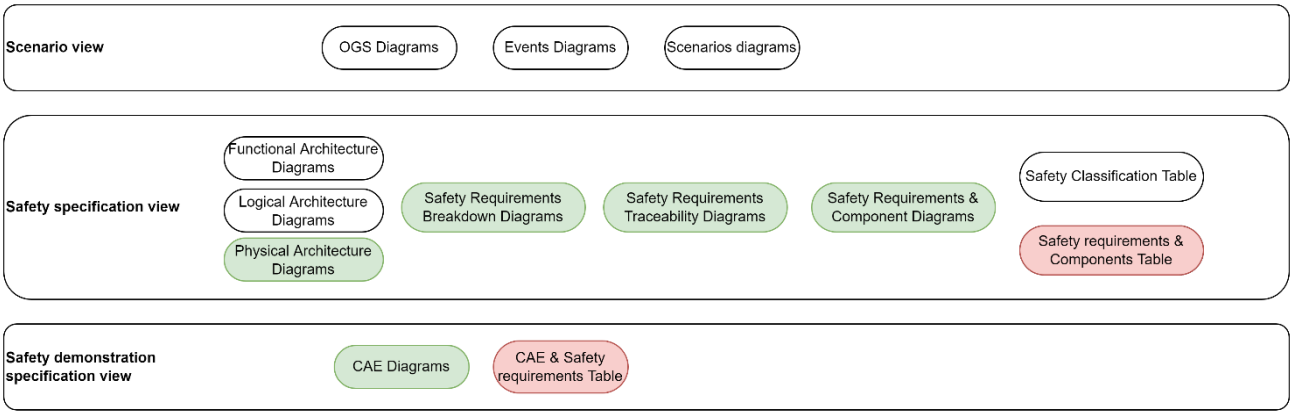


Figure 88 Diagrams and tables of the XSMR fuel pump case study

In the following sections, we will not go into detail about the diagrams already introduced in the first case study (VDA system for EPR).

Physical Architecture Diagram

A simplified representation of the pump (without entering mechanical, I&C etc. details) in the physical architecture diagram allows us to allocate our safety requirements. In term of requirements:

- FPI are in red;
- EX are in blue.
- CA are in orange.
- ED are in yellow.

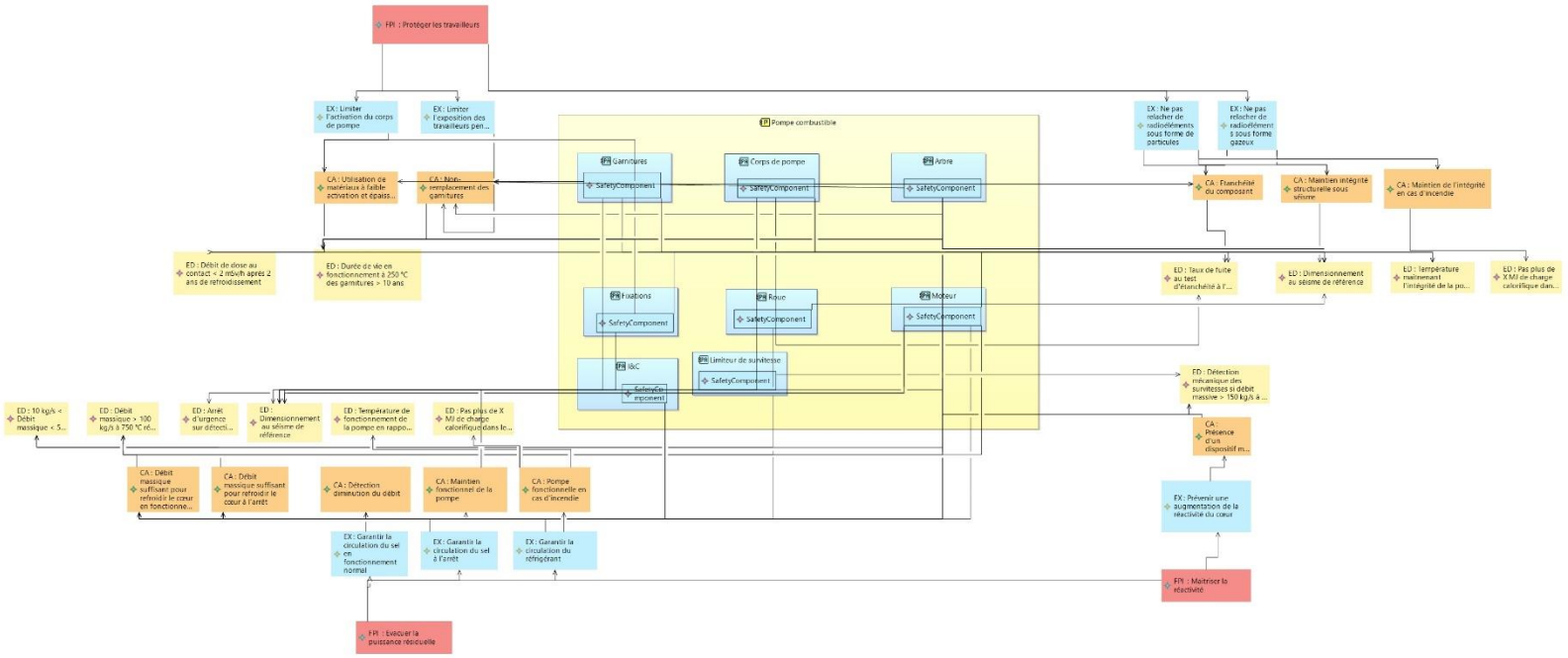


Figure 89 XSMR fuel pump physical architecture diagram with safety requirement allocation

Safety Requirements Breakdown Diagram / Safety Requirements Traceability Diagram

As explained for the case of the VDA system, we can generate the SRBS and traceability diagrams to the sources of the requirements (cf. Figure 90). In the case of the traceability diagram, our requirement sources are scenarios or agressions related to internal risks as well as agressions related to external risks.

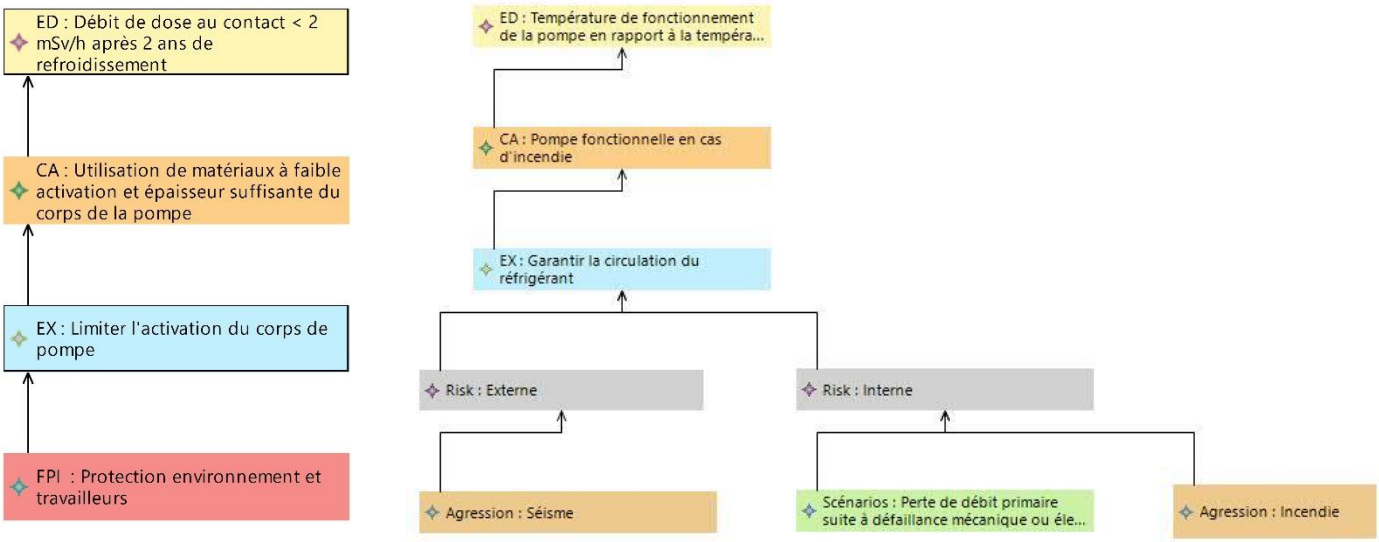


Figure 90 SRBS and traceability diagram to requirements sources

Safety Requirements and Requirements Table

For this case study we have not considered the safety classes, we can however generate the safety requirements allocation tables on the different components of the fuel pump (cf. Figure 91) with the possibility of adding, deleting, and modifying these requirements directly from the table.

Figure 91 Allocation table for safety requirements on components

Safety CAE diagrams + tables

Finally, the safety demonstration specification diagram details the demonstration (introduced in section 5.1.5.15.1.5). In the Figure 92 and Figure 93 the safety demonstration specification diagrams are shown for two FPIs. The top claims are then FPIs. These requirements are transformed into a claim by changing the text into a statement. For the FPI "Evacuate residual power" the Claim is then: "Residual power is evacuated". This claim must now be demonstrated. The decomposition into sub-claims leads to further requirements being demonstrated as the demonstration proceeds.

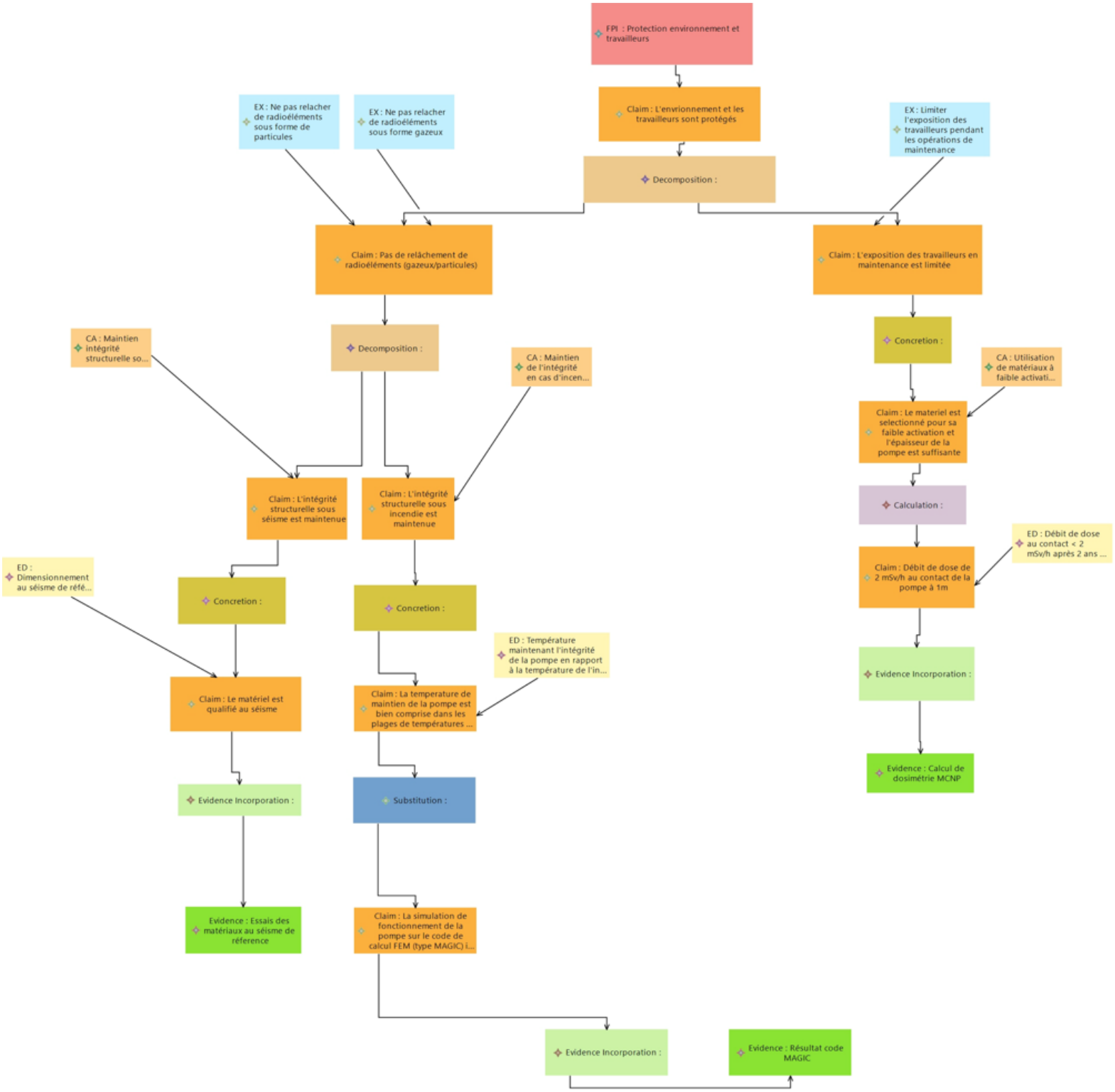


Figure 92 CAE specification for safety demonstration of the FPI for environmental and worker protection

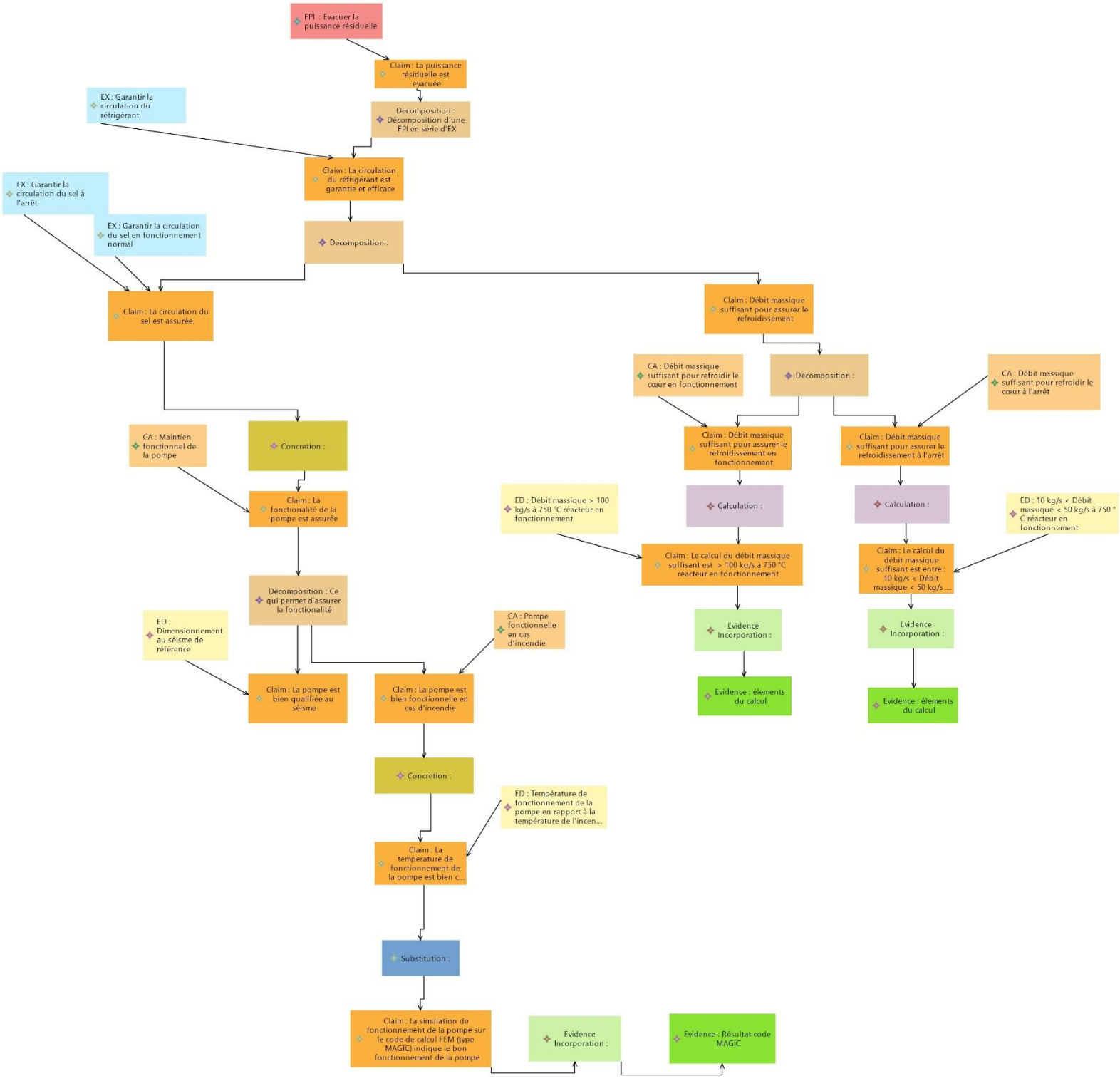


Figure 93 CAE specification for safety demonstration of Residual power removal FPI

In the matrix below (Figure 94), the allocation of the requirements to their respective claims is shown. This makes it possible to check whether all the safety requirements are at least present in a demonstration diagram. If this is not the case, the safety requirements are not demonstrated.

	L'envr...	Pas d...	L'exp...	L'inté...	L'inté...	Le ma...	Le ma...	La temperature de maintien de la pompe est bien comprise dans les
Ne pas relacher de radioéléments sous forme gazeux		X						
Ne pas relacher de radioéléments sous forme de particules		X						
Taux de fuite au test d'étanchéité à l'hélium globale inférieur à 6,69.10-9 Pa.m3/s								
Limiter l'activation du corps de pompe								
Utilisation de matériaux à faible activation et épaisseur suffisante du corps de la pompe						X		
Débit de dose au contact < 2 mSv/h après 2 ans de refroidissement								
Limiter l'exposition des travailleurs pendant les opérations de maintenance			X					
Non-remplacement des garnitures								
Durée de vie en fonctionnement à 250 °C des garnitures > 10 ans								
Garantir la circulation du sel en fonctionnement normal								
Garantir la circulation du sel à l'arrêt								
Débit massique suffisant pour refroidir le cœur en fonctionnement								
Débit massique suffisant pour refroidir le cœur à l'arrêt								
10 kg/s < Débit massique < 50 kg/s à 750 °C réacteur en fonctionnement								
Débit massique > 100 kg/s à 750 °C réacteur en fonctionnement								
Prévenir une augmentation de la réactivité du cœur								
Présence d'un dispositif mécanique contre les survitesses								
Détection mécanique des survitesses si débit massive > 150 kg/s à 750 °C								
Garantir la circulation du réfrigérant								
Détection diminution du débit								
Arrêt d'urgence sur détection de perte de débit								
Maintien intégrité structurelle sous séisme				X				
Dimensionnement au séisme de référence							X	
Maintien fonctionnel de la pompe								
Dimensionnement au séisme de référence								
Pompe fonctionnelle en cas d'incendie								
Température de fonctionnement de la pompe en rapport à la température de l'incendie								
Maintien de l'intégrité en cas d'incendie					X			
Température maintenant l'intégrité de la pompe en rapport à la température de l'incendie								X

Figure 94 Matrix linking safety requirements to demonstration claims

6.2 Discussion and limits

We started by setting the context of our study, introducing the issues of nuclear safety, the general concepts as well as the elements that seem to be an issue in this domain. In a second step, the problematic was formalised through several barriers. We then reviewed the state of the art in the treatment of these problems by experts in the field. Finally, we presented our work through our various contributions as well as an illustration of the latter on two case studies. In this part, we wish to make the link between our contributions and how they contribute to the lifting of these barriers. Also, we would like to come back to the use-cases and the context of the latter. Finally, we will analyse the limits of our study to begin to draw up the elements of research that should follow our work.

6.2.1 Review of the response to the barriers through our contributions

6.2.1.1. Conceptual barriers

Table 12 Conceptual element barriers

Type of barrier	N°	Barrier
Conceptual	1	Lack of agreement on common terminology in relation to the demonstration of nuclear safety
	2	Definition of elements strongly present in safety such as: Requirements, Safety argumentation (CAE framework [34]
	3	How to link the nuclear safety demonstration to the design of the installation?

As mentioned in our summary of the state of the art on the group of conceptual barriers, previous work has provided definitional elements that clarify the subject but very rarely take the form of a detailed metamodel. However, this has been done for the I&C modelling approaches. Through our approach we have tried to consider the field of nuclear safety as a whole. Although there are divergent views on the names of these concepts, this meta-model and its implementation in a tool will allow to refocus the discussion and even to adapt the terms defining such or such concept for a given context. For example, the work of qualifying the typology of safety requirements will be found for each project but sometimes under different terms depending on the operator and his terminology. Therefore, we proposed to link the design of the installation, for which the requirements are one of the fundamental elements, with the safety demonstration, for which the "claims" are the fundamental elements. The matrices for allocating requirements to claims represent the keystone between the design of the installation and its demonstration. Together with the related diagrams (CAE diagram), they provide a common ground for exchange between the engineers in charge of the architecture and the engineers in charge of the safety demonstration to the authorities.

6.2.1.2. Methodological challenges

Table 13 Methodological barriers

Type of barrier	N°	Barrier
Methodological	4	How to facilitate communication between teams?
	5	How to facilitate collaboration between different domains?
	6	How to conduct the safety demonstration?
	7	How to integrate nuclear safety into MBSE models as a viewpoint?
	8	How to have a traceability of safety requirements?
	9	Lack of clear vision in the standards of the methodology to adopt.
	10	Scattered information, fragmented documentation.
	11	How AI can help on nuclear safety demonstration?

As far as methodological issues are concerned, we have been able to provide a method through the development of different languages instantiated into diagrams and matrices which are mapping a certain subset of our metamodel. These diagrams are themselves part of a more general method that maps the processes that the safety engineer must follow to the diagrams to be used. We hope to refine this method with its extensive use in projects involving nuclear safety. This is where some of the interest of the MBSE approach lies, our diagrams allow the integration of the nuclear safety domain through a visual collaboration of their contributions to the project. These diagrams can then be used to extract certain attributes and represent other elements of interest such as the traceability of requirements to their sources or to the requirements from which they derive. The integration of artificial intelligence into this method allows us to put in its place a powerful technology that is too often misjudged in terms of the contributions it can make. The failures of artificial intelligence projects (about one in 10 data science projects will not go into production [110]) are partly due to a poor understanding of the domain issues. Elegant integration of AI into MBSE is about understanding the functions of each of these domains, the type of AI, the purpose. We have tried to identify elements of the nuclear safety demonstration that can benefit from the contribution of AI algorithms. Initially, these algorithms are mainly from the NLP domain but, as mentioned in our state of the art, the safety demonstration can benefit from algorithms processing all types of data (images, videos, graphs, texts, etc.). However, it is necessary to have the right concepts, the right languages, the right methodologies, and the right interoperability.

6.2.1.3. Technical barriers

Table 14 Technical barriers

Type of barrier	N°	Barrier
Technical	12	How can the tools/techniques enable the lifting of these barriers?
	13	What tools can be used to integrate the approach to both the safety demonstration and the design in order to have an integrated approach to safety in the project.
	14	What type of AI is to be considered for nuclear safety tasks?

The conceptual and methodological approach seems satisfactory to be developed further. However, it seemed important to us in the context of an industrial thesis to bring a reflection around the tools and their interoperability. It seems judicious, when bringing concepts and modelling from a new domain (here nuclear safety), to prefer to extend existing approaches rather than start from scratch. In the context of the development of the methods resulting from this thesis, the work cited around MBSA in our state of the art [45] seemed relevant to us. As has been pointed out, it is useful to avoid the multiplication of software, languages, etc. which will not be maintained and for which documentation will be scarce. Open source standards, as part of the work to improve approaches in the field, facilitate collaboration between different stakeholders who wish to make contributions These may be from different institutions (safety authorities, operators, service providers, expert support etc.). Where possible, it may be interesting to open these modelling software packages to programming languages in order to interoperate with approaches from other domains. For the integration of artificial intelligence algorithms in the Capella software, the gateway offered by "Python4Capella" has been very useful. The Python language and its libraries have documentation and a user community to facilitate development work. We have seen at some of the gatherings on the use of artificial intelligence in certain areas (health, agriculture etc.) that specific libraries and metamodels have been developed for a while now.

6.2.1.4. Organisational and human barriers

Table 15 Organisational and human barriers

Type of barrier	N°	Barrier
Human and Organisational	15	Document-oriented work
	16	Volume of data considered.
	17	Lack of staff with multi-disciplinary experience and a global vision

	18	Financial: lack of money to make the budgetary drift of projects acceptable.
	19	Psychological: difficulty of cognition of complexity in a "document-oriented" project context.
	20	Usage: reductionism in engineering which prevents the adoption of the understanding postures of other disciplines and which is not facilitated by the document-oriented approach.
	21	Ethics: nuclear demonstration often leads to mistrust by default because of past accident records, leading to increased rigour in this field.

In the context of organisational and human barriers, our work offers a possibility for a solution. Indeed, the use of MBSE approaches and the mix of data-centred and model-based approaches can allow to move away from document-oriented project management. Their use provides answers to the question of how to deal with large volumes of data, the difficulty of cognition of complexity and the budgetary overruns that these difficulties can bring. However, it is necessary for industrialists to take up these approaches and transform these potentialities into reality. Implementation will in turn bring other issues that need to be addressed for the nuclear industry to mature on model/data centric approaches.

6.2.2 Review of the use cases

For the first case, the atmospheric discharge valve (VDA) of the secondary circuit, the elements on which we have relied are data from the public safety report of the English EPR. The architecture, the choice of events and the scenarios are already well advanced, and modelling is therefore an important support to the studies carried out by the engineers. However, for this type of case, specific case developments for this type of study can be important to adapt our approach and make it optimal for this type of project. Also, it was quite difficult to link the safety demonstration elements with the design elements. The Preliminary Safety Report alone is about 8500 pages long and does not constitute all the elements of the safety demonstration. Indeed, this document summarises the general elements of the installation but refers to many other various documents (studies, plans, etc.). This led us to put forward scenario analysis and safety specification diagrams for this case study and leave the safety demonstration specification diagrams. (cf. 6.1.1 and Figure 95).

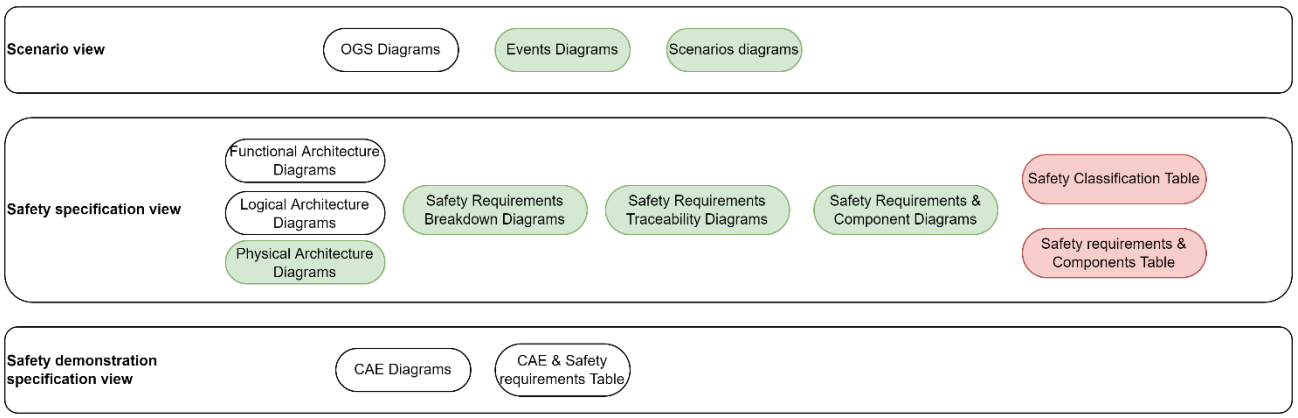


Figure 95 Diagrams/Tables for VDA case

In the case of the XSMR pumps, the innovative nature of this new type of reactor and the search for a solution made it much easier to compare it with the MBSE processes. Indeed, we have in general the safety aspects to ensure. The research and analysis approach and the collaborative aspects take on their full meaning in a search for the optimal solution. The link with the safety demonstration was also easier, the installation being less formalised than for the EPR (cf. 6.1.16.1.2 and Figure 96).

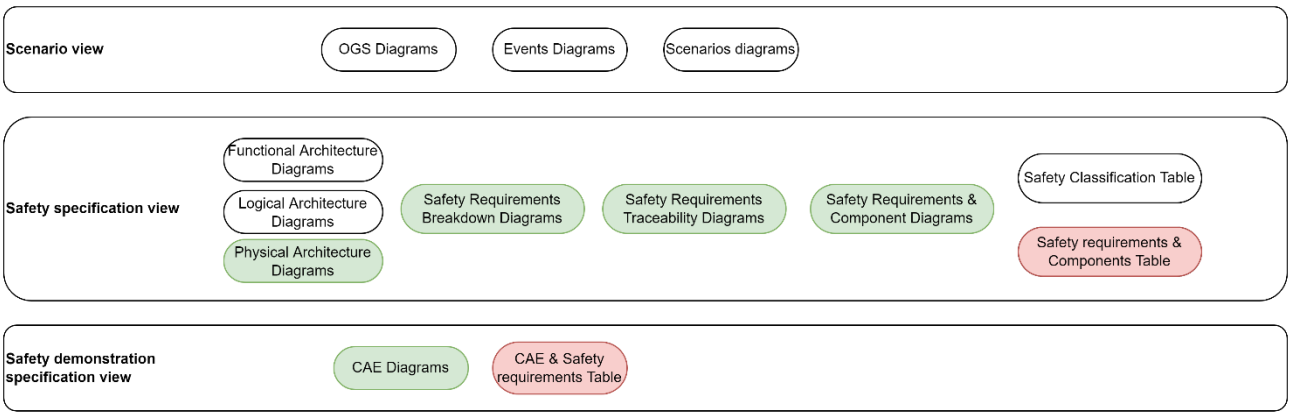


Figure 96 Diagrams/Tables for XSMR case

6.2.3 Limits

Beyond the scope considered in our hypotheses for our study (deterministic studies in the context of the installation design basis), our work is intended to be a first step in a series of applied research studies. Indeed, among the elements mentioned above, the following were mentioned

- The semantic variability of concepts.
- The completeness of the latter.
- Differences in methodology between projects depending on the type of installation, the country, the methods developed by the operator etc.

We find in the heart of the method the adaptability to these differences, but it would be pretentious to think that a context-specific variation of the work wouldn't necessary. These points are important to understand the logic to adopt for the integration of this thesis work into the existing methods. A real change management and an adaptation of the method in return are necessary to convince of the interest of the approach. Some diagrams may be less used than others depending on the operator and the project. Some diagrams may need to be modified. Mastery of the development tools is essential, and the flexibility offered by Capella and its development environment (Capella studio) is a real advantage in these aspects.

The case studies also have their limitations. They were mainly intended to demonstrate the feasibility of the method. They should be followed by application cases aimed at providing real safety studies, thus requiring operating data in project contexts. The follow-up of usage during the project can improve and refine the method through several iterations between the nuclear safety domain, the project teams and the method development teams. It may also help to confirm or refute some of the assumptions of this work. It is important to understand that the methodological proposal to consistently integrate nuclear safety into MBSE practices is a multi-dimensional process. It involves many stakeholders, and nuclear safety is composed of several sub-fields of expertise. It is important to be aware of this point and to consider this work as the basis for future development in

coherence with all these disciplines and the specific fields of MBSE and AI. In the conclusion of this manuscript, we will discuss the perspectives of future work which we consider interesting for the validation and improvement of existing work.

7 General Conclusion

In the context of this work, we have developed a method to integrate the nuclear safety domain into an MBSE approach and AI-related contributions. This method describes the concepts of nuclear safety, their attributes, and the links between these concepts through a metamodel. Languages are used to manipulate these concepts. Concrete syntaxes have been developed to model diagrams and tables of interest in the framework of 3 important views for the nuclear safety engineer:

- The scenario view.
- The safety specification view.
- The safety demonstration. specification view.

Also, this method includes processes in the form of BPMNs which formalises the operational approach. It also indicates the concrete syntaxes to be used according to the progress in the operating procedure. The method and AI contributions has been developed in an add-on for a software already used in the engineering projects concerned. Interoperability has been implemented with APIs of AI algorithms for extraction and various methods of searching for applicable requirements. Consideration was given to the possible use of the REK (Repository of Expertise and Knowledge).

In the following figures (Figure 97, **Erreur ! Source du renvoi introuvable.**, **Erreur ! Source du renvoi introuvable.**), the general expectation of the barriers has been shared between our three pillars and their objectives which cover the purpose of this thesis fairly well. We show our contributions as well as their

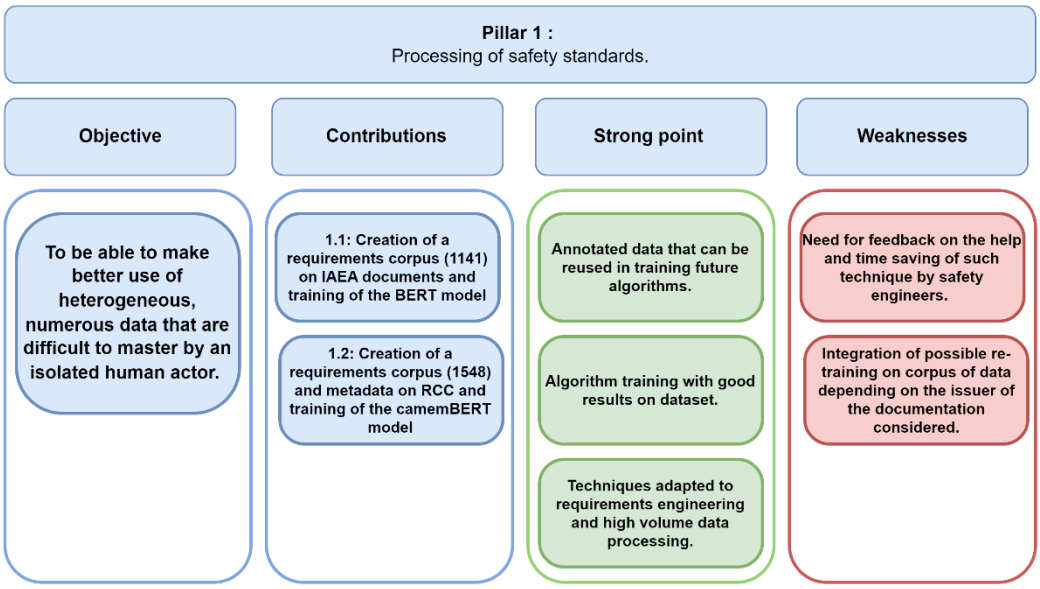


Figure 97 Pilar 1 contribution, strong point, and weaknesses

strengths and weaknesses.

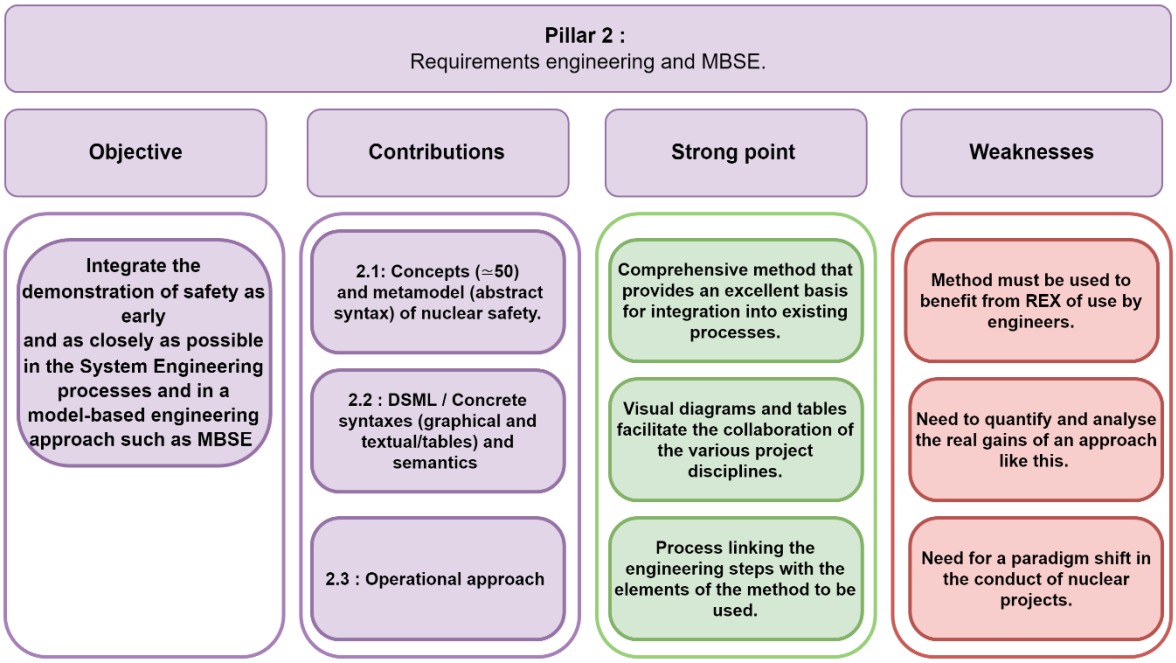


Figure 98 Pilar 2 contribution, strong point, and weaknesses

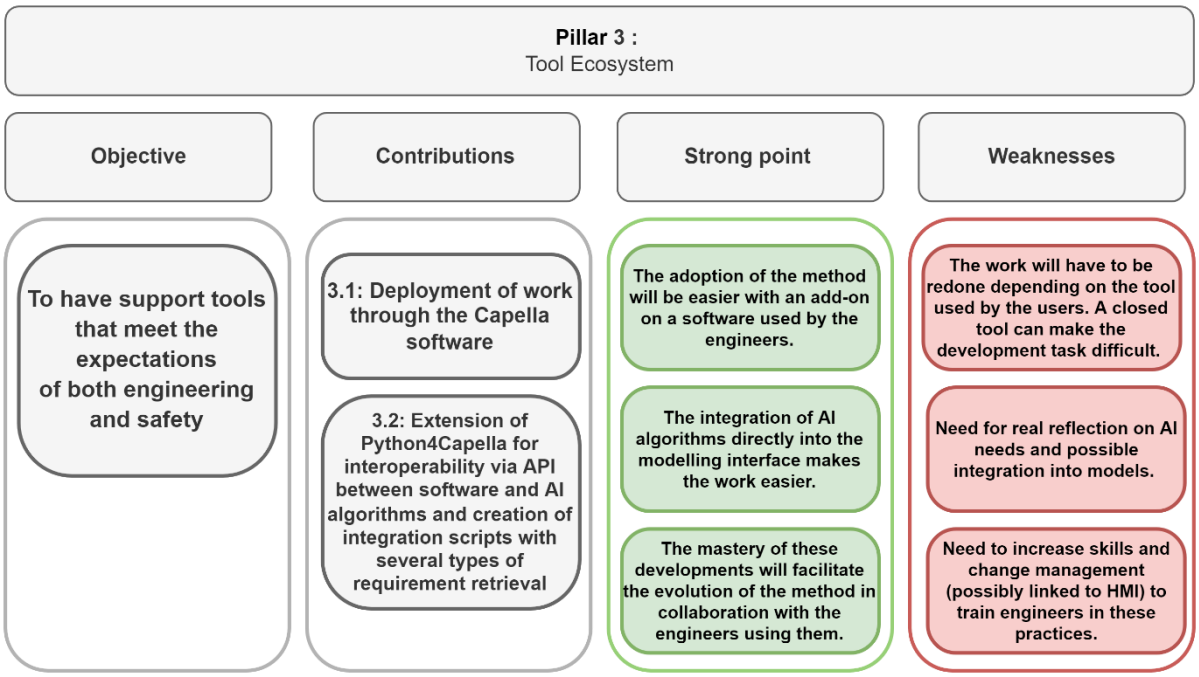


Figure 99 Pilar 3 contribution, strong point, and weaknesses

This work opens the way to other areas of reflection on the subjects covered. The continuity of this work is quite broad, and the following subjects seem relevant and worth exploring:

- Interoperability of organisations, processes, domain specific actors and support tools to further facilitate the preparation (engineering of the safety demonstration) and then the execution of the safety demonstration;
- How to integrate the close link between safety demonstration and installation commissioning, which take place in parallel from the start of engineering and should coexist more closely?;
- Integration of the safety demonstration in the SE processes which do talk about safety requirements but remain rather simplistic or at least too generic to really take this demonstration into account. A possible influence on standard could be imagined;
    - Consider early V&V (Verification and Validation) aspects to check and validate the quality of the proposed demonstrations (by simulation, by formal model analysis, and demonstration simulation). This could be done by proposing an approach of simulation of compliance with requirements? It is then important to consider the work on MBSA [45] to identify the type of safety analysis performed and whether they are directly demonstrable from the models;
- Deployment of such a global method of preparation and follow-up of a safety demonstration in a company or even in an extended enterprise. Indeed, all these activities cannot, and should not, be carried out by a single company for several reasons.

Among the shorter-term elements related to the method, further reflection on the integration of the ISO 15026 [50] standard in the diagrams related to the safety demonstration could facilitate the modelling of this demonstration. In addition, a more complex approach to the scenarios by adapting them to the specific cases encountered in incidental/accidental conduct in the nuclear industry could provide significant added value for the understanding of the role of the components in these scenarios. This could provide a link to probabilistic safety studies which were not the focus of this thesis.

Finally, we hope that our work has contributed to the reflections on the possible and enlightened hybridization of artificial intelligence with MBSE approaches in an Industry 4.0 logic. These approaches have their own domain and scope of application. It seems important to reflect on the contributions that each approach can make rather than having them in competition, as is sometimes seen. Wise approaches in AI aim to link the symbolic approach with the connectionist approach (cf. [66]) It seems to us that models from MBSE constitute in some way this symbolic approach. The metamodel and the resulting models have an organisation that can be used in symbiosis with connectionist AI (learning algorithms). They can also be used in engineering processes and thus benefit from a domain ontology refined by its use by engineers. This vast field is fascinating, and the entire nuclear industry could benefit from the results of such research.

8 Bibliography

[1] « Rapport 2022 du Giec : une nouvelle alerte face au réchauffement climatique », *vie-publique.fr*. https://www.vie-publique.fr/en-bref/284117-rapport-2022-du-giec-nouvelle-alerte-face-au-rechauffement-du-climat (consulté le 4 août 2022).

[2] « Le nucléaire en chiffres | EDF FR », 29 janvier 2021. https://www.edf.fr/groupe-edf/espaces-dedies/l-energie-de-a-a-z/tout-sur-l-energie/produire-de-l-electricite/le-nucleaire-en-chiffres (consulté le 3 octobre 2022).

[3] « Emmanuel Macron va lancer un programme nucléaire d'ampleur », *Les Echos*, 8 février 2022. https://www.lesechos.fr/industrie-services/energie-environnement/emmanuel-macron-va-lancer-un-programme-nucleaire-dampleur-1385397 (consulté le 3 août 2022).

[4] N. Mayer, « Le combustible nucléaire », *Futura*. https://www.futura-sciences.com/sciences/dossiers/physique-energie-nucleaire-a-z-126/page/6/ (consulté le 3 octobre 2022).

[5] « Les émissions carbone du nucléaire français : 4g de CO2 le kWh », *Sfen*. https://www.sfen.org/rgn/les-emissions-carbone-du-nucleaire-francais-37g-de-co2-le-kwh/ (consulté le 3 octobre 2022).

[6] « IAEA increases projection of nuclear power growth : Regulation & Safety - World Nuclear News ». https://www.world-nuclear-news.org/Articles/IAEA-increases-projection-of-nuclear-power-growth (consulté le 3 octobre 2022).

[7] A. de sûreté nucléaire, « Sûreté nucléaire ASN ». https://www.asn.fr/lexique/S/Surete-nucleaire (consulté le 3 mai 2022).

[8] International Atomic Energy Agency, « Managing the First Nuclear Power Plant Project IAEA-TECDOC-1555 ». IAEA, 28 février 2019. Consulté le: 3 mai 2022. [En ligne]. Disponible sur: https://www.iaea.org/publications/7746/managing-the-first-nuclear-power-plant-project

[9] IAEA, « IAEA Safety Glossary », IAEA, Text, févr. 2019. Consulté le: 16 juin 2021. [En ligne]. Disponible sur: https://www.iaea.org/publications/7648/iaea-safety-glossary

[10] *Arrêté du 7 février 2012 fixant les règles générales relatives aux installations nucléaires de base*.

[11] A. de sûreté nucléaire, « Article ASN Arrêté 2012 ». https://www.asn.fr/l-asn-reglemente/cadre-legislatif/arretes/arrete-du-7-fevrier-2012-fixant-les-regles-generales-relatives-aux-inb (consulté le 4 mai 2022).

[12] « Les Français et le nucléaire : adhésion et traits d'image », *IFOP*. https://www.ifop.com/publication/les-francais-et-le-nucleaire-adhesion-et-traits-dimage/ (consulté le 26 septembre 2022).

[13] Internationale Atomenergie-Organisation, *Fundamental safety principles: safety fundamentals*. Vienna: Internat. Atomic Energy Agency, 2006.

[14] A. de sûreté nucléaire, « Rapport de sûreté Lexique ASN ». https://www.asn.fr/lexique/R/Rapport-de-surete (consulté le 16 mai 2022).

[15] A. de sûreté nucléaire, « Règle fondamentale de sûreté ». https://www.asn.fr/l-asn-informe/actualites/regle-fondamentale-de-surete (consulté le 10 juin 2022).

[16] « IRSN_fiche_principes_radioprotection.pdf ».

[17] G. K. Gillmore, R. Crockett, T. Denman, A. Flowers, et R. Harris, « Radium dial watches, a potentially hazardous legacy? », *Environment International*, vol. 45, p. 91-98, sept. 2012, doi: 10.1016/j.envint.2012.03.013.

[18] « NF ISO 19443 », *Afnor EDITIONS*. https://www.boutique.afnor.org/fr-fr/norme/nf-iso-19443/systemes-de-management-de-la-qualite-exigences-specifiques-pour-lapplicatio/fa184390/82160 (consulté le 12 septembre 2022).

[19] *Directive 2014/87/Euratom du Conseil du 8 juillet 2014 modifiant la directive 2009/71/Euratom établissant un cadre communautaire pour la sûreté nucléaire des installations nucléaires*, vol. 219. 2014. Consulté le: 14 juin 2022. [En ligne]. Disponible sur: http://data.europa.eu/eli/dir/2014/87/oj/fra

[20] A. de sûreté nucléaire, « Barrières ». https://www.asn.fr/lexique/b/Barrieres (consulté le 14 juin 2022).

[21] J. Couturier, *Eléments de sûreté nucléaire: les réacteurs à eau sous pression*. 2020.

[22] L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, et W. Kröger, Éd., *Safety and Reliability of Complex Engineered Systems: ESREL 2015*. CRC Press, 2015. doi: 10.1201/b19094.
[23] « La défense en profondeur en sûreté nucléaire », IAEA, Text, 1997. Consulté le: 15 juin 2022. [En ligne]. Disponible sur: https://www.iaea.org/fr/publications/4714/la-defense-en-profondeur-en-surete-nucleaire
[24] ASN, « Guide de l'ASN n°22 », 2017. Consulté le: 15 juin 2022. [En ligne]. Disponible sur: https://www.asn.fr/l-asn-reglemente/guides-de-l-asn/guide-de-l-asn-n-22-conception-des-reacteurs-a-eau-sous-pression
[25] ASN, Éd., « RFS-I.3.a. » 5 août 1980.
[26] « TVO - Safety features ». https://www.tvo.fi/en/index/production/plantunits/ol1andol2/safetyfeatures.html (consulté le 11 juillet 2022).
[27] EDF Energy, « Public Version of HPC PCSR3.pdf ».
[28] « AREVA/EDF - UK EPR - Generic Design Assessment - AREVA EDF - UK EPR™ GDA Submission ». http://www.epr-reactor.co.uk/scripts/ssmod/publigen/content/templates/show.asp?P=290&L=EN (consulté le 17 juillet 2022).
[29] A. de sûreté nucléaire, « Règles générales d'exploitation ». https://www.asn.fr/lexique/R/Regles-generales-d-exploitation (consulté le 20 juin 2022).
[30] Project Management Institute, Éd., *A guide to the project management body of knowledge (PMBOK guide)*, Fifth edition. Newtown Square, Pennsylvania: Project Management Institute, Inc, 2013.
[31] E. Roumili, J.-F. Bossu, V. Chapurlat, R. Plana, et J. Tixier, « Collaborative safety requirements engineering: an approach for modelling and assessment of nuclear safety requirements in MBSE context », p. 10.
[32] « EPR de Flamanville : dix ans de retard et un coût hors normes », *Les Echos*, 29 juillet 2019. https://www.lesechos.fr/industrie-services/energie-environnement/epr-de-flamanville-dix-ans-de-retard-et-un-cout-hors-de-controle-1041255 (consulté le 23 juin 2022).
[33] J. Valkonen, T. Tommila, J. Linnosmaa, P. Karpati, et V. Katta, « Demonstrating and argumenting safety of I&C systems: 10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, NPIC & HMIT 2017 », *Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2017)*, p. 568-580, 2017.
[34] IAEA, *Dependability assessment of software for safety instrumentation and control systems at nuclear power plants.* 2018.
[35] « Golden thread: factsheet », *GOV.UK*. https://www.gov.uk/government/publications/building-safety-bill-factsheets/golden-thread-factsheet (consulté le 23 juin 2022).
[36] J. Linnosmaa, « Structured safety case tools for nuclear facility automation », p. 74, avr. 2016.
[37] T. Tommila et J. Alanen, « Conceptual model for safety requirements specification and management in nuclear power plants », p. 150, 2015.
[38] J. Valkonen, T. Tommila, J. Linnosmaa, et T. Varkoi, « Safety demonstration of nuclear I&C-an introduction: SAUNA Task 3.1 report », 2016.
[39] ISO, « ISO/IEC 15288 Systems and software engineering — System life cycle processes », 2015. Consulté le: 16 juin 2021. [En ligne]. Disponible sur: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/35/43564.html
[40] J. Valkonen, T. Tommila, J. Alanen, J. Linnosmaa, et T. Varkoi, « Views on safety demonstration and systems engineering for digital I&C », mai 2016.
[41] J. Alanen, J. Linnosmaa, et T. Tommila, « Conformity assessment data model », *VTT research report VTT-R-06743-17*, p. 34, 2017.
[42] J. Linnosmaa, A. Pakonen, N. Papakonstantinou, et P. Karpati, « Applicability of AADL in modelling the overall I&C architecture of a nuclear power plant », in *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, Singapore, oct. 2020, p. 4337-4344. doi: 10.1109/IECON43393.2020.9254226.
[43] J. Linnosmaa, J. Alanen, H. Atte, I. Essi, et H. Jaroslav, « Specification_on_the_key_features_of_efficient_and_integrated_safety_engineering_process process safety.pdf ». 1 août 2021.

[44] B. Ouni, C. Aussagues, S. Dhouib, et C. Mraidha, « Model-Driven Architectural Framework towards Safe and Secure Nuclear Power Reactors », *Sensors*, vol. 21, n° 15, p. 5136, juill. 2021, doi: 10.3390/s21155136.
[45] O. Lisagor, T. Kelly, et R. Niu, « Model-based safety assessment: Review of the discipline and its challenges », in *The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety*, Guiyang, China, juin 2011, p. 625-632. doi: 10.1109/ICRMS.2011.5979344.
[46] A. A. Abdellatif et F. Holzapfel, « Model Based Safety Analysis (MBSA) Tool for Avionics Systems Evaluation », in *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, oct. 2020, p. 1-5. doi: 10.1109/DASC50938.2020.9256578.
[47] N. Sannier et B. Baudry, « INCREMENT: A Mixed MDE-IR Approach for Regulatory Requirements Modeling and Analysis », in *Requirements Engineering: Foundation for Software Quality*, vol. 8396, C. Salinesi et I. van de Weerd, Éd. Cham: Springer International Publishing, 2014, p. 135-151. doi: 10.1007/978-3-319-05843-6_11.
[48] Y. Choi, M. D. Nguyen, et T. N. Kerr, « Syntactic and semantic information extraction from NPP procedures utilizing natural language processing integrated with rules », *Nuclear Engineering and Technology*, vol. 53, n° 3, p. 866-878, mars 2021, doi: 10.1016/j.net.2020.08.010.
[49] S. Suman, « Artificial intelligence in nuclear industry: Chimera or solution? », *Journal of Cleaner Production*, vol. 278, p. 124022, janv. 2021, doi: 10.1016/j.jclepro.2020.124022.
[50] ISO, « ISO/IEC/IEEE 15026-1:2019 ». Consulté le: 29 août 2022. [En ligne]. Disponible sur: https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/07/35/73567.html
[51] B. Nastov, « Contribution to an equipped approach for the design of executable, verifiable and interoperable Domain Specific Modelling Languages for Model Based Systems Engineering », Theses, Université Montpellier, 2016. Consulté le: 30 septembre 2022. [En ligne]. Disponible sur: https://tel.archives-ouvertes.fr/tel-01809000
[52] « A conceptual, methodological and technical contribution for Modeling and V&V in MBSE context ».
[53] A. van Deursen, P. Klint, et J. Visser, « Domain-specific languages: an annotated bibliography », *SIGPLAN Not.*, vol. 35, n° 6, p. 26-36, juin 2000, doi: 10.1145/352029.352035.
[54] N. Papakonstantinou, J. Linnosmaa, J. Alanen, A. Z. Bashir, B. O'Halloran, et D. L. Van Bossuyt, « Early Hybrid Safety and Security Risk Assessment Based on Interdisciplinary Dependency Models », in *2019 Annual Reliability and Maintainability Symposium (RAMS)*, Orlando, FL, USA, janv. 2019, p. 1-7. doi: 10.1109/RAMS.2019.8768943.
[55] H.-J. Bär et P. Bopp, « M. H. Kalos and P. A. Whitlock: Monte Carlo Methods, Volume I: Basics, John Wiley and Sons, New York, Chichester, Brisbane, Toronto and Singapore 1986, Library of Congress QA298.K35 1986. 186 Seiten mit einem Index, Preis: £ 29.00 », *Berichte der Bunsengesellschaft für physikalische Chemie*, vol. 92, n° 4, p. 560-560, 1988, doi: 10.1002/bbpc.198800128.
[56] C. Yu et E. Gnanapragasam, « RESRAD: Model description and evaluation of model performance », International Atomic Energy Agency (IAEA), 1011-4289, 1996.
[57] « Guide to the Systems Engineering Body of Knowledge (SEBoK) », INCOSE. Consulté le: 16 juin 2021. [En ligne]. Disponible sur: https://www.sebokwiki.org/w/images/sebokwiki-farm!w/9/90/Guide_to_the_Systems_Engineering_Body_of_Knowledge%2C_v._2.4.pdf
[58] B. Schindel, « INCOSE Model-Based SE Transformation », p. 30.
[59] S. Friedenthal, R. Griego, et M. Sampson, « INCOSE model based systems engineering (MBSE) initiative », in *INCOSE 2007 symposium*, 2007, vol. 11.
[60] ISO/IEC/IEEE, « 42010:2011 ». Consulté le: 21 mai 2022. [En ligne]. Disponible sur: https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/05/05/50508.html
[61] J. Navas, P. Tannery, S. Bonnet, et J.-L. Voirin, « Bridging the Gap Between Model-Based Systems Engineering Methodologies and Their Effective Practice – A Case Study on Nuclear Power Plants Systems Engineering », *INCOSE INSIGHT*, vol. 21, mars 2018, doi: 10.1002/inst.12185.
[62] M. Zhuang, X. Zhao, et Z. Siqiao, « Study on the NPP general operation strategy design method based on MBSE », mai 2019, Consulté le: 16 juin 2021. [En ligne]. Disponible sur: http://inis.iaea.org/Search/search.aspx?orig_q=RN:51005223

[63] S. J. Russell, P. Norvig, et E. Davis, *Artificial intelligence: a modern approach*, 3rd ed. Upper Saddle River: Prentice Hall, 2010.
[64] A. Colmerauer et P. Roussel, « The birth of Prolog », in *History of programming languages---II*, New York, NY, USA: Association for Computing Machinery, 1996, p. 331-367. Consulté le: 2 octobre 2022. [En ligne]. Disponible sur: https://doi.org/10.1145/234286.1057820
[65] R. Hoehndorf et N. Queralt-Rosinach, « Data Science and symbolic AI: Synergies, challenges and opportunities », *DS*, vol. 1, n° 1-2, p. 27-38, déc. 2017, doi: 10.3233/DS-170004.
[66] « Sémantiques Métier pour l'exploitation de Données multi-sources (SMD) », *IRT SystemX*. https://www.irt-systemx.fr/projets/SMD/ (consulté le 25 août 2022).
[67] Stanford University, « Measuring trends in Artificial Intelligence », *aiindex.stanford.edu*. https://public.tableau.com/views/ResearchDevelopment_16145904716170/1_1_1b?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=no&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en&:loadOrderID=0 (consulté le 21 mai 2022).
[68] Pierre Lison, Language Technology Group (LTG), « An introduction to machine learning LGT, University of Oslo », Oslo, 3 octobre 2012. Consulté le: 21 mai 2022. [En ligne]. Disponible sur: https://studylib.net/doc/11539838/an-introduction-to-machine-learning-pierre-lison--languag...
[69] E. D. Liddy, « Natural Language Processing », p. 15.
[70] R. M. French, « The Turing Test: the first 50 years », *Trends in Cognitive Sciences*, vol. 4, n° 3, p. 115-122, mars 2000, doi: 10.1016/S1364-6613(00)01453-4.
[71] F. De Saussure, *Course in general linguistics*. Columbia University Press, 2011.
[72] N. Chomsky, *Aspects of the Theory of Syntax*, vol. 11. MIT press, 2014.
[73] A. Vaswani *et al.*, « Attention Is All You Need ». arXiv, 5 décembre 2017. doi: 10.48550/arXiv.1706.03762.
[74] J. Devlin, M.-W. Chang, K. Lee, et K. Toutanova, « BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding », in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, Minneapolis, Minnesota, juin 2019, p. 4171-4186. doi: 10.18653/v1/N19-1423.
[75] E. Roumili, J.-F. Bossu, V. Chapurlat, A. Iancheruk, R. Plana, et J. Tixier, « Requirements Engineering enabled by Natural Language Processing and Artificial Intelligence for Nuclear Safety Demonstration. », p. 15.
[76] « NLP's ImageNet moment has arrived », *The Gradient*, 8 juillet 2018. https://thegradient.pub/nlp-imagenet/ (consulté le 26 août 2022).
[77] C. J. Cellucci, A. M. Albano, et P. E. Rapp, « Comparative study of embedding methods », *Phys. Rev. E*, vol. 67, n° 6, p. 066210, juin 2003, doi: 10.1103/PhysRevE.67.066210.
[78] Y. Goldberg, *Neural network methods for natural language processing*. San Rafael, Calif.: Morgan & Claypool Publishers, 2017. doi: 10.2200/S00762ED1V01Y201703HLT037.
[79] K. W. Church, « Word2Vec », *Natural Language Engineering*, vol. 23, n° 1, p. 155-162, janv. 2017, doi: 10.1017/S1351324916000334.
[80] « Papers with Code - Deep contextualized word representations ». https://paperswithcode.com/paper/deep-contextualized-word-representations (consulté le 26 août 2022).
[81] J. Pennington, R. Socher, et C. Manning, « Glove: Global Vectors for Word Representation », in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, Doha, Qatar, 2014, p. 1532-1543. doi: 10.3115/v1/D14-1162.
[82] KAIZEN Solutions, *Lunch CRRA - AFIS // Les travaux Agile-Systems Engineering au sein de l'AFIS*, (9 février 2022). Consulté le: 21 juin 2022. [En ligne Vidéo]. Disponible sur: https://www.youtube.com/watch?v=19dNPbindRM
[83] E. C. Conforto, D. C. Amaral, S. L. da Silva, A. Di Felippo, et D. S. L. Kamikawachi, « The agility construct on project management theory », *International Journal of Project Management*, vol. 34, n° 4, p. 660-674, mai 2016, doi: 10.1016/j.ijproman.2016.01.007.

[84] M. Fowler et J. Highsmith, « Facilitating change is more effective than attempting to prevent it. Learn to trust in your ability to respond to unpredictable events; it's more important than trusting in your ability to plan for disaster. », p. 7.
[85] M. A. Robinson, « An empirical analysis of engineers' information behaviors », *Journal of the American Society for Information Science and Technology*, vol. 61, n° 4, p. 640-658, 2010, doi: 10.1002/asi.21290.
[86] N. Reimers et I. Gurevych, « Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks », arXiv, arXiv:1908.10084, août 2019. doi: 10.48550/arXiv.1908.10084.
[87] L. Martin *et al.*, « CamemBERT: a Tasty French Language Model », in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, 2020, p. 7203-7219. doi: 10.18653/v1/2020.acl-main.645.
[88] Stephanie, « Matthews Correlation Coefficient », *Statistics How To*, 29 novembre 2020. https://www.statisticshowto.com/matthews-correlation-coefficient/ (consulté le 9 septembre 2022).
[89] M. Verleysen, Éd., *ESANN 2014: 22nd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning : Bruges, Belgium, April 23-24-25, 2014 : proceedings*. Louvain-la-Neuve: Ciaco - i6doc.com, 2014.
[90] D. Chicco et G. Jurman, « The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation », *BMC Genomics*, vol. 21, n° 1, p. 6, janv. 2020, doi: 10.1186/s12864-019-6413-7.
[91] M. Chemuturi, *Requirements Engineering and Management for Software Development Projects*. Springer Science & Business Media, 2012.
[92] K. I. G. Sotelo, X. Yi, C. Baron, P. Esteban, C. Y. A. G. Estrada, et L. de J. L. Velázquez, « Avez-vous identifié toutes les parties prenantes ? », juin 2018, p. 8p. Consulté le: 29 août 2022. [En ligne]. Disponible sur: https://hal.laas.fr/hal-01827377
[93] S. Das, N. Deb, A. Cortesi, et N. Chaki, « Sentence Embedding Models for Similarity Detection of Software Requirements », *SN COMPUT. SCI.*, vol. 2, n° 2, p. 69, févr. 2021, doi: 10.1007/s42979-020-00427-1.
[94] W. Alhoshan, R. Batista-Navarro, et L. Zhao, « Semantic Frame Embeddings for Detecting Relations between Software Requirements », in *Proceedings of the 13th International Conference on Computational Semantics - Student Papers*, Gothenburg, Sweden, mai 2019, p. 44-51. doi: 10.18653/v1/W19-0606.
[95] R. Sonbol, G. Rebdawi, et N. Ghneim, « The Use of NLP-Based Text Representation Techniques to Support Requirement Engineering Tasks: A Systematic Mapping Review », *IEEE Access*, vol. 10, p. 62811-62830, 2022, doi: 10.1109/ACCESS.2022.3182372.
[96] ISO/IEC, « ISO/IEC 19510:2013 BPMN ». Consulté le: 22 mai 2022. [En ligne]. Disponible sur: https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/06/26/62652.html
[97] « Eclipse Modeling Framework - Interview with Ed Merks », *JAXenter*, 16 avril 2010. https://jaxenter.com/eclipse-modeling-framework-interview-with-ed-merks-100007.html (consulté le 22 mai 2022).
[98] « EMOF : Essential Meta Object Facility ». https://www.eclipse.org/modeling/emft/search/concepts/EMOF.html (consulté le 17 mars 2022).
[99] OMG, « Meta Object Facility Specification Version 2.5.1 ». Consulté le: 22 mai 2022. [En ligne]. Disponible sur: https://www.omg.org/spec/MOF/
[100] F. Budinsky, R. Ellersick, D. Steinberg, T. J. Grose, et E. Merks, *Eclipse Modeling Framework: A Developer's Guide*. Addison-Wesley Professional, 2004.
[101] P. Roques, « MBSE with the ARCADIA Method and the Capella Tool », Toulouse, France, janv. 2016. Consulté le: 16 juin 2021. [En ligne]. Disponible sur: https://hal.archives-ouvertes.fr/hal-01258014
[102] AFNOR, « XP Z67-140 Norme ARCADIA », *Afnor EDITIONS*. https://www.boutique.afnor.org/fr-fr/norme/xp-z67140/technologies-de-linformation-arcadia-methode-pour-lingenierie-des-systemes-/fa192970/1723 (consulté le 22 mai 2022).
[103] « Eclipse (projet) - Wikiwand ». https://www.wikiwand.com/fr/Eclipse_(projet) (consulté le 17 mars 2022).
[104] « Kitalpha ». https://www.eclipse.org/kitalpha/ (consulté le 17 mars 2022).

[105] *Python4Capella*. Labs for Capella, 2022. Consulté le: 2 octobre 2022. [En ligne]. Disponible sur: https://github.com/labs4capella/python4capella
[106] I. A. El-Khair, « Term Weighting », in *Encyclopedia of Database Systems*, L. LIU et M. T. ÖZSU, Éd. Boston, MA: Springer US, 2009, p. 3037-3040. doi: 10.1007/978-0-387-39940-9_943.
[107] G. A. Miller, R. Beckwith, C. Fellbaum, D. Gross, et K. J. Miller, « Introduction to WordNet: An On-line Lexical Database* », *International Journal of Lexicography*, vol. 3, n° 4, p. 235-244, déc. 1990, doi: 10.1093/ijl/3.4.235.
[108] Imagile, « Accueil », *Naarea*. https://www.naarea.fr/ (consulté le 9 septembre 2022).
[109] Z. Liu et J. Fan, « Technology readiness assessment of Small Modular Reactor (SMR) designs », *Progress in Nuclear Energy*, vol. 70, p. 20-28, janv. 2014, doi: 10.1016/j.pnucene.2013.07.005.
[110] J. Larsen, « Why do 87% of data science projects never make it into production? », *VentureBeat*, 19 juillet 2019. https://venturebeat.com/ai/why-do-87-of-data-science-projects-never-make-it-into-production/ (consulté le 24 septembre 2022).

9 Annex

9.1 Summary of the Metamodel

All concepts from the metamodel are synthetized in net table.

Retained Safety Demonstration Concept	***Definition***
Aggression	External aggression: General definition of an external aggression Phenomenon or event that may have adverse consequences for the operation or functioning of an installation and whose cause is external to the installation Objectives of the protection approach against external aggression: Following an external aggression, the fundamental objectives are to : To preserve the integrity of the main primary circuit To stop the reactor and evacuate the residual power To limit the possible release of radioactive substances to an acceptable value Protection approach against external hazards: Protection against hazards at the design stage and during the operation of the installations Choice of the site Characterisation of the hazard or risk: intensity/frequency or probability Identification of the structures and equipment to be protected Definition of the protection provisions: constructional, warning system, operation... Definition of the requirements associated with the protection provisions (classification, electrical emergency, periodic monitoring, etc.) Review (evolving hazards/evolution of knowledge, feedback, sufficiency of protection provisions over time) Internal aggressions
Argument	Arguments, which link the evidence to the claim. These are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established" [28], together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit.
BehaviorModellingDSML	DSML to model scenarios for safety specification.
CA	Defined Quality (DQ) (here considered as an expected characteristic) Definition: all the functional performances of the Item Important for Protection as well as the operating and environmental conditions in which these performances must be ensured Objective: to ensure the good behaviour (integrity or functional capacity) of the PIEs with respect to the actions to which they may be subjected or which they must ensure Example: PIE: Control of the containment of radioactive substances PIE: Nuclear ventilation Depression level Renewal rate PIE: Filtration device Filtration efficiency

CAEFrameworkModellingDSML	The key elements of the CAE approach are: — Claims, which are assertions put forward for general acceptance. These are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims. — Arguments, which link the evidence to the claim. These are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established", together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit. — Evidence, which is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis.
Characteristic	A distinctive attribute or aspect of something.
Claim	Assertions put forward for general acceptance. These are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims.
ClaimCalculation	This block is used to claim that the value of a property of a system can be computed from the values of related properties of other objects (e.g. its subsystems). One application of the block is to provide a quantitative argument when the value of one property can be calculated from the values of other specific properties.
ClaimConcretion	This block is used when a claim needs to be given a more precise definition or interpretation. This is often the case of top-level claims, which generally need to be expressed in more measurable, less abstract, terms.
ClaimDecomposition	This block is concerned with structure. Many claim decompositions are about partitioning some aspect of the claim, for example, according to the functions of the system, the architecture, the properties being considered or with respect to some sequence such as life cycle phases or modes of operation.
ClaimEvidenceIncorporation	This block is used at the edge of the CAE structure to incorporate evidence into the assessment. It is used to demonstrate that a subclaim is directly satisfied by its supporting evidence.
ClaimSubstitution	Another common type of claim expansion involves transforming a claim about an object (or property) into a claim about an equivalent object (or property), which can be viewed as a form of substitution.
ClassificationDependFromFPI	Depending on the FPI considered, different classifications will be given to the components.

Component	A sub-element of the installation performing functions allocated to it.
ConnexionInteraction	Abstract Class: to model links, flows and other interaction between other objects (components, functions, FPI, ...)
Data	Collection of discrete values that convey information, describing quantity, quality, fact, statistics, other basic units of meaning, or simply sequences of symbols that may be further interpreted.
DataStructureModelingDSML	DSML dealing with the data structure.
DecomposableConnectableElement	Element which can be decomposed and connected.
DecomposableElement	Abstract Class; Element that can be decomposed.
Document	a piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record.
ED	ED: requirements assigned to a IIP (Item Important for Protection) or AIP (Activity Important for Protection) to meet its objectives as described in the demonstrative part of the safety report or other binding document. Article 251: The requirements necessary to achieve and maintain the quality of IIPs shall be identified. They shall be proportionate to the issues at stake in order to guarantee for each element the functions assigned to it. These requirements are referred to as "defined requirements" in this order. [The defined requirements are adapted according to the importance for the safety of the IIP considered.]
EngineeringModel	Model used in engineering processes.
Event	Incident/Accident occurring in the installation and triggering a scenario.
Evidence	Evidence, which is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis.
EX	High level of safety requirements, necessary in the regulation.
Flow	Any set of items that are from energy, material or data nature. A flow is exchanged between functions....
FPI	Fundamental safety functions (see Figure 5) for the protection of people and environment: - The control of the nuclear chain reaction, - Thermal power removal. - Containment of radioactive substances. - Protection of people and the environment against ionising radiation. These functions must be ensured in all possible states of the installation. They are also called "FPI" Interest Protection Functions.

Function	An action, a task, or an activity performed to achieve a desired outcome. (Hitchins 2007)
FunctionningCondition	Demonstration of safety against internal events (1/2) : Design Basis Operating Conditions Identification of a limited number of representative and enveloped events called Design Basis Operating Conditions. Internal events divided into 4 categories of annual frequencies/reactor Category: I- Normal conditions II- Moderate frequency accidents Ill- Very low frequency accidents IV- Hypothetical accidents Annual frequency/reactor 10-2 to 1 10-4 to 10-2 10-6 to 10-4
ICFunction	Instrumentation & Control function.
Link	Any logical or physical relation (e.g. cable, tube, wifi protocol, ...) that connects logical or physical components and transfer flows from various nature: data, material or energy
MeasurementFunction	Physical characteristics measurement function.
ModelKind_DSML	Abstract Class: to model any modelling language (i.e. model kind or DSML) and allow to structure metamodel by sharing common relations and attributes of such modelling languages
ModelStatement	Element which can be extracted from models and is a statement used in a demonstration for example.
NamedElement	Abstract Class: requested to structure and organise metamodel
Qualification	Process of determining whether a system or component is suitable for operational use.
QualificationDependFromAggression	Qualification of a system to resist a type of aggression.
Repository	Abstract Class: to model any kind of data repositories
Requirement	A requirement is “a statement that identifies a system, product or process characteristic or constraint, which is unambiguous, clear, unique, consistent, stand-alone (not grouped), and verifiable, and is deemed necessary for stakeholder acceptability.” (INCOSE 2010)
RequirementsRepository	Repository that gathers all requirements (in our case: safety requirements).
Risk	A multi-attribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with exposures or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences. (IAEA)
SafetyActivity	Activity aimed at ensuring nuclear safety.

SafetyFeatureGroup	Group of Components which assures together a Safety Function (cf Safety Function).
SafetyFunction	A specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions.
SafetyGlobalObjective	Objective set for each situation in the installation not to be exceeded (dosimetry etc.)
SafetyNamedElement	Element which is linked to safety.
SafetyReferenceKnowledgeRepository	DSML to model scenarios with the aim of enabling safety specification.
SafetyReferenceKnowledgeRepository	Repository storing safety references
SafetyRequirementsSpecificationModellingDSML	DSML for specification of nuclear safety requirements through several diagrams (architecture diagrams etc.).
SafetyStudySystemBlock	Element of our metamodel grouping all other elements. This element allows us to integrate our metamodel into a developed tool.
Scenario	A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility, or the possible future evolution of a disposal facility and its surroundings. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes).
SideClaim	Claims which are supposed to validate the arguments used.
Situation	Circonstances dans lesquelles se trouvent l'installation (normal, incidentel, accidentel).
Stakeholder	Individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations (ISO/IEC/IEEE 2015)

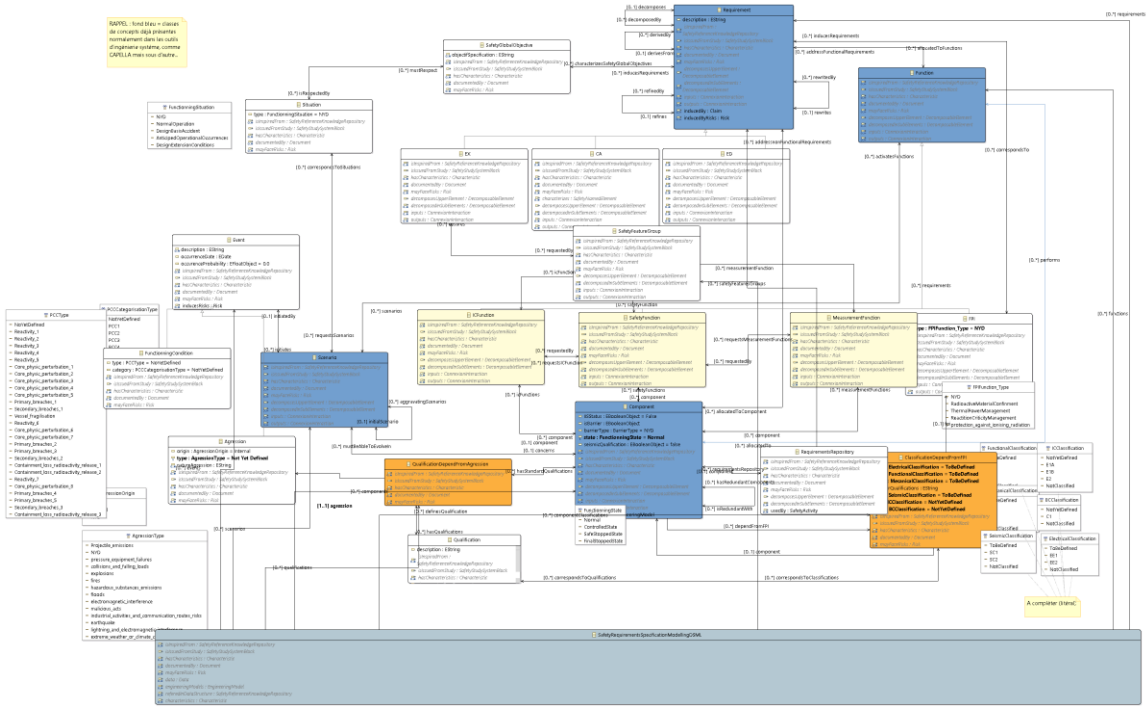


Figure 100 [ModelKind] Safety requirements specification

Function	**An action, a task, or an activity performed to achieve a desired outcome (Hitchins 2007)**
Aggression	External aggression : - Definition general definition of an external aggression : Phenomenon or event likely to have consequences harmful to the functioning or operation of an installation and whose cause is external to the installation. - Objectives of the approach to protection against external hazards: Maintain the integrity of the main primary circuit, Shut down the reactor and evacuate the residual power Limit the possible release of radioactive substances to an acceptable value. Protection approach with regard to external hazards: Protection against hazards at the design stage and during the operation of the installations, Choice of site, Characterisation of the al éa or risk: intensity/ frequency or probability, Identification of the structures and equipment to be protected , Definition of the protection provisions: construction, warning system, operation... Definition of the requirements associated with the protection provisions (classification, backup electrical, periodic monitoring, etc.) Re-examination (changing hazards / evolution of knowledge, REX, sufficient protection provisions over time
SafetyFeatureGroup	Group of Components which together ensure a Safety Function (see Safety Function).
CA	Defined Quality (DQ) (here considered as an expected characteristic) Definition: all the functional performances of the Item Important for Protection as well as the operating and environmental conditions in which these performances must be ensured Objective: to ensure the good behaviour (integrity or functional capacity) of the IIPs with respect to the actions to which they may be subjected or which they must ensure
Component	A sub-element of the installation performing functions allocated to it.
Situation	Circumstances in which the facility is operating (normal, incidental, accidental).
SafetyFunction	A specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions.
RequirementsRepository	Repository that gathers all requirements (in our case: safety requirements).
ICFunction	Instrumentation & Control function.
Event	Incident/Accident occurring in the installation and triggering a scenario.

SafetyGlobalObjective	Objective set for each situation in the installation not to be exceeded (dosimetry etc.)
REIT	Fundamental safety functions for the protection of people and environment: - The control of the nuclear chain reaction - Thermal power removal. - Containment of radioactive substances. - Protection of people and the environment against ionising radiation. These functions must be ensured in all possible states of the installation. They are also called "FPI" Interest Protection Functions.
SafetyRequirementsSpecificationModellingDSML	DSML for specification of nuclear safety requirements through several diagrams (architecture diagrams etc.).
MeasurementFunction	Physical characteristics measurement function.
ClassificationDependFromFPI	Depending on the FPI considered, different classifications will be given to the components.
Scenario	A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility, or the possible future evolution of a disposal facility and its surroundings. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes).
QualificationDependFromAgression	Qualification of a system to resist a type of aggression.
FunctioningCondition	Demonstration of safety against internal events (1/2) : Design Basis Operating Conditions Identification of a limited number of representative and enveloped events called Design Basis Operating Conditions. Internal events divided into 4 categories of annual frequencies/reactor Category: I- Normal conditions II- Moderate frequency accidents Ill- Very low frequency accidents IV- Hypothetical accidents Annual frequency/reactor 10-2 to 1 10-4 to 10-2 10-6 to 10-4
Qualification	Process of determining whether a system or component is suitable for operational use.
Requirement	A requirement is "a statement that identifies a system, product or process characteristic or constraint, which is unambiguous, clear, unique, consistent, stand-alone (not grouped), and verifiable, and is deemed necessary for stakeholder acceptability. (INCOSE 2010)
ED	ED: requirements assigned to a IIP (Item Important for Protection) or AIP (Activity Important for Protection) to meet its objectives as described in the demonstrative part of the safety report or other binding document. Article 251: The requirements necessary to achieve and maintain the quality of IIPs shall be

	identified. They shall be proportionate to the issues at stake in order to guarantee for each element the functions assigned to it. These requirements are referred to as "defined requirements" in this order. [The defined requirements are adapted according to the importance for the safety of the IIP considered].
EX	High level of safety requirements, necessary in the regulation.

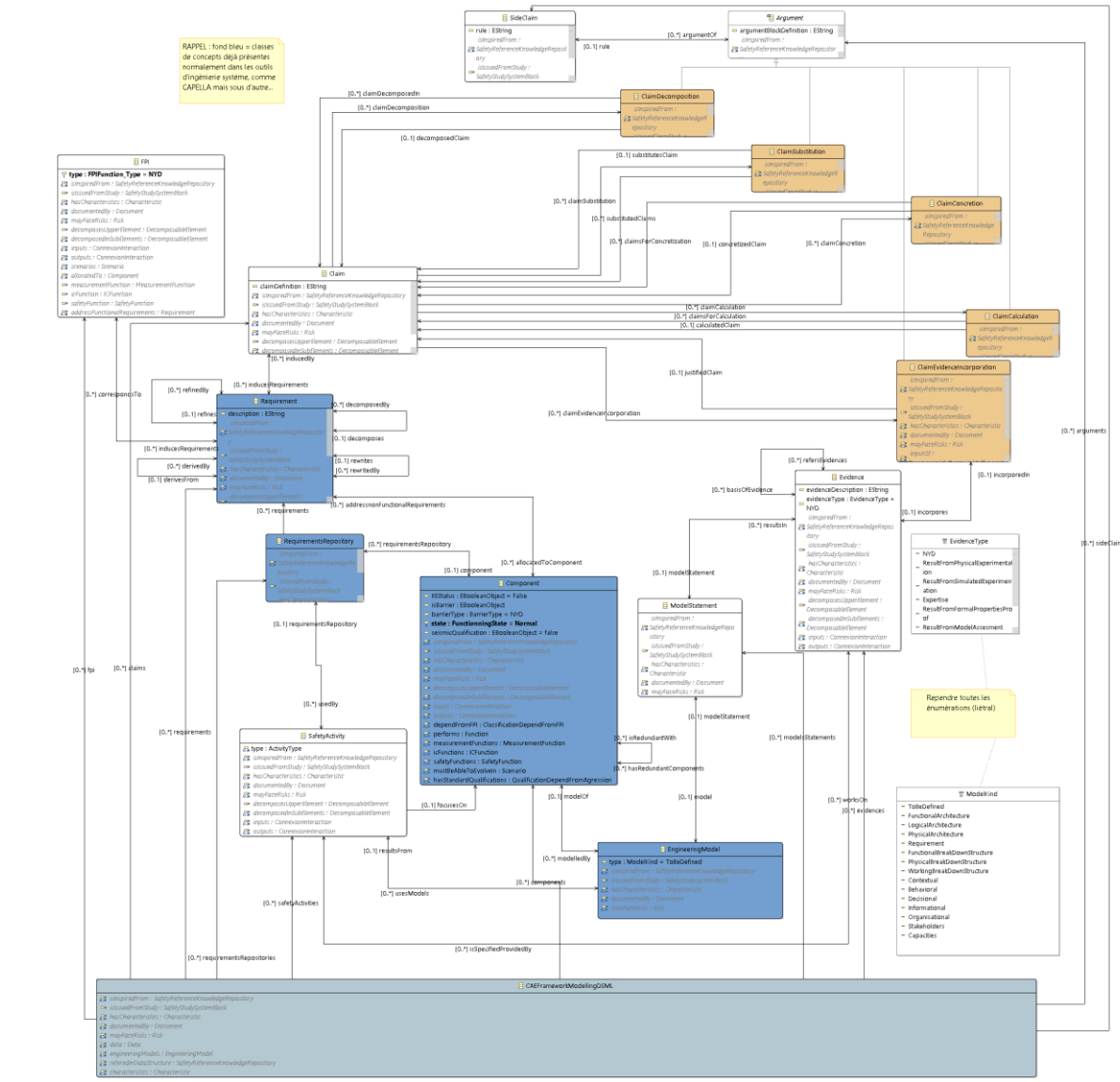


Figure 101 [ModelKind] CAE framework specification

ClaimSubstitution	Another common type of claim expansion involves transforming a claim about an object (or property) into a claim about an equivalent object (or property), which can be viewed as a form of substitution.
ModelStatement	Element which can be extracted from models and is a statement used in a demonstration for example.
Evidence	Evidence, which is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis.
Component	A sub-element of the installation performing functions allocated to it.
RequirementsRepository	Repository that gathers all requirements (in our case: safety requirements).
ClaimCalculation	This block is used to claim that the value of a property of a system can be computed from the values of related properties of other objects (e.g. its subsystems). One application of the block is to provide a quantitative argument when the value of one property can be calculated from the values of other specific properties.
REIT	Fundamental safety functions (see Figure 5) for the protection of people and environment: - The control of the nuclear chain reaction - Thermal power removal. - Containment of radioactive substances. - Protection of people and the environment against ionising radiation. These functions must be ensured in all possible states of the installation. They are also called "FPI" Interest Protection Functions.
SafetyActivity	Activity aimed at ensuring nuclear safety.
CAEFrameworkModellingDSML	The key elements of the CAE approach are: - Claims, which are assertions put forward for general acceptance. These are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims. - Arguments, which link the evidence to the claim. These are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established", together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit. - Evidence, which is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis.
ClaimConcretion	This block is used when a claim needs to be given a more precise definition or interpretation. This is often the case of top-level claims, which generally need to be expressed in more measurable, less abstract, terms.
ClaimDecomposition	This block is concerned with structure. Many claim decompositions are about partitioning some aspect of the claim, for example, according to the

	functions of the system, the architecture, the properties being considered or with respect to some sequence such as life cycle phases or modes of operation.
ClaimEvidenceIncorporation	This block is used at the edge of the CAE structure to incorporate evidence into the assessment. It is used to demonstrate that a subclaim is directly satisfied by its supporting evidence.
Claim	Assertions put forward for general acceptance. These are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims.
SideClaim	Claims which are supposed to validate the arguments used.
Requirement	A requirement is "a statement that identifies a system, product or process characteristic or constraint, which is unambiguous, clear, unique, consistent, stand-alone (not grouped), and verifiable, and is deemed necessary for stakeholder acceptability. (INCOSE 2010)
Argument	Arguments, which link the evidence to the claim. These are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established" [28], together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit.
EngineeringModel	Model used in engineering processes.

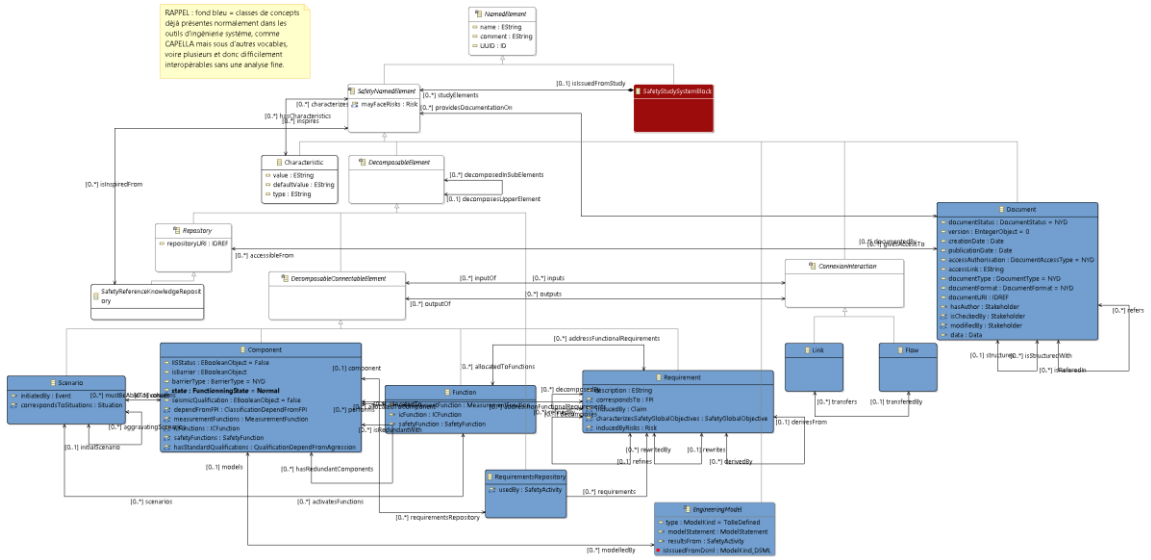


Figure 102 [Structuring] Shared elements

Function	See Function
SafetyReferenceKnowledgeRepository	Repository storing safety references
Link	Any logical or physical relation (e.g. cable, tube, wifi protocol, ...) that connects logical or physical components and transfer flows from various nature:

	data, material or energy
NamedElement	Abstract Class: requested to structure and organise metamodel
ConnectionInteraction	Abstract Class: to model links, flows and other interaction between other objects (components, functions, FPI, ...)
Flow	Any set of items that are from energy, material or data nature. A flow is exchanged between functions....
SafetyStudySystemBlock	See SafetyStudySystemBlock
Repository	See Repository
DecomposableElement	See DecomposableElement
Characteristic	See Characteristic
Requirement	See Requirement
Document	See Document
SafetyNamedElement	See SafetyNamedElement
Component	See Component
Scenario	See Scenario
DecomposableConnectableElement	See DecomposableConnectableElement
RequirementsRepository	See RequirementsRepository
EngineeringModel	See EngineeringModel

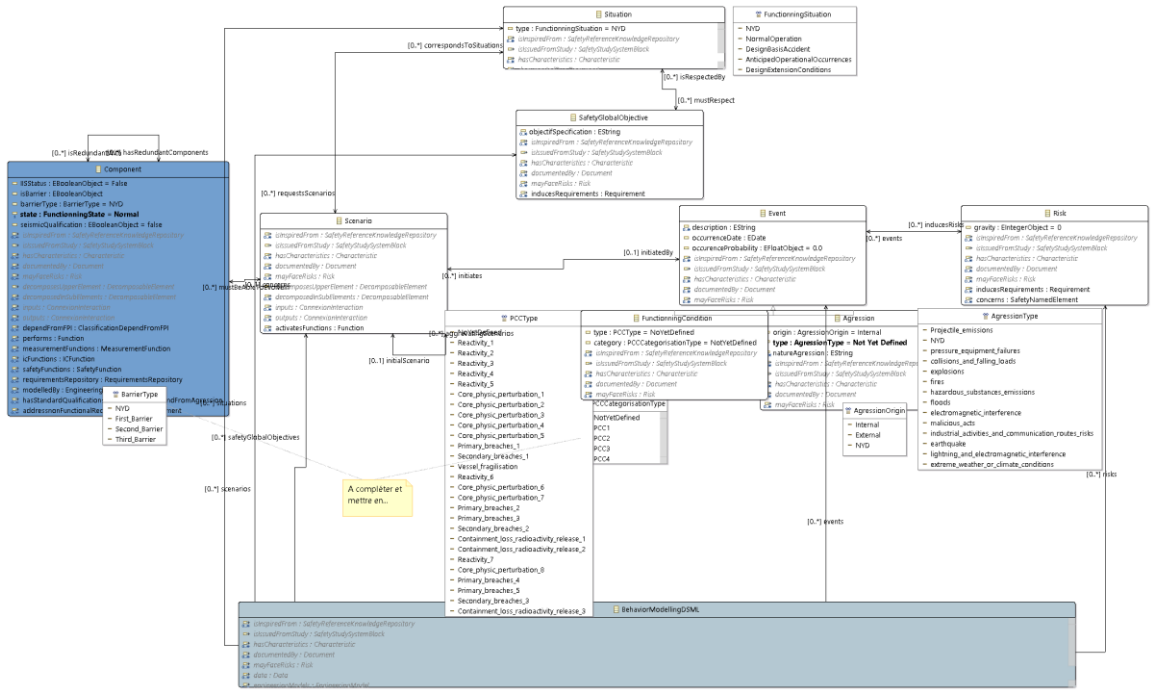


Figure 103 [ModelKind] Behavioral specification (scenario, situation, ...)

BehaviorModellingDSML	See BehaviorModellingDSML
Aggression	See Aggression
Component	See Component
Situation	See Situation
Scenario	See Scenario
FunctioningCondition	See FunctioningCondition
Event	See Event
SafetyGlobalObjective	See SafetyGlobalObjective
Risk	A multiattribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with exposures or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences. (IAEA)

Résumé : Démontrer la sûreté nucléaire est une priorité dans tous les projets de développement d'installation nucléaire. Ces projets sont cependant de plus en plus complexes. Ils visent en effet le développement de systèmes eux-mêmes complexes comme une centrale nucléaire (NPP, plus de 50 bâtiments, 500 km de tuyauterie, 500 000 composants et entraine la production de 100 millions de données, rapports, schémas, etc. Ils impliquent enfin plusieurs parties prenantes (client, exploitant, acteurs métier, régulateur, usagers, public, ...) avec des attentes (besoins opérationnels, environnementaux, sûreté, sécurité, disponibilité, …) et des contraintes variées de délais, de budget, de qualité, de ressources ou encore de savoirs faire. Cette démonstration de sûreté exige donc un effort particulier, une méthode et des outils de travail pour assurer et convaincre toutes ces parties prenantes de la tenue des attentes, en particulier en termes de sûreté nucléaire. Différentes difficultés doivent donc être étudiées et les moyens de les maitriser doivent être proposés dans le cadre de ces travaux :

- Absence d'accord sur une terminologie commune de la démonstration de la sûreté nucléaire ;
- Définition insuffisante d'éléments fortement présents dans la sûreté (e.g. exigence, ou argument);
- Peu de liens entre la démonstration de sûreté nucléaire d'une installation et l'ingénierie de celle-ci ;
- Difficultés méthodologiques diverses : communication dificile entre équipes, absence d'approches pour mener la démonstration, absence d'une réelle traçabilité des exigences de sûreté, manque de vision claire et globale des normes, informations éparses, documentation fragmentée, pas d'approche intégrée de la sûreté dans le projet, difficulté de cognition de la complexité dans un contexte de projet " orienté documents ".
- Difficultés techniques : interopérabilité limitée des outils/techniques souvent dédiés ;
- Difficultés organisationnelles / humaines : manque de personnel ayant une expérience pluridisciplinaire et une vision globale avec un travail privilégiant des modèles à l'instar de documents, réductionnisme de l'ingénierie qui empêche l'adoption des postures de compréhension des autres disciplines.
- Problème éthique et sociétal global : la démonstration nucléaire entraîne souvent une méfiance par défaut en raison des accidents passés.

Ces travaux combinent l'utilisation des techniques d'Intelligence Artificielle et les principes et processus de l'Ingénierie Système, tout particulièrement visent à accentuer et faciliter le rôle de la modélisation, du partage et de l'analyse de modèles qui est promu par l'approche MBSE. La contribution de ces travaux est ainsi une méthode outillée permettant de soutenir toutes les parties prenantes et les ingénieurs de sûreté en charge, concernés ou impactés par les objectifs de démonstration de sûreté. Des techniques d'IA sont utilisées pour aider ces acteurs à cibler et spécifier les exigences de sûreté requises. L'approche MBSE est ensuite enrichie en proposant de nouveaux paradigmes de modélisation et en enrichissant ou promouvant de nouveaux langages de modélisation afin de compléter et vérifier étape par étape la démonstration de sûreté. Une démarche opératoire a ensuite été définie et équipée par le biais de quelques extensions d'une plateforme d'ingénierie système existante. Enfin, un cas de test sur un système de centrale nucléaire est utilisé pour démontrer la viabilité de cette méthode.

Abstract: Demonstrating nuclear safety is a priority in all nuclear installation development projects. However, these projects are becoming increasingly complex. They involve the development of complex systems such as a nuclear power plant (NPP), more than 50 buildings, 500 km of piping, 500,000 components and the production of 100 million data, reports, diagrams, etc. Finally, they involve several stakeholders (customer, operator, business actors, regulator, users, public, etc.) with different expectations (operational, environmental, safety, security, availability, etc.) and various constraints in terms of deadlines, budget, quality, resources, or know-how. This safety demonstration therefore requires a special effort, a method and working tools to ensure and convince all these stakeholders that the expectations are met, particularly in terms of nuclear safety. Various difficulties must therefore be studied and the means to overcome them must be proposed as part of this work:

- - Lack of agreement on a common terminology for the demonstration of nuclear safety.
- - Insufficient definition of elements strongly present in safety (e.g., requirement, or argument);
- - Little linkage between the demonstration of nuclear safety of an installation and its engineering.
- - Various methodological difficulties: difficult communication between teams, lack of approaches to carry out the demonstration, lack of real traceability of safety requirements, lack of a clear and global vision of the standards, scattered information, fragmented documentation, no integrated approach to safety in the project, difficulty in understanding the complexity in a "document-oriented" project context.
- - Technical difficulties: limited interoperability of often dedicated tools/techniques.
- - Organisational / human difficulties: lack of staff with multidisciplinary experience and a global vision with a work that favours models as well as documents, engineering reductionism that prevents the adoption of the understanding postures of other disciplines.
- - Global ethical and societal problem: nuclear demonstration often leads to mistrust by default because of past accidents.

This work combines the use of Artificial Intelligence techniques with the principles and processes of Systems Engineering, particularly to emphasise and facilitate the role of modelling, sharing and analysis of models that is promoted by the MBSE approach. The contribution of this work is thus a tool-based method to support all stakeholders and safety engineers in charge of, concerned with or impacted by safety demonstration objectives. AI techniques are used to help these actors to target and specify the required safety requirements. The MBSE approach is then enriched by proposing new modelling paradigms and enriching or promoting new modelling languages in order to complete and verify the safety demonstration step by step. An operational approach was then defined and equipped through some extensions of an existing system engineering platform. Finally, a test case on a nuclear power plant system is used to demonstrate the viability of this method.