Cross-domain Resilience in Cloud-native, Critical Cyber-Physical Systems Networks : Availability Modeling, Analysis, and Optimization of Critical Services Provisioning

Khaled Sayad

université PARIS-SACLAY

Cross-domain Resilience in Cloud-native, Critical Cyber-Physical Systems Networks : Availability Modeling, Analysis, and Optimization of Critical Services Provisioning

Résilience croisée dans les réseaux de systèmes cyber-physiques cloud-natifs : Modélisation de la Disponibilité, Analyse et Optimisation du provisionnement des services critiques

Thèse de doctorat de l'université Paris-Saclay

École doctorale n°573 matériaux, systèmes, usages (INTERFACES)
Spécialité de doctorat : Ingénierie des Systèmes Complexes
Graduate School : Sciences de l'ingénierie et des systèmes. Référent : CentraleSupélec

Thèse préparée à **CentraleSupélec**, sous la direction de **Pr. Anne BARROS**, la co-supervision de **Mr. Benoît LEMOINE *(Orange Innovation Networks)***, et le co-encadrement de **Pr. Yi-Ping FANG** et de **Pr. Zhiguo ZENG**.

Thèse soutenue à Paris-Saclay, le 10 Avril 2024, par

Khaled SAYAD

Composition du jury

Membres du jury avec voix délibérative

Sorin OULU Professeur, Université de Lorraine	Président du jury & Examinateur
Alexandre VOISIN Professeur, Université de Lorraine	Rapporteur & Examinateur
Mitra FOULADIRAD Professeure, Centrale Marseille	Rapportrice & Examinatrice
Vu Hai Canh Enseignant Chercheur, Université de Technologie de Compiègne	Examinateur

THESE DE DOCTORAT

NNT : 2024UPAST028

université PARIS-SACLAY | ÉCOLE DOCTORALE Interfaces: matériaux, systèmes, usages

Titre :Résilience croisée dans les réseaux de systèmes cyber-physiques cloud-natifs : Modélisation de la Disponibilité, Analyse et Optimisation du provisionnement des services critiques
Mots clés : Résilience des infrastructures critiques, modélisation de la disponibilité, virtualisation des fonctions réseau, réseaux définis par logiciel , optimisation, partage d'informations.

Résumé : La résilience des Infrastructures Critiques (ICs) est cruciale pour assurer la sécurité et la stabilité socio-économique dans la société moderne. Ces ICs s'appuient sur un réseau complexe de systèmes cyber-physiques (SCPs) couvrant plusieurs domaines tels que les télécommunications et l'énergie, afin de garantir un flux continu de services critiques. L'évolution du mode opérationnel des ICs modernes, illustré par l'intégration accrue des technologies cloud-natif dans les réseaux SCPs sous-jacents, introduit de nouveaux défis en termes de résilience face aux cyber-risques, qui s'ajoute au problème du dimensionnement optimal du réseau des SCPs avec la contrainte des coûts de déploiement qui résultent des schémas de protection géo-redondant. Dans cette thèse, nous attaquons ces défis en premier lieu par le développement d'un modèle d'évaluation de disponibilité avec comme objectif, la quantification de l'efficacité d'adoption des schémas de protection croisée. Ensuite, on présente un modèle d'orchestration optimale des ressources cloud-natifs mutualisées avec l'objectif de minimiser les coûts des schémas de protection. Enfin, nous abordons la problématique de coordination inter-opérateurs d'ICs d'un point de vue *"confiance"* en proposant une plateforme de partage d'information et de ressource qui exploite la convergence des paradigmes cloud-natif des DataSpaces.

Title : Cross-domain Resilience in Cloud-native, Critical Cyber-Physical Systems Networks : Availability Modeling, Analysis, and Optimization of Critical Services Provisioning
Keywords : Critical Infrastructures Resilience, Availability Modeling, Network Function Virtualization, Software-Defined Networking, Optimization, Information-sharing.

Abstract : The dependability of Critical Infrastructures (CIs) operations is crucial to ensure security and socio-economic stability in modern society. These CIs rely on a complex network of Critical Cyber-Physical Systems (CCPSs), spanning multiple domains such as telecommunication and energy, to guarantee a continuous flow of critical services. The paradigm shift in modern CIs' operational mode, illustrated by the increased integration of cloud-native technologies in the underlying CCPSs networks, brings more challenges in terms of resilience against cyber-risks, and increased deployment costs due to redundancy-based protection schemes. In this dissertation, we tackle these challenges by, first, proposing a model-based, cross-domain dependability evaluation to assess the availability of cloud-native, interdependent critical services and quantify the impact of adopting cross-domain protection mechanisms on critical services' dependability. Secondly, we study the problem of optimal service provisioning based on resource sharing in cloud-native, CCPSs networks with deployment cost and performance constraints. Finally, we tackle the problem of cross-domain coordination from a *Trust* perspective by proposing an architecture for secure and trustful information and resource sharing that exploits the convergence of cloud-native management and DataSpaces paradigm to ensure secure, trustful, and sovereign coordination.

To Yemma, my mom, Zahia Rachedi-Sayad,
Despite your absence, knowing that you would be proud was enough to motivate me to overcome the toughest moments during these last years. This humble achievement is dedicated to you.
-Your son "li y7abbek bezzaf " Moncef-

Acknowledgements

First and foremost, I would like to thank the members of my thesis jury : Pr. Sorin Oulu, Pr. Alexandre Voisin, Pr. Mitra Fouladirad, and Dr. Vu Hai Canh, for taking the time to review my thesis work and for their valuable feedback during the thesis defense process.

I would like to thank my supervisor Benoît LEMOINE for his valuable support during the last three years, and during the thesis defense process. Without his patience, availability, expertise, and dedication, this thesis wouldn't be possible. I extend my deepest gratitude for the members of NAVI team at Orange Innovation for all the shared knowledge during the three years. I am grateful to my manger Jérôme Demay for the support, the good vibes, and his responsiveness. Also, I thank Mr. Benoît Radier and Dr. Nancy Perrot from Orange Innovation for their availability to answer my research questions and for the valuable insights they shared during our meetings.

I would like to thank my supervisors at the LGI/CentraleSpélec : Pr. Anne Barros, Pr. Yiping Fang, and Pr. Zhiguo Zeng for their guidance and patience during the three last years. I extend my gratitude to all my fellow colleagues in the Safety and Risk group for the shared knowledge and unforgettable moments during our ESREL trips.

I would like to acknowledge the financial support of Orange Innovation and the Chair of Risk and Resilience of Complex Systems which allowed the unfolding of this thesis.

This achievement is dedicated to "baba", my father, Ahmed SAYAD. looking back at your sacrifices, and what you had to endure to rise me well, despite the many unfortunate events that impacted your health, fills me with a profound sense of gratitude. I realize now that my adult years, which I once thought difficult, pale in comparison to what you had endured. Inheriting your faith in Allah, perseverance, and values is the best gift I could think of.

This achievement is dedicated to Douàa, my fiancée, your constant support, understanding, and love, are what pushed me to give my best and finish this adventure. To many other adventures...together.

This achievement is also dedicated to my brothers and sisters. Thank you for taking care of me and being there whenever I needed you. I extend this dedication to my nephews and nieces. I want you to know when you grow up and read this manuscript, that Moncef is verry proud to have you in his life and will always be there for you.

I would like to thank my friends : Amine, Hakim, Salah, and Djamel for the hospitality which made my trips to the lab in saclay much enjoyable.

Finally, this thesis is dedicated to the memory of : Mr. Abdelkrim Bouchouta, Mr. Lahcen Abdelouel, and Mr. Pierre Antoine.

Table des matières

Table des figures

Liste des tableaux

Acronymes

5G Fifth Generation of Mobile Telecommunication Technologies

5G-RAN 5G Radio Access Network.

5GC 5G Core

AN Activity Network

CAPEX Capital Expenditures

CCPSs Critical Cyber-Physical Systems

CIs Critical Infrastructures

COTS Commercial Off-The-Shelf

CPS Cyber-Physical System

CRO Centralized Resilience Orchestrator

CSPs Communication Services Providers

DBMS Database Management System

DCs Data Centers

DPaaS Data Plane as a Service

EDC Eclipse DataSpace Components

eDCs Edge Data Centers

EM Element Management

EMS Energy Management System

EPI Electrical Power Infrastructure

ETSI European Telecommunication and Standarization Institute

FAN Field Area Network

FMEA Failure Modes and Effects Analysis

IaaS Infrastructure as a Service

IBN Intent-based Networking

ICT Information and Communication Technologies

IDS International Data Space

IED Intelligent Electronic Device

ISG Industry Specification Group

LCM Life Cycle Management

MANO Management and Orchestration

MILP Mixed Integer Linear Program
MINLP Mixed Integer Non Linear Program
MPC Model Predictive Control
MTTF Mean Time To Failure
MTTR Mean Time To Repair
NAN Neighborhood Area Network
NFV Network Function Virtualization
NFVI Network Function Virtualization Infrastructure
NFVO Network Function Virtualization Orchestrator
NIST National Institute of Standards and Technology
NS Network Service
OPEX Operational Expenditures
OSS Operation Support System
P2P Peer-to-Peer
PaaS Platform as a Service
QoS Quality of Service
RAM Reference Architecture Model
RAN Radio Access Network
SaaS Software as a Service
SANs Stochastic Activity Networks
SCADA Supervisory Control and Data Acquisitiony
SD-SPG SDN-enbaled Smart Power Grid
SDN Software Defined Networking
SDN-C SDN controller
SLOs Service Level Objectives
SOA Service Oriented Availability
SPG Smart Power Grid
SSA Steady State Availability
UPS Uninterruptible Power Supply
URLLC Ultra-Reliable Low-Latency Communications
VIM Virtualization Infrastructure Manager
VNF Virtualized Network Function
VNFD VNF Descriptor
VNFM VNF Manager
WAN Wide Area Network

1 - Introduction

1.1 . General Context

Critical Infrastructures (CIs) like telecommunication, energy, and transportation networks, are the backbone of a nation's economy, and their protection is essential to ensure socioeconomic stability and the well-being of individuals. In the framework of the European Union, CIs are defined as : *"an asset or system which is essential for the maintenance of vital societal functions. The damage to critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, may have a significant negative impact on the security of the EU and the well-being of its citizens."* [1].

Accordingly, the *European Program for Critical Infrastructure Protection (EPCIP)* [2] was launched in order to set the overall procedures and practices to increase the resilience of European CIs by leveraging coordination and information sharing between member states. Similar efforts are witnessed in other regions out of Europe like the United States and the United Kingdom [3, 4], with the same objectives but sometimes with different approaches which is due to cultural, political, technological, and societal differences.

From a technological perspective, CIs can be seen as complex and interdependent networks of Critical Cyber-Physical Systems (CCPSs) spanning multiple domains like telecommunication, energy, and transportation. These CCPSs networks are built on heterogeneous technologies, managed by independent operators, and operate at different timescales [5]. Hence, ensuring CIs protection is a hard and complex task as it requires the coordination of many organizations' efforts which depends on the willingness of all parties to cooperate. Indeed, Public-Private Partnership (PPP) is an intensively discussed topic in CIs protection research [6, 7, 8], which aims to promote information sharing and coordination between public authorities and private CIs operators during disruptive events and enable these private stakeholders to find a trade-off between business interests and their responsibility to protect critical assets.

Furthermore, most of the efforts in coordination-based CIs protection focus on post-disaster information sharing [9, 10]. It turns out that, with the increased penetration of digital technologies in modern CIs, and to keep pace with the proliferating cyber-risks resulting from such transformation [11, 12], developing proactive resilience procedures while minimizing human intervention is urgent in order to reduce response time and minimize the loss induced

by disruptive events.

In this thesis, we focus on telecommunication and power infrastructures as the main CIs of interest. On one hand, the high reliance on telecommunication and power networks, their geographical expansion, and the presence of strong interdependencies make these two CIs more vulnerable to manned and unmanned disruption events as well as failure propagation phenomenon as experienced in major blackouts in Europe and North America [13, 14]. On the other hand, the Information and Communication Technologies (ICT) and Electrical Power Infrastructure (EPI) are shifting towards cloud-native management of their critical asset to deliver more sophisticated services to support complex emerging use cases, and effectively respond to increasing demand for energy and telecommunications to unlock the potential of modern technologies like the fifth generation of mobile telecommunication (5G), Industry 4.0, and Smart Power Grid.

As an example of this shift, we are witnessing the rise of *Telco Cloud* concept where ICT operators manage their network services in cloud infrastructure by means of virtualization technologies [15]. This adds more resilience, flexibility, and cost-effectiveness to service provisioning by auto-scaling computing resources to respond to different situations. For example, in [16], security function like firewalls can be deployed as Virtualized Network Function (VNF)s to be instantiated in case of a high risk of cyber-attacks. This would decrease the cost of running the functions during periods of low risk and enhance the security elsewhen. Overall, the NFV paradigm paves the way to support new ICT use cases with strict performance requirements in terms of latency, connectivity, and computing power.

In the same way, cloud-native technologies are promising enablers for the Smart Power Grid (SPG) [17, 18, 19]. The high penetration of renewable energies, the apparition of micro-grids, and the fast development of electrical mobility might disturb power distribution due to bi-directional power flows. Hence, EPI operators must update power load balancing strategies to ones with strict latency requirements [17]. To this end, virtualization and cloud-native technologies are key enablers of real-time data analytics and processing which is the backbone of modern SPG services (smart metering, real-time load balancing, and third-party applications support). In addition, the flexibility and agility of cloud-native service deployments enable EPI operators to quickly, and fault-free updating of their services in response to changing conditions. This highly relies on the telecommunication infrastructure as a backhaul to support data flow between data generation points and control centers in the power infrastructure [20].

1.2 . Problem Statement & Research Questions

It is obvious from the previous section that the migration of ICT and EPI operators towards cloud-native is crucial to deal with the evolving complexity of telecommunication and energy services delivery. The combination of modern virtualization and edge DC technologies depicted by the deployment of critical energy and telecommunication services as VNFs hosted in geographically distributed, and small size DCs close to physical plants, motivates the need to explore the virtuous cycle of *"reliable energy supply for reliable DCs* and *reliable DCs for reliable energy supply"*. Nevertheless, the journey of ICT and EPI operators toward cloud-native management of their assets faces some bottlenecks which can be classified into three dimensions :

- **Economical** : cloud-native technologies are disruptive in the sense that operators must radically change the technological infrastructure and invest to rearchitect their physical networks. Mainly, by installing new Data Centers (DCs) to support the new business use cases. This will induce huge costs and increase Capital Expenditures (CAPEX) and Operational Expenditures (OPEX) [21].

- **Legislation** : CIs operator must adhere to the country's law in terms of technology integration from other countries/regions in the context of sovereignty. In the example of European CIs, operators cannot rely on non-European cloud providers to host critical services. This will constrain and delay the adoption of cloud-native technologies by operators and force them to adopt local/trustful technologies [22]. In addition, the business interests fueling the cloud migration are conflicting with the environmental obligations of operators to reduce their carbon footprint [23].

- **Risk** : the migration of EPI and ICT toward software-defined service provisioning must be accompanied by corresponding tools to assess the risks and exposure to manned or unmanned attacks due to such transformation from a vulnerability and security perspectives. Also, in order to avoid the impact of new emerging interdependencies [11, 24].

Within this context, sharing the infrastructure at the DC level seems interesting in the sense that it enables ICT and EPI operators to overcome the previous bottlenecks in chorus by tackling them in one unifying framework. In the telecom domain, sharing infrastructure among ICT operators is a viable solution to reduce costs and ensure high service availability and Service Level Objectives (SLOs) [25, 26].

Thanks to the standardization efforts of virtualization technologies, it could be interesting to analyze the correspondent problem of sharing DCs resources among ICT and EPI operators in a geographical area where the resource shortage of an operator in terms of installed DC capacity could be compensated by another operator's DCs resources as illustrated in Figure 1.1 where a *DCs Resource Sharing Orchestrator* is assumed to ensure the cross-domain coordination allowing ICT and EPI operators to "virtually" increase their available resources to build a redundancy scheme usually refereed to as "Availability Zone" in the cloud domain. This latter redundancy scheme can be made dynamic and be adapted to different risk situations, paving the way to reduce CAPEX and OPEX costs by minimizing the installed resources, and thus, reducing energy consumption and the operator's carbon footprint. Also, this would allow ICT and EPI operators to integrate cross-domain risk assessment modules into the shared DCs infrastructure to better estimate the risk of cross-domain failure propagation, and *"software-define"* procedures to withstand disruptive events in real-time. This could be made possible by means of the advancements in service life-cycle management tools in virtualized DCs [27, 28], allowing the automation and integration of resilience strategies into service orchestration level.

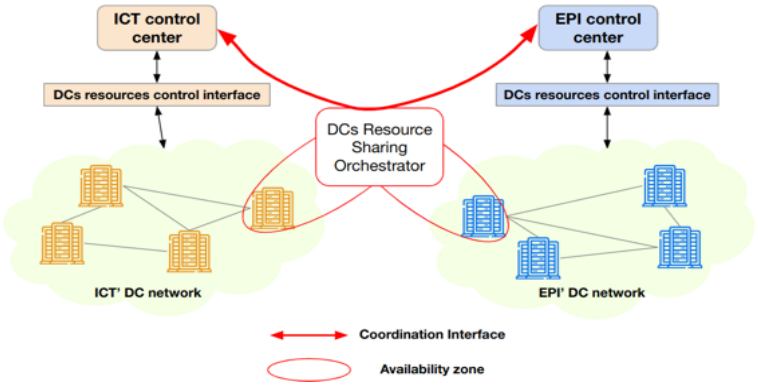


Figure 1.1 – Illustration of the cross-domain resource orchestration interface between ICT and EPI operators.

In the context of this thesis, our primary focus lies in constructing the coordination interface depicted in Figure 1.1. To achieve this goal, a series of steps must be undertaken. First, we need to specify which interdependent services in the telecommunication and power domains might benefit from the coordination-based protection. This requires the availability assessment of such services in different coordination and risk scenarios in order to quantify the gains in terms of availability when sharing resources. Then, the im-

plementation of the cross-domain resilience procedure must be specified. Finally, the problem of information sharing must be addressed in order to deal with privacy and security concerns when sharing the required information to build the cross-domain resilience. In order to tackle these problems, four research questions are formulated, and to be addressed by the present thesis work :

- ***RQ1*** : How to characterize the integration of cloud-native technologies in ICT and EPI operations in terms of complex interdependencies emergence, and opportunities of adopting cross-domain resilience strategies ?

- ***RQ2*** : How to assess the efficiency of cross-domain, coordination-based protection schemes on critical services availability ?

- ***RQ3*** : How to build cross-domain, service protection schemes taking into account performance and cost constraints ?

- ***RQ4*** : How to ensure trustful, private, and secure data exchanges for cross-domain resilience while ensuring an operator's control over its data usage ?

Within these circumstances, the present work aims to address aforementioned research questions by the development of a decision support system to assist ICT and EPI operators in planning their shift towards cloud-native management of networking and energy services.

1.3 . Thesis outline & Summary of contributions

In Chapter 2, we introduce cloud-native technologies : Network Function Virtualization (NFV) and Software Defined Networking (SDN) as two catalysts for the paradigm shift in ICT and EPI services management characterized by the emergence of *Telco Cloud* and *SPG* concepts. The decoupling between the control and data planes in SDN, and the decoupling between applications software and hardware in NFV, enable the ICT operator to flexibly control its network element and propose Data Plane as a Service (DPaaS). This class of services is of interest for the EPI operator to reach real-time, dynamic control and monitoring of the power distribution. This leads to the introduction of an architecture of SDN-enbaled Smart Power Grid (SD-SPG) which will be used to formulate a use-case of dynamic DCs resource sharing as a tool to increase critical services redundancy and thus, enhance their availability. The formulation of this use-case led to the following publication :

Paper A : Khaled Sayad, Benoît Lemoine, Anne Barros, Yi-ping Fang, Zhiguo Zeng. (2021). *Dynamic Orchestration of Communication Resources Deployment for Resilient Coordination in Critical Infrastructures Network.* 2055-2062. (10.3850/978-981-18-2016-8_219-cd).

Moreover, we assume that Energy Management System (EMS) applications are hosted as VNFs and depend on the network programmability service to ensure real-time monitoring and control of the power distribution network via distributed power substations. To gain insights into the potential consequences of service disruptions in one domain affecting interconnected services in another domain, we undertake a Failure Modes and Effects Analysis (FMEA) analysis. In this analysis, we delineate the pivotal subsystems within ICT and SPG, wherein unreliable operations can trigger the propagation of failures across domains. The outcomes of this analysis led to the publication of the following research paper :

Paper B : Khaled Sayad, Benoît Lemoine, Anne Barros, Yi-ping Fang, Zhiguo Zeng. (2023). *Towards Cross-Domain Resilience in Interdependent Power and ICT Infrastructures : A Failure Modes and Effects Analysis of an SDN-enabled Smart Power Grid* .

In Chapter 3, we build a cross-domain availability evaluation procedure to quantify the impact of different protection mechanisms at the DC level on critical services availability. We start by presenting the architecture of an SDN-enabled Smart Power Grid which incorporates interdependent ICT and EPI services at the DCs level. We assume that network programmability is key to ensuring real-time monitoring and control of the power distribution network. Also, this feature is provided as a service by the ICT operator via an SDN controller (SDN-C) hosted as a VNF following European Telecommunication and Standarization Institute (ETSI) specifications [29].

Based on the defined architecture, we are able to capture complex interactions between the subsystems in the ICT and EPI domains through a Stochastic Activity Networks (SANs) modeling. Then, an availability evaluation is conducted to study the sensitivity of the service-oriented availability measure with respect to each subsystem's reliability parameters (Mean Time To Failure (MTTF) and Mean Time To Repair (MTTR) for example), and cross-domain protection strategies. This work led to the publication of the following paper :

Paper C : *Khaled Sayad, Benoît Lemoine, Anne Barros, Yiping Fang, Zhiguo Zeng.Availability Modeling and Analysis of Cloud-native, Interdependent Cyber-Physical Systems : Application to SDN-enabled Smart Power Grids.*

In Chapter 4, we study the problem of optimal resource orchestration in

virtualized DCs networks underlying the SDN-enabled SPG with the objective to ensure high service availability while managing resources, availability, and cost constraints. In our scenario, dynamic virtual resource orchestration is a tool to mitigate cross-domain failure propagation, by dynamically updating the redundancy scheme of critical services hosted in DCs with high risk of power outage. This approach takes advantage of the flexibility and automation brought by the NFV to service management, allowing to design a backup strategy to optimally withstand failure propagation in virtualized environments.

As opposed to existing research targeting failure propagation modeling in SPG networks, which focus on power domain attributes [30, 31], we study the equivalent problem by considering the communication resources control via the formulation of a Mixed Integer Linear Program (MILP) model. This work led to the publication of the following paper :

Paper D : Khaled Sayad, Anne Barros, Yiping Fang, Zhiguo Zeng, Benoît Lemoine. *Interdependency-Aware Resource Allocation for High Availability of 5G-enabled Critical Infrastructures Services*. 32nd European Safety and Reliability Conference (ESREL 2022), Aug 2022, Dublin, Ireland. (10.3850/978-981-18-5183-4_S28-03-640-cd).

Also, the process of ensuring dynamic redundancy of virtualized services spanning interdependent ICT and EPI infrastructures, taking into account power supply conditions, resulted in the creation of the following patent :

Patent 1 : Khaled Sayad, Benoît Lemoine. (2022). Procédé de gestion d'une architecture distribuée de centres de données, dispositif et programme d'ordinateur correspondants. France, N° de brevet : 202736FR01. (hal-03896719)

In Chapter 5, we tackle the problem of trustful resource orchestration by proposing a resource and information-sharing platform based on the convergence of Intent-based Networking (IBN) and the International Data Space (IDS) architecture. That is, sharing virtual resources among ICT and EPI operators requires respect for privacy, trust, security, and sovereignty constraints due to the criticality of shared services. In addition, effective orchestration requires the sharing of critical data about service and network state in order to ensure cross-domain life-cycle management. In the literature, a similar problem is encountered when studying Radio Access Network (RAN) sharing between several ICT operators which requires sensitive data exchanges.

To overcome this challenge, Distributed Ledger Technology (DLT) was proposed to incorporate trust into data exchanges [32, 33]. In our work, we propose a hybrid framework composed of a *Centralized Resilience Orchestrator*

for network observability and proactive resource orchestration and a peer-to-peer mechanism that enables two DCs Management and Orchestration (MANO) modules to share the required data to instantiate critical services VNFs and ensure dynamic protection scheme. This work led to the publication of the following paper :

Paper ?? : K. Sayad and B. Lemoine, "Towards Cross-domain Resilience in SDN-enabled Smart Power Grids : Enabling Information Sharing through Dataspaces," 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Berlin, Germany, 2023, pp. 1-6, doi : 10.1109/COINS57856.2023.10189319.

Overall, the aforementioned thesis organization is summarized in Figure 1.2 which illustrates the order by which the formulated research questions are tackled and in which chapter, alongside the associated contribution.

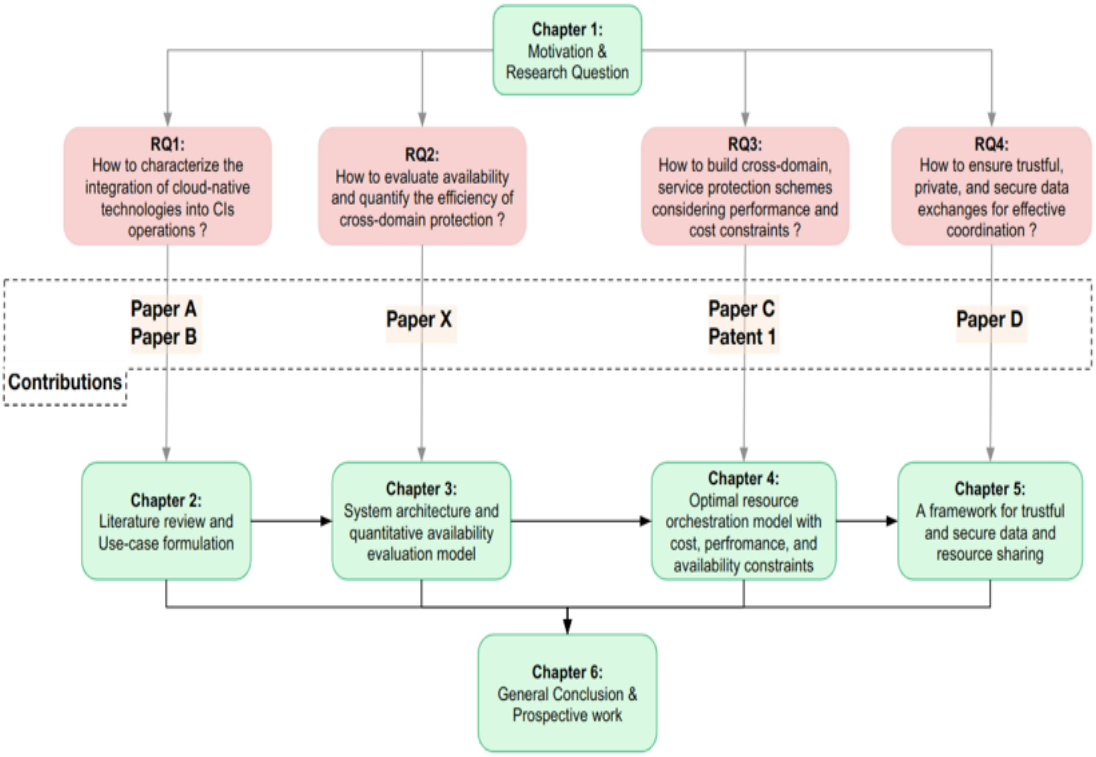


Figure 1.2 – Thesis organization.

2 - Cloud-native management of Critical Infrastructures Services

In this chapter, we present the use case through which we will study the problem of coordinated resilience between ICT and EPI operators. First, we provide an overview of the *Telco Cloud* concepts and the main paradigms fueling the cloud-native migration, namely, NFV and SDN. Then, we represent DPaaS as an example of services enabled by the aforementioned concepts, allowing the ICT operator to enhance the Quality of Service (QoS) and respond to high-demanding use-cases in terms of latency and connectivity. One particular use-case is the support of the monitoring and control of power distribution network. In this context, we provide and overview of the SPG, its architecture, and how the NFV and SDN-based telecommunication services are well suited to enhance the quality of control. To study this use-case, we present the architecture of SDN-enabled Smart Grid (SDN-SPG) and perform a FMEA applied to specific subsystems of this system based on their involvement in cross-domain failure propagation. The objective of this analysis is to qualify the impact failure manifestation and propagation on critical services availability, and hence, provide directives to design sophisticated cross-domain protection mechanisms.

2.1 . Overview of *Telco cloud*

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as : *"pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g.,networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [34]. This definition covers the concept of location-independent service provisioning in which cloud users can access services in different geographical locations without experiencing QoS fluctuations. Also, this concept comprehends the notion of *elasticity* which means that computing, networking, and storage resources can scale to meet demand fluctuations. Moreover, the multi-tenancy concept of cloud computing implies that different users can use the same physical infrastructure at the same time thanks to sophisticated logical and security tenancy management tools. We enumerate three main cloud service provisioning schemes compared to an on-premise service provisioning as illustrated in Figure 2.1 :

- **Infrastructure as a Service (IaaS) :** In this scheme, the cloud service provider offers computing, storage, networking services, and a virtualization infrastructure so that the user can run its operating system, runtime, and applications. In addition, the user is given an access to use as resources as needed to run its applications on a pay-as-you-go fashion.

- **Platform as a Service (PaaS) :** In this scheme, cloud service provider manages the hardware as well as the software resources (operating system, virtualization layer, and the runtime), and let the user to develop its applications software and manages the generated application data, using a predefined development stack.

- **Software as a Service (SaaS) :** In this scheme, the cloud provider offers an application that is accessible by the users via a specific interface (web browser for example). The users only pay for the application usage and don't contribute to service development, deployment, and maintenance.

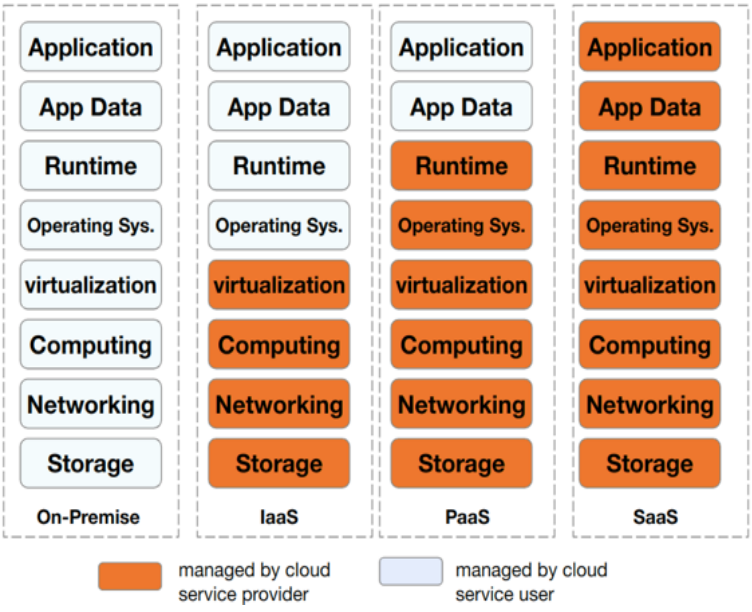


Figure 2.1 – Different cloud service provisioning schemes.

For ICT operators, the need for a distributed architecture is urgent in order to deal with the increasing mobile traffic resulting from the growing number of connected devices and bandwidth-intensive services. Considering that cloud computing gains its efficiency from the distributed nature of service delivery (the reliance on distributed DCs networks), it is possible to extend the

computing and storage services to support also mobile telecommunication services [35]. In this context, the *Telco Cloud* concept is being adopted by major ICT operators to migrate their legacy services to the cloud-native environment in order to reduce costs and enhance the QoS.

By means of virtualization technology, modern mobile telecommunication applications like the 5G Core (5GC) and 5G Radio Access Network. (5G-RAN) can be virtualized and deployed as a service in a cloud-native style. To achieve that, a *Telco Cloud* architecture was proposed by [35] which is divided into five layers encompassing the different stockholders involved in the *Telco Cloud* as depicted in Figure 2.2. The five layers are defined as follows :

- **Physical infrastructure :** in this layer, we find the *public network infrastructure provider* which connects the physical resources in DCs to the public internet. These DCs are managed by a *DC infrastructure provider* which manages also hardware installation and power supply. Finally, interconnecting servers inside and between DCs is ensured by a *private network infrastructure provider*.

- **Virtual infrastructure :** in this layer, a *cloud infrastructure provider* is responsible of providing the virtualization technologies which abstracts physical resources to run services and applications. In addition, a *cloud service provider* delivers a set of functionalities to enable geo-redundancy of applications and load balancing between different DCs.

- **Carrier cloud service platform :** in this layer, VNFs of telecommunication services (5G-RAN, virtualized 5GC) are provided as a service for requesting applications.

- **Service providers layer :** in this layer, a service provider may utilize the platforms provided in the previous layer in order to deliver different services. For example, 5G-RAN cloud platform can be utilized to provide wireless communication service to targeted users. Note that, the network management can be done by the mobile network operator (on premise), or can be provided as a service by the *Carrier cloud service platform*.

- **User layer :** in this layer, potential users of the virtual network are presented by means of the different emerging use-cases scenarios of the *Telco Cloud*.

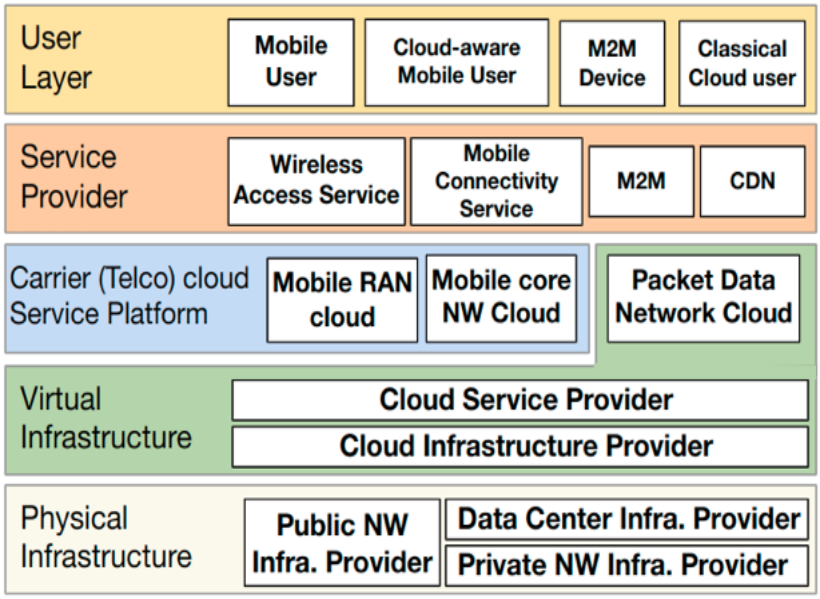


Figure 2.2 – *Telco Cloud* architecture as proposed by [35] .

Note that, an ICT operator can play the role of all the stakeholders involved in the previous architecture. For example, by installing its own DCs network, developing the associated virtualization layer and developing VNFs for core network applications. However,in the current ecosystem of *Telco Cloud*, VNFs vendors, physical platforms providers, and RAN solutions are developed by different actors. In what follows, we will explain the NFV, SDN, and edge computing concepts as key catalysts for the *Telco Cloud*.

2.1.1 . Network Function Virtualization

NFV is a concept which involves the use of virtualization technologies to deploy and run network applications software on standard hardware to enable on-demand Network Service (NS) provisioning. That is, this concept aims to decouple the network functions (firewalls, load balancers, core and access network applications..) software from the hardware on which it runs as opposed to traditional network management where the network functions software are tied with dedicated hardware [36].

In addition to cost related benefits of NFV resulted from optimized and flexible resource usage in virtualized environments, the wide range of possible VNFs deployments on a multitude of hardware leads to a reduced vendor lock-in problem. That is, an ICT operator can compose a networking service by choosing VNFs from different vendors to run on Commercial Off-The-Shelf (COTS) hardware. In this context, standardization efforts play a major role in ensuring interoperability between different actors (hardware providers, ICT

operators, and VNFs vendors) [36].

The architectural framework being developed by ETSI Industry Specification Group (ISG) aims to foster innovation and interoperability by introducing normative specifications allowing to run cloud-native ICT services in multi-vendor environments [37]. In addition to legacy Operation Support System (OSS) and Element Management (EM), the architectural framework introduces another set of management applications embedded into the MANO as depicted in the architecture in Figure 2.3. In this architecture, the Network Function Virtualization Infrastructure (NFVI) encompasses the physical resources (computing, networking, and storage hardware) on which the VNFs are instantiated, and the virtualization layer which abstracts and allocates specific physical resources to each VNF. NFVI is managed by the Virtualization Infrastructure Manager (VIM) which is part of the NFV-MANO and responsible of controlling physical resources usage via the *Nf-Vi* reference point.

The Network Function Virtualization Orchestrator (NFVO) fulfills the resource orchestration function via the *Or-Vi* reference point, by distributing and managing NFVI resources among several VIMs. In addition, it fulfills the network service orchestration function by managing the lifecycle of NSs. Also, it manages the lifecycle of VNFs (onboarding, scaling, healing, and termination) through the VNF Manager (VNFM) via the *Or-Vnfm* reference point.

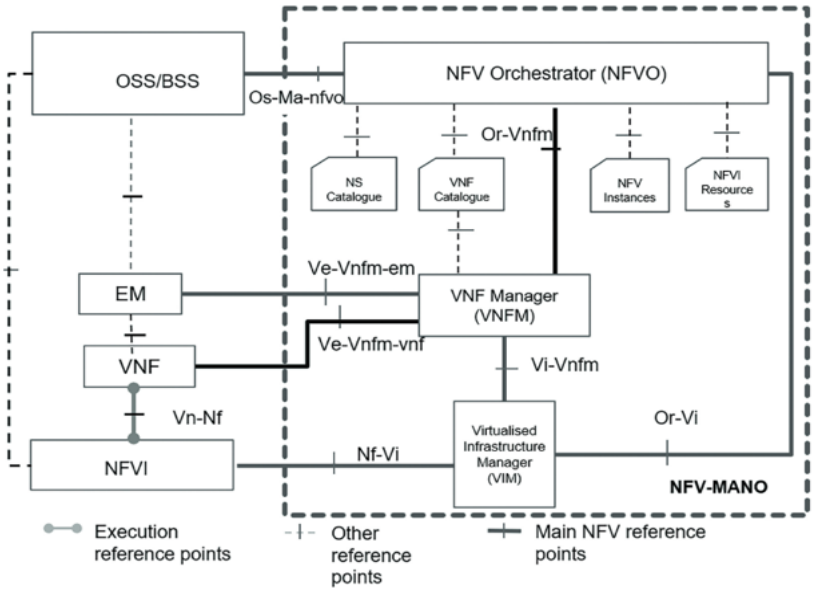


Figure 2.3 – ETSI NFV Architectural Framework (taken from [36]).

2.1.2 . Software Defined Networking

SDN is a paradigm where, in a networking device whose main function is to forward a received data packets to a specific destination, the forwarding logic (decide the optimal route) and actions (packet coding and forwarding) are separated and performed at different planes called the control and data plane. Hence, network programmability is enabled through controller software applications in the control plane, and a data plane composed of general purpose, programmable hardware [38]. The programmability feature serves as a tool to optimize traffic management by adapting routing logic to specific applications' requirements. Also, SDN enables to avoid vendor lock-in as it relies on open standards , and leads to reduced network management cost because of the centralized control of data plane components which allows to have better observability and monitoring of forwarding devices and thus, helps to optimize their energy consumption, dimensioning, and operation.

From the SDN architecture of Figure 2.4, the control plane is composed of an SDN-C whose main function is to orchestrate resources and control data routing by imposing the rules (for example security and access control functions and congestion control policies) to data plane devices via the southbound interface. An examples of existing implementations of SDN-C are OpenDayLight [39], ONOS [40], and other solutions provided by vendors. A comparative study of open source SDN-C implementation is presented in [41] where a performance evaluation study is conducted considering different metrics. Finally, The northbound interface in Figure 2.4 connects the SDN-C to application plane. In this latter plane, different applications expose their data routing and manipulation objectives which are translated into policies by the SDN-C.

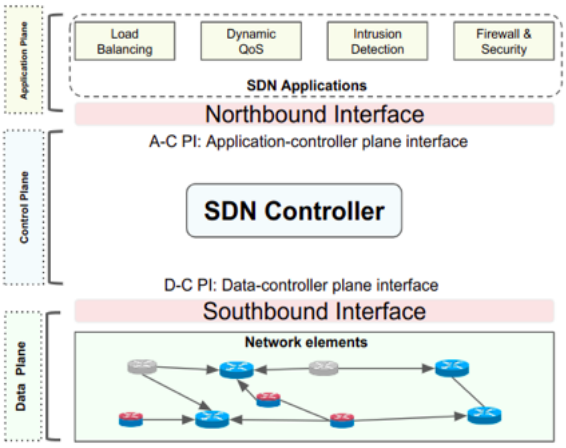


Figure 2.4 – Software Defined Networking Architecture Components.

The mapping of SDN architecture components into the ETSI NFV-MANO architecture of Figure 2.3 has been conducted in [38]. This combines the benefits of NFV in terms of flexible resource usage, and the decoupling of control and data plane as a core principle of SDN. Hence, offering a wide range of opportunities for an ICT operator in optimizing telecommunication services delivery. In Figure 2.5, we present the possible mappings of SDN components to the ETSI NFV architecture. Our assumptions in terms of SDN components mappings are encircles in red and will be used to define our use-case in section 2.3.

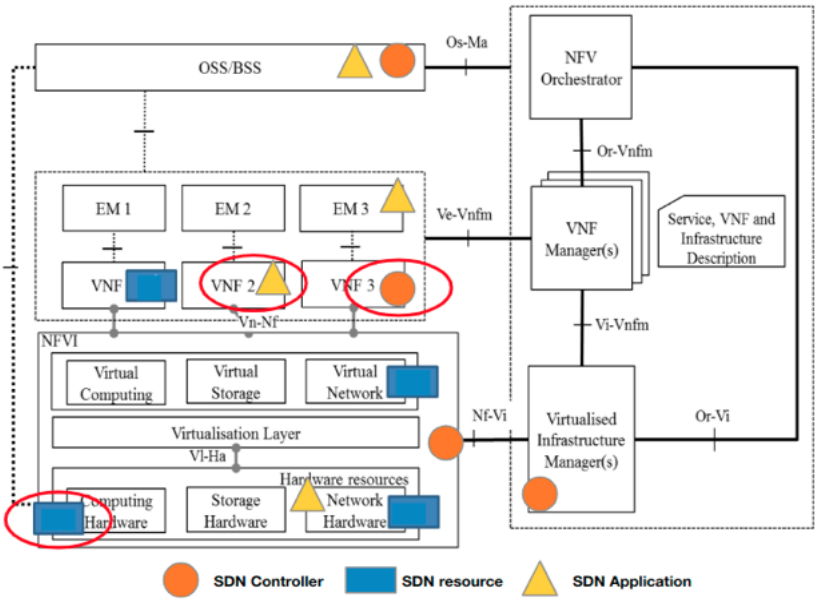


Figure 2.5 – Possible mappings of SDN components to ETSI NFV architecture (taken from [38]).

2.1.3 . DPaaS : Data Plane as a Service

As an example of a cloud-native telecommunication service, we will study DPaaS is a networking model which provides data plane capabilities (data forwarding, inspecting, processing...) as a service in pay-per-use pricing model. In this model an ICT operator deploys the VNFs composing the SDN-C which interfaces with SDN application VNFs that can be hosted in client DCs, and which exposes dynamic QoS requirements that could be translated into data flow control policies.

In Figure 2.6, we show an illustration of the Dynamic Optimization of Packet Flow Routing (DOPFR) as defined by ETSI as an network programmability

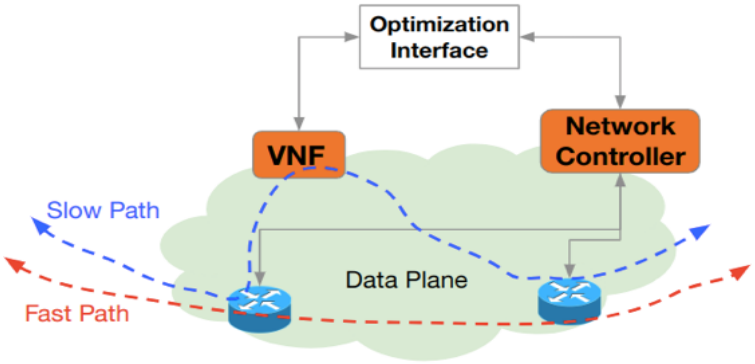


Figure 2.6 – Illustration of Dynamic Optimization of Packet Flow Routing (adapted from [42]).

acceleration use-case [42, 43]. In this scenario, data packet processing functions can be offloaded from a VNF to the network element in order to reduce travel time-by switching from the slow path (in blue) to the fast path (in red). This is noteworthy in scenarios where the network plays a crucial role in supporting applications with low-latency requirements, such as power distribution monitoring and control in SPGs.

In the cloud-native era, as ICT operators seek innovative ways to extract value from their networks, and considering the challenges that EPI operators face in upgrading their networking infrastructure, DPaaS emerges as a compelling service that ICT operators could potentially tailor to the needs of EPI operators in the context of efficient monitoring and control of power substations. An example of a possible data plane service is on-demand, real-time, and resilient routing of SPG monitoring and control data flows between control centers and power substations in the distribution network.

2.2 . Overview of Smart Power Grid

A Smart grid can be defined as *" an advanced digital two-way power flow system capable of self-healing, and adaptive, resilient, and sustainable, with foresight for prediction under different uncertainties. It is equipped for interoperability with present and future standards of components, devices, and systems that are cyber-secured against malicious attacks."* [44]. From this definition, we can extract key features of a SPG, among which, self-healing capabilities against disruptions, the reliance on continuous network state data measurements to dynamically compute control strategies, the support of bi-directional power flow, and the interoperability with a wide range of standards, devices, and systems ensuring flexibility and the support of different use-cases.

2.2.1 . Migrating Energy Management Systems to the cloud

The high penetration of renewable energies in modern power grids is one of the main factors that influences the transition towards a smarter management of the power assets. Renewable energy (wind and solar) generation is inherently intermittent and requires real-time, advanced monitoring and control strategies to deal with the associated stochasticity [45]. In addition, the geographical expansion of Distributed Energy Resources (DERs) brings some overhead into their integration to the grid. This latter point is important in the framework of this thesis work as it constitutes one of the key drivers to study the coordinated expansion of ICT and EPI DCs network to support their new services respectively.

Energy management systems can be implemented based on Supervisory Control and Data Acquisitiony (SCADA) systems which are widely used to fulfill robust control and monitoring requirements of large-scale, mission-critical systems. The main functionalities of a SCADA system are data retrieval from remote sites and enabling control of actuators at those remote sites. An EMS uses the data collected by the SCADA to compute real-time control and archive this data or future analysis. A generalized architecture of a SCADA system based on IEEE Standard for SCADA and Automation Systems [46], is represented in Figure 2.7.

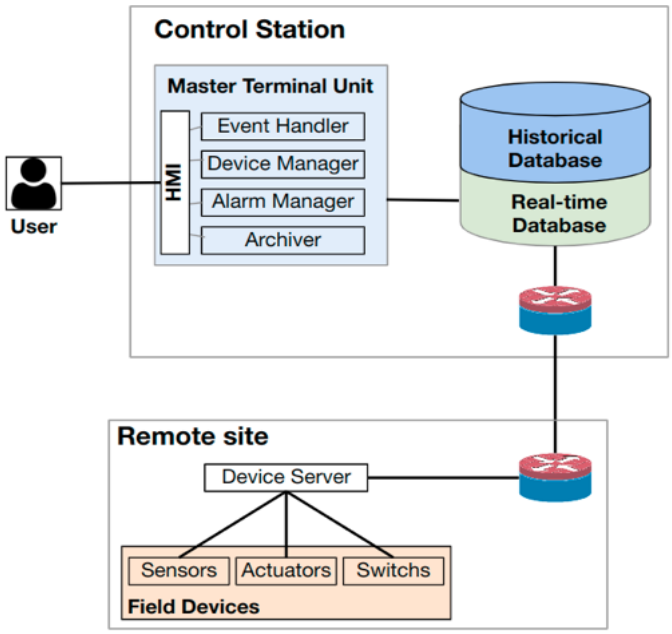


Figure 2.7 – Generalized SCADA Architecture.

The system is segregated into two main components : a control station, which includes a *Control Server* interfacing with the human user, and a remote station which includes the field devices (sensors, relays, and actuators) connected to a *Device Server*. The data generated by the field devices is transmitted to a control station database to be processed by the different components of the *Control Server* : an *Event Handler* which reacts to changes in real-time data values (exceeding a boundary for example), a *Device Manager* which changes the state of the field devices (apply a control on actuators/switches), and an *Alarm Manager* whose main purpose is to allow human user to setup the monitoring rules and manages notifications.

Nonetheless, the substantial volume of data generated due to the proliferation of distributed energy resources and the challenges posed by bi-directional power flow necessitate the enhancement of current SCADA systems to enable the real-time and efficient management of this extensive data. In pursuit of this goal, the cloud computing paradigm emerges as a solution for upgrading existing SCADA-based EMSs. In Table 2.1, we summarize the requirements of SCADA-based critical systems, and how to fulfill them via the cloud-native solutions. First, the high security requirements associated with the processing of sensitive data can be met by adopting a private cloud solution. In addition, thanks to the separation between the control plane and data plane, SDN enables the protection of data by easily adopting new security protocol [47]. Also, the flexibility of managing virtualized services in geo-distributed locations is key to achieve high availability. Moreover, the real-time communication requirements can be met by means of SDN paradigm

SCADA Requirements	**Cloud computing solution**
High security requirements	Private IaaS, SDN-based data encryption and protection.
High availability	Geo-redundancy concepts (availability zones), Dynamic scaling.
Real time communication	SDN-based data routing with dynamic QoS policies.
Ease of use	Automation and zero-touch service management, simplified application update/upgrade.

Table 2.1 – SCADA Requirements and correspondent cloud-based solutions (adapted from [48]).

which is well suited for ensuring data flows in latency sensitive scenarios [48]. Finally, the ease of use requirements concern the life-cycle management of the software applications in cloud-native environments, which, unlike applications built on proprietary hardware, can be automated which reduces human intervention and probability of faulty manipulations.

The development of cloud-based SCADA systems can take one of two approaches [49] : either constructing all SCADA components and features in a cloud-native manner from scratch, or migrating selected functionalities to the cloud and overseeing them in an *as-a-service* fashion. The convergence of SCADA and cloud-native technologies can yield advantages for the EPI operator by enhancing its capability to incorporate new latency-sensitive applications. In addition, this represents an opportunity for SCADA system providers to embrace innovative business models.

Several works in the literature have studied the opportunities in migrating SCADA systems to the cloud. In [50], authors studies the opportunities in terms of cost reduction, increased availability, and flexible and dynamic redundancy that could be brought by provisioning SCADA services in an IaaS cloud. The authors provide the steps to ensure the migration of SCADA services to the cloud. Then, using open-source EclipseSCADA platform, a proof-of-concept is presented along recommendations to enhance he adoption of a cloud-based SCADA functionalities. In [51], authors tackle the problem of interoperability of micro-grid platforms in modern smart power grids. This problem is characterized by the lack of common information models and communication protocols that might foster collaboration between independent micro grids operators. In this approach, critical functions are run on-site to eliminate the security overhead, and shared applications data is transferred to a remote SCADA implemented as a PaaS-based servers where interoperability is guaranteed, allowing participants to access data of their pairs.

In [52], Coordinated Voltage Control (CVC) is implemented via SCADA-as-a-Service approach which provided an interoperability framework allowing the better coordination between micro-grid operators. In [53], a series of experimental setups are conducted to evaluate cloud-based SCADA solutions under different scenarios. The authors propose four implementation scenarios (plan, centralized, distributed, and hierarchical) in addition to a reference architecture. The evaluation of the performance of different implementations demonstrated the feasibility of cloud-based SCADA implementation with three main factors that could impact the performance : virtualization, networking with cloud DCs, and additional security measures.

2.2.2 . Architecture and Standards

A multi-layer architecture of the SPG is presented in [54] and illustrated in Figure 2.8. In this architecture, a Wide Area Network (WAN) is implemented using cellular or optical fiber technologies to support operations in the generation and transmission portions of the SPG. Whereas, a Neighborhood Area Network (NAN) or a Field Area Network (FAN) are implemented to support operations in the power distribution network, mainly the monitoring and control of power substations. In this context, the *IEC 61850* standard provides directives for the design of interface between utility control centers and power substation to enable interoperable monitoring, control, and automation [55].

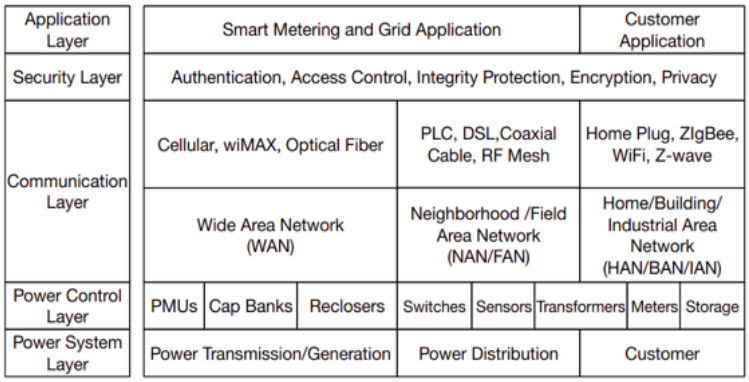


Figure 2.8 – Multi-layer Architecture of Smart Power Grid (adapted from [42]).

An architecture of a digital power substation as conceptualized by *IEC 61850*, defines three level of interfaces as illustrated in Figure 2.9. First, in the process level we identify the communication interfaces for circuit breaker control, and monitoring through sensor data collection using Merging Units (MUs). Secondly, the bay level compromises communication systems supporting the aggregation and coordinated control of multiple circuit breakers or Intelligent Electronic Device (IED)s associated with a specific area. Finally, the station level comprehends the control of the entire power substation enabled via interfaces with the control center and the local SCADA system.

In our work, we focus on the communication interfaces between the control center and the controlled power substations. A detailed view of the topology of this interface is depicted in Figure 2.10 adapted from the topology in [56]. In this topology, the utility control center hosts an EMS which monitors and controls one or many substations in order to load balance power distribution. A substation hosts power relays to control power flows in the distribution network, and a relay controller and a remote terminal unit for monitoring

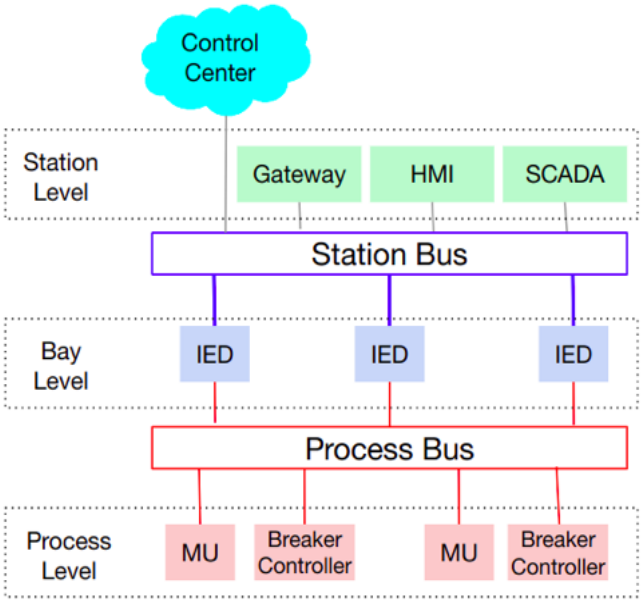


Figure 2.9 – A conceptual architecture of Communication levels in a Power Substation as defined by *IEC-61850* .

and control. Note that, we distinguish between global control applied by the utility control center as a response to high power demand fluctuations, and local control computed at the substation level to deal with local and low disturbances.

As mentioned previously, we articulate our study around the possible evolution of the communication interface between the utility control center (respectively, the EMS), and the power substation by relying on a programmable network managed as a service by the ICT operator (the aforementioned DPaaS) to support the reliable, and dynamic routing of monitoring and control data between the EMS and the controlled power substations. In the following subsection, we furnish an overview of resilience assessment within an SPG . We also reference various control strategies tailored to diverse network conditions and emphasize the importance of depending on a robust communication network.

2.2.3 . Resilience assessment and Control of Smart Power Grid

Numerous studies in the literature have addressed the issue of evaluating the resilience of a SPG due to its critical role in developing efficient restoration and recovery strategies [57, 58]. In [59], power generation and transmission security is viewed as an application of a series of continuous control actions in order to maintain the desired level of operation. The operational

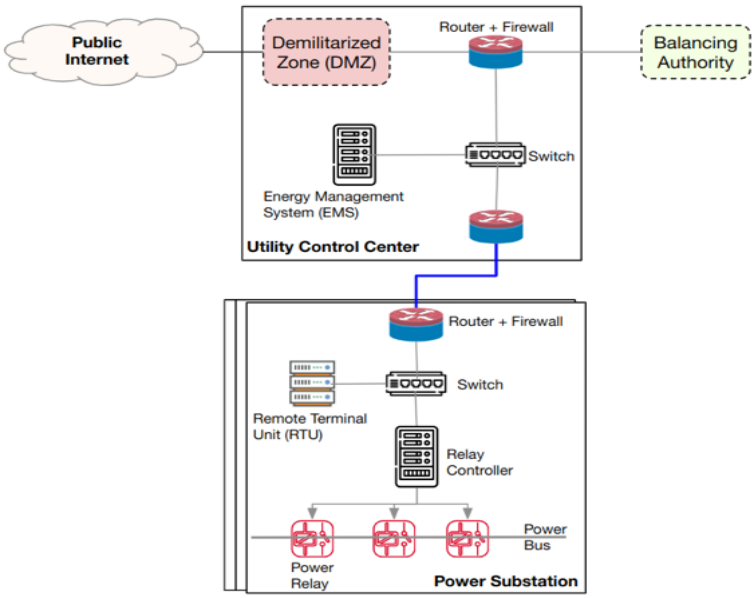


Figure 2.10 – A conceptual topology of utility control center, and power substations (adapted from [48]) .

state changes wether because of a maintenance intervention, load fluctuations or simply a disruption. Accordingly, possible control actions range from the activation of available units to replace deteriorated ones, generation rescheduling, or load balancing. Three operational states are defined : *preventive, emergency, and restorative*, and presented via the state diagram of in Figure 2.11 where :

- **Normal or Preventive state** : which refers to a situation where all loads demands are satisfied at the desired operating voltage and standard frequency. The control objective in this situation is to maintain the same level of operation with minimum cost.

- **Emergency state** : this state refers to a situation where some operation limits are violated. The control objective in this scenario is to relieve the system overhead and maximize demand satisfaction.

- **Restorative state** : this state refers to a situation where the service experiences an outage following an emergency. The control objective in this case is to increase demand satisfaction and decrease the recovery time.

In the power distribution network, authors in [60] propose a MILP to optimize service restoration in smart grids via the placement of protection re-

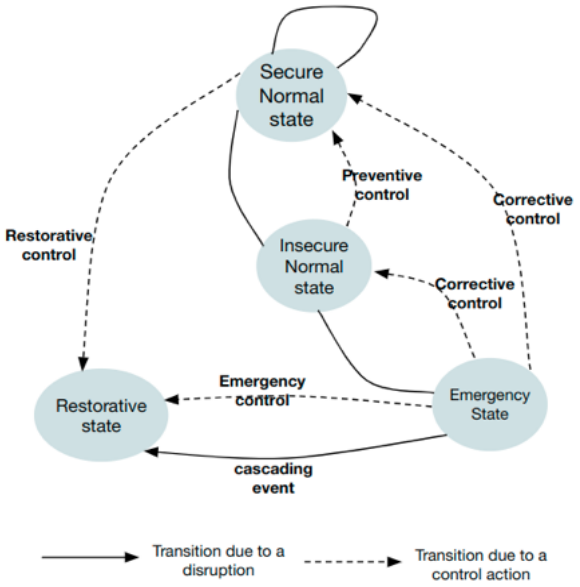


Figure 2.11 – Operation State Diagram of a Power grid (adapted from [46]).

source while considering different scenarios of telecommunication services availability. Interdependencies between the two domains are captured by considering that ICT components as loads and EPI substations as client in the ICT domain. However, the level of abstraction of the ICT components doesn't provide details into how failures manifest in the ICT domain and wether protection mechanisms are needed in parallel to the power domain ones. That is, understanding how operators respond to propagated failures is crucial to adopt an optimal coordinated protection action that could benefit both operators.

Reliable restoration and recovery depends on reliable control, which also depends on reliable underlying ICT infrastructure. That is, computing the adequate control strategy and the reliable application of this control are two separate problems. Given that the control strategy can be seen as a sequence of data to be transmitted from the control center to the system under control, the latter problem deals with the challenges in ensuring a safe and reliable transmission by ensuring the availability of network elements : data plane as well as the availability of the control plane in the context of SDN-enabled data transmission. In Paper C, we provided a literature review covering the topic of failure propagation in interdependent telecommunication-power networks. Some findings suggest that ensuring the power supply, and thus the availability, of some telecommunication nodes connecting the power nodes, is crucial to ensure effective load balancing in the power domain.

In our work, we propose to study this problem from an ICT operator pers-

pective by formulating the problem of resilient orchestration of NFV and SDN resources to ensure high availability of cloud-native services supporting power distribution control applications. To this end, we provide a details architectural view of the main components involved in failure propagation between interdependent ICT and EPI networks. Afterwards, we apply a FMEA to each subsystem to retrieve critical failure modes information which will serve in designing effective cross-domain resilience strategies.

2.3 . Use-case : Ensuring high availability of critical services in SDN-enabled Smart Power grid

In order to illustrate the risk associated with the cloud-native management in telecommunication and power networks on cross-domain failure propagation, and the opportunities in terms of coordinated cross-domain resilience, we develop an architecture of SDN-enabled Smart Power grid to highlight the functional dependencies between specific ICT and EPI services. This architecture allows us to overcome the limitations of existing network models of failure propagation between power and telecommunication networks. These limitations are illustrated by the high level of abstraction of the main subsystems in both domains which restrains our understanding on how failures generate and propagate. Hence, we present an architecture that separates the interactions between different components into three planes : control, data, and power.

Also, we detail how the failure of each subsystem impacts the Service Oriented Availability (SOA) measure. This paves the way to study both : the concern of ICT operators in terms of ensuring reliable power supply of their services, and the concern of EPI operator in terms of reliable telecommunication services to support real-time monitoring and control of the distribution network. These concerns can be tackled by adopting adequate, coordination-based protection mechanisms which will be studied in detail in Chapters 3 and 4.

2.3.1 . system architecture

The system architecture is presented in Figure 2.12 and is taken from Paper C. We assume that real-time control and monitoring of power substations are performed by EMS hosted as virtualized applications (green box) in eDCs (red box) operated by the power network operator. The EMS relies on network programmability to dynamically configure the monitoring and control data flow. This feature is assumed to be delivered as a service by a telecom

network operator which (in the context of SDN), hosts the control plan as a virtualized application in eDCs as well. Due to geographical proximity, the eDCs hosting the control plane depend on the reliable operation of power substations (purple box) to ensure a reliable flow of power for eDCs operations via Uninterruptible Power Supply (UPS) (blue box).

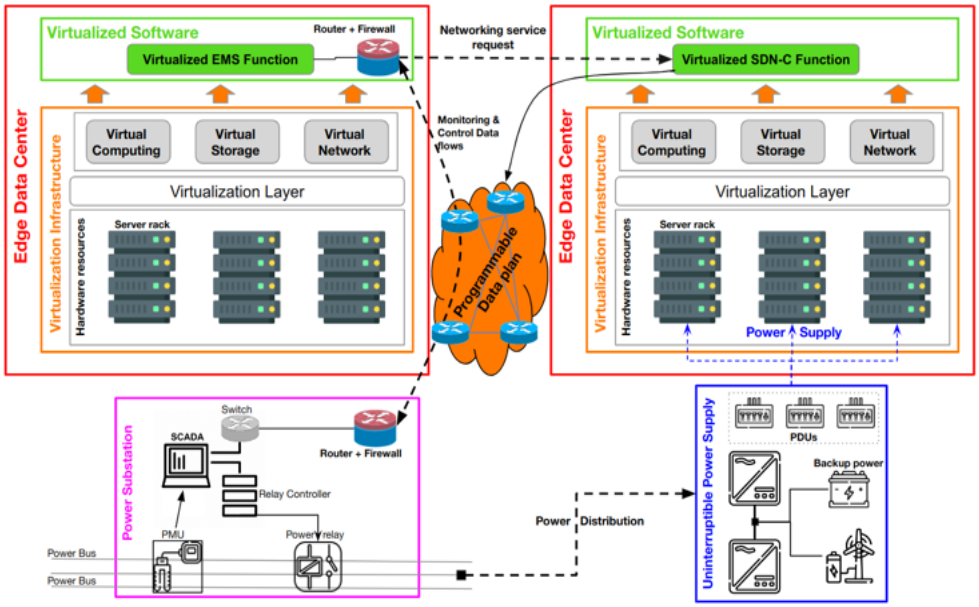


Figure 2.12 – Proposed architecture of an SDN-enabled SPG.

In Figure 2.13, we provide an extended view of the architecture presented in Figure 2.12. The fact that one EMS instance may control several power substations [56], Figure 2.13 offers a network-oriented perspective, elucidating the telecommunication connections linking the SDN-C, the EMS, and the Power Substations. It also highlights the power connections connecting the Power Substations to the DCs hosting the SDN-C. This view will be used to study the impact of topology (different connections between EMS and SDN-C instances density of Power Substations, and the redundancy of DC's power supply) , on services availability. In this network-oriented view of the SDN-SPG, interactions between the components of telecom and power domains are separated into three planes : control, data, and power as follows :

2.3.1.1 Control Plane

In the control plane, we assume that the SDN-C and EMS applications are deployed over a virtualization infrastructure installed in the eDCs following the ETSI-NFV reference architecture. The EMS performs monitoring of the power substations by receiving the monitoring data through the communication

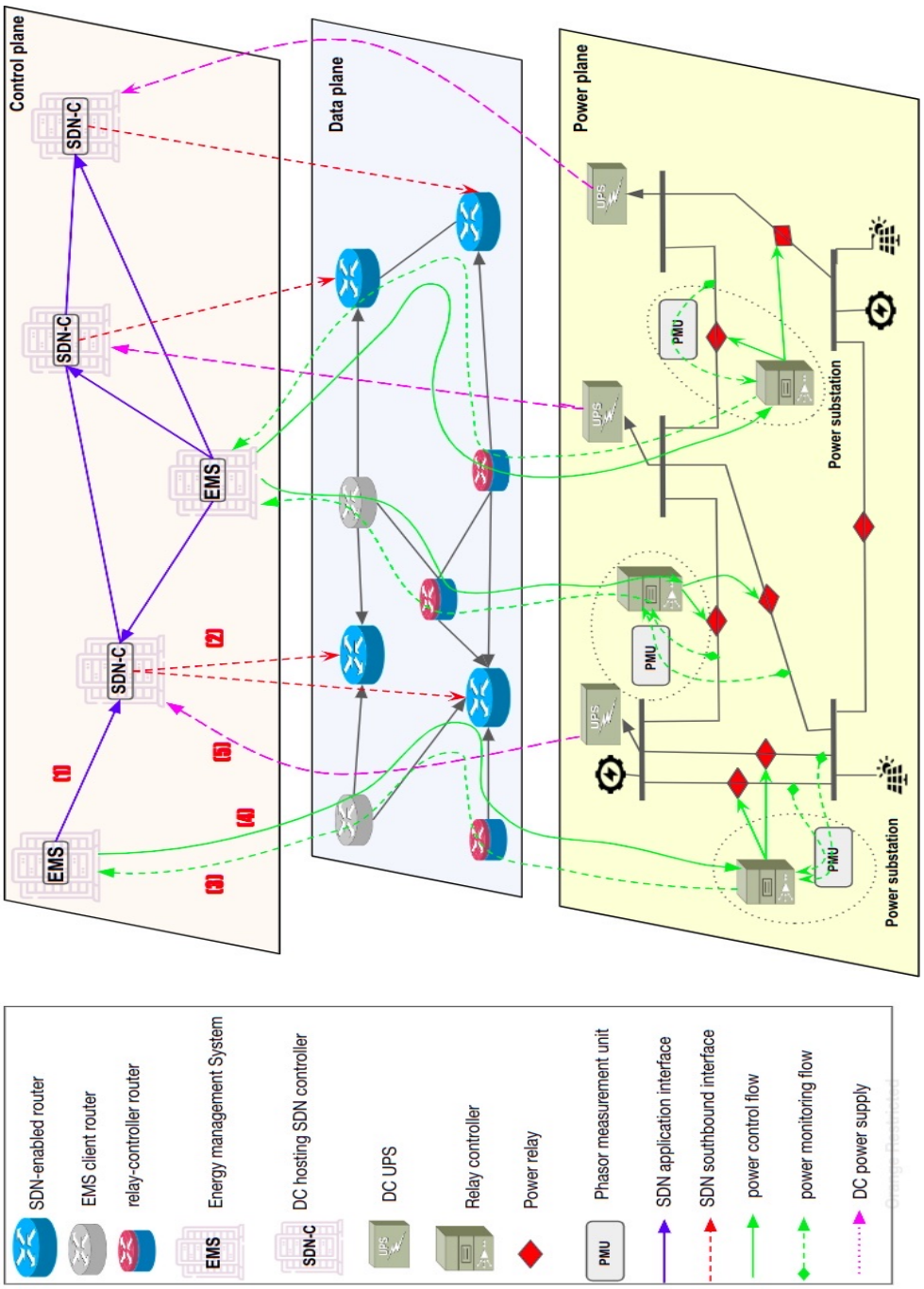


Figure 2.13 – Network-like view of the SDN-enabled SPG.

network (link 3 : *EMS*←*Data Plan*←*Power substation*) and ensures the dynamic and real-time control of the power relays to satisfy power loads demand fluctuations (link 4 : *EMS*→*Data Plan*→*Power substation*). In addition, the EMS interfaces with the SDN-C via the northbound interface. For example, to request the update of data routing paths in the data plane (link 1 : *EMS* →*SDN-C*).

The SDN-C ensures the dynamic control of SDN-enabled routers in the data plane (link 2 : *SDN-C* → *SDN-enabled router*) to meet desired service level agreements (resilience, latency…), exposed via the interface with the EMS (SDN application interface : link 1).

2.3.1.2 Data Plane

In the data plane, we consider SDN-enabled routers connected via a southbound interface with their correspondent SDN-C. These routers apply the control setup imposed by the SDN-C (through link 2) to the data flow. In addition, we consider the routers of EMSs and power substations as part of the data plane. These routers serve as an entry and exit point of all data generated at the EMS or the Power substation. They could also be equipped with security functions like firewalls and intrusion detection systems.

2.3.1.3 Power Plane

In the power plane, we consider power substations composed of :

- Phasor Measurements Units (PMUs) collecting sensor data about the state of the power distribution network.
- Power relays controller (a SCADA system for example) responsible for aggregating sensor data, generating local control, sending monitoring data to the EMS (link 3) and applying the global control imposed by the EMS (link 4).
- Power relays which are devices whose main function is to act as controlled circuit breakers.

In addition, we assume that eDCs power supply (link 5) is ensured by a smart-grid-ready(SG-ready) UPS [61]. That is, unlike tradition UPS systems whose functions are limited to backup batteries management and servers protection against power disturbance, SG-ready UPS are capable of (autonomously) interacting with the power distribution network by : supplying energy in a bi-directional power-flow scheme, and fast frequency response for renewable

energy penetration.

2.4 . Failure Modes and Effects Analysis of the SDN-SPG

FMEA is a systematic methodology deployed to identify and assess failure modes of a system, their causes, and their effects. The objective of such methodology is to enhance the availability and performances. The methodology is outlined in the *IEC-60812* standard [62]. The objective behind the application of FMEA to the SDN-SPG architecture components defined above is to detect component-level failure modes which lead to system-level complex failures, and hence, service interruption.

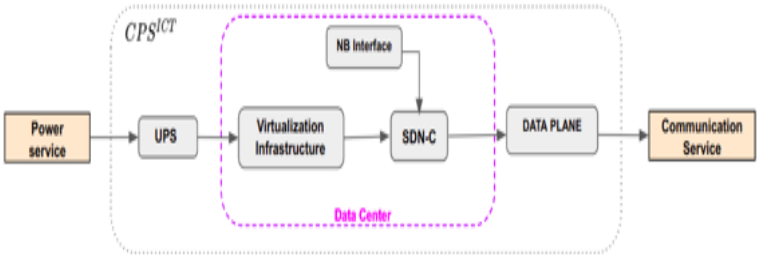
Two services are defined in an SDN-SPG : networking and power distribution control. We use functional block diagrams to represent the contribution of different subsystems of the presented architecture to the delivery of the two services (see Figure 2.14). We define a Cyber-Physical System (CPS) aggregation level to better understand multi-level failure manifestation from component to service level. In Figure 2.14a, a CPS^{ICT} is the system responsible of delivering the communication service. It is a CPS because it is composed of cyber-components (Virtualization infrastructure and SDN-C), and a physical component (UPS). This assumption is motivated by the work in [63] proving the efficiency of CPS modeling in capturing the different complexities of a DC both at the computing and energy levels.

In Figure 2.14b, we assume that the power supply of a DC hosting EMS instance is reliable and thus, it is not represented in the diagram. Also, it is assumed that the southbound interface between the SDN-C and the data plane is reliable, and thus, is not considered as well. Note that, the communication service is primordial input to the PMUs network in order to send sensor data to the EMS. Also, the EMS relies on the communication service to send real-time control to the power relays, which explains the double representation of communication service in Figure 2.14b.

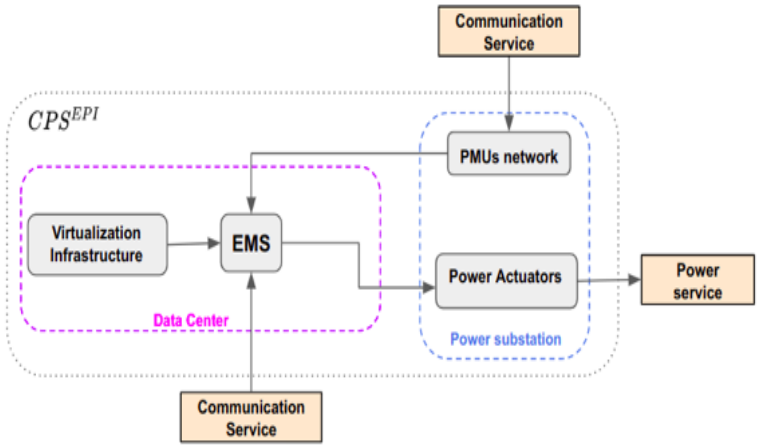
The FMEA is represented in Table 2.2 where we analyze the failure modes of each component, the cause, and effects on the component itself and other subsystems. Starting with the SDN-C, three classes of failure modes were identified on commercial SDN-C solutions and highlighted in [64]. Deterministic software failures emerge from the apparition of a particular sequence of entries leading to a fault activation. Whereas, non-deterministic software failures occur due to the combination of errors and stochastic arrival time making them hard to predict in advance. The last software-like failure modes are related to software ageing which is a subset of the non-deterministic failure

Component	Function	Failure Modes	Failure Cause	Failure Effect
SDN-C	Control the data plane.	1- Inability to handle incoming requests. 2-Inability to reconfigure the data-plane.	1-Failure of the NB interface . 2-Unavailability of the virtualization infrastructure.	1-Reject requests to configure the data plane 2-Non transmission of data from EMS to power substation (control flow) and from power substation to EMS (monitoring flow) .
Data plane	Apply the control plane configuration.	1-Forwarding the data flow to wrong destination 2-Physical equipment (links) deterioration	1-Wrong routing/forwarding rules. 2-Extreme weather conditions.	Communication service interruption
Virtualization Infrastructure	Provide dynamic computing, storage and networking resources to run VNFs.	1-Inability to instantiate VNFs and provide required resources.	1-Abnormal electrical state.	Perturbation of VNFs continuity and availability.
UPS	Provide uninterrupted power supply for physical servers	1-Inability to provide reliable power.	1-Power distribution network failure.	Inability to launch new servers in the DC.
EMS	Control and monitoring of power distribution network.	1-Reconstruct wrong state of the network. 2-Apply outdated control to the power network.	1-Delayed transmission of monitoring data. 2-Latency requirements not satisfied in the data plane.	1-Compute wrong control. 2- Destablization of power distribution network.
PMUs	Collect sensor data of power distribution network state.	1-Sensor fusion failure. 2-Send delayed measurements.	1-Error accumulation in the measurements. 2-Data plane failure.	1-Destabilize the monitoring function of the EMS.
Power actuators	Apply power network stabili--zation control sent by the EMS.	1-Electro-mechanical degradation	1-Heat, oxidation, acidity, and moisture	1-Inability to satisfy power demands in the power distribution network.

Table 2.2 – FMEA of main components involved in SDN-enabled smart power grid network.



(a) Functional Block diagram of a cyber-physical system in the ICTdomain whose main function is to provide communication service.



(b) Functional Block diagram of a cyber-physical system in the EPI domain whose main function is to provide power service. Note that, we assume that the power supply of a DC hosting EMS instances, is reliable and thus, it is not represented in the diagram.

Figure 2.14 – Functional Block Diagrams of systems responsible network and power services delivery.

modes, characterized by performance degradation over time due to various reasons like memory leaks, resource exhaustion, and accumulated complex states with relation to the total time of system operation [65]. Finally, the software failure may be caused by the failure of the underlying computing infrastructure, in our case the virtualization infrastructure encompassing the operating system, hardware, and virtualization manager software. Accordingly, the failure modes of the SDN-C are characterized by its inability to handle upcoming EMS requests and update the Data plane which might be caused by a software failure impacting the SDN-C itself, or the failure of the underlying virtualization infrastructure. Moreover, the Data plane, composed by programmable network elements (switches or routers) exhibits two failure modes : forwarding data to wrong destination, and physical link deterioration. The former failure mode imight be caused by a failed SDN-C generating wrong forwarding rules. Whilst, the latter failure mode might be caused by external, weather conditions.

A virtualized EMS application has two failure modes : a wrong reconstruction of the power network states, and the application of wrong load balancing control. Both of these failure modes are caused by the unreliability of the data transport network leading to delayed transmission of monitoring and control data from/to power substations. Given that a EMS is assumed to be hosted as a virtualized software like the SDN-C, the failure of the underlying virtualization infrastructure might be an external cause of failure. In our case, Virtualization infrastructure aggregates both the hardware (physical servers) and the managing software (VIM). The inability of perform life-cycle management operations (instantiation, update, scaling, and termination) of virtualized application might be caused a software failure or a hardware interruption due an abnormal electrical state. The abnormal power state, for example a faulty management of backup batteries is a failure mode of the UPS which fails to regulates power supply fluctuations due to the abnormal power distribution network.

Based on this analysis, we observe that the availability attribute of any components contributes to the service-oriented availability and might trigger cross-domain failure cascade between the ICT and EPI domains. However, the likelihood of triggering of such events varies depending on the criticality of the component itself to the whole system operation. Hence, a FMECA analysis should be taken by extending the FMEA with criticality study in order to assess the severity of a particular component's failure.

2.5 . Conclusion

In this chapter, we provided an overview on cloud-native technologies integration in modern ICT and EPI infrastructures. Also, we presented the architecture of SDN-enabled Smart Power Grid which highlights the interactions between SDN and NFV-based services which span the telecommunication and power domain. The FMEA study pointed out some directives towards the study of cross-domain, coordinated resilience. One takeaway from the FMEA study concerns the improvements actions to be taken in order to attenuate the effect of component's failure. From a system-level view, component redundancy is essential to increase overall availability and avoid single-point of failure. From an operator-responsibility view, network dimensioning (installed DCs capacity, UPS redundancy, and Power devices redundancy) is a sequential decision process which lies in an operator responsibility and doesn't involve other interdependent operators. The fixed network capacity represents a bottleneck towards adopting a redundancy scheme because of pos-

sible resources shortage. However, due to the standardized and softwarized management nature of SDN-C and EMS services, a redundancy scheme of an SDN-C of the ICT domain could be designed by considering DCs of the EPI domain (and vice-versa for virtualized EMS applications).

Note that, the objective of a coordination-based resilience is to mitigate the failure cascades impacting the defined communication and power control functions which must involve the ICT as well as the EPI operators. This problem can be studied in an optimization framework where the redundancy schemes are dynamically updated to deal with network state fluctuations. Consequently, we focus on dynamic resource orchestration in virtualized DCs spanning the ICT and EPI domains, and hosting EMS and SDN-C services. The study of different coordination patterns will be presented in chapter 3. Whereas, the implementation of such redundancy strategies will be presented in 4.

3 - Cross-domain evaluation of critical services availability

The growing adoption of cloud-native technologies into the control layer of telecommunication and power infrastructures should be accompanied with tools to model and quantify the impact of emergent failure modes on critical services availability. In this section, we assess the availability of interdependent networking and power-distribution services through a conceptual framework of a SDN-enabled Smart Power Grid (SDN-SPG) using a hierarchical modeling approach based on SANs formalism. The core component of this conceptual framework are the virtualized Edge Data Centers (eDCs) hosting critical networking and power control applications, whose dimensionning in the virtualiztion and power domains is crucial to guarantee high availability of hosted services. In this context, the hierarchical model allows us to quantify the impact of different protection strategies in the virtualization domain while considering different scenarios of power-domain interconnections. The proposed conceptual framework allows to capture the impact of inter-domains, cascading failures, and thus, the design of adequate, cross-domain resilience strategies. To this end, we first present the architecture of the SDN-SPG with a focus on the subsystems that contribute to cross-domain failure propagation between the power and telecommunication infrastructures. Then, we introduce the hierarchical model where the lower level is composed of the SAN models of the defined subsystems. These lower level SAN models incorporate internal failure dynamics and the impact of cascading failures as a result of interdependencies with other subsystems. In the upper level of the hierarchical model, we gather lower level models in a network-like structure to study the impact of critical services redundancy schemes on the defined availability measures. Afterward, we conduct a sensitivity analysis to study the impact of changes in the proposed models parameters on the obtained results in the reference setup. We focus our analysis on two particular parameters, the power backup capacity of the virtualized eDCs, and the power control frequency. The obtained results suggest that power domain knowledge might be useful to design more efficient and robust protection of virtualized services. Also, this would help CIs stakeholders, in particular power and ICT operators, to coordinate their efforts in the migration towards cloud-native management and optimize the dimensionning of the underlying eDCs infrastructure.

3.1 . Introduction

Cloud-native concepts like NFV, SDN, and edge computing are being integrated into modern CIs operations in order to enhance the QoS and provide more reliable critical services. For services with strict latency and availability requirements, this implies that the software applications composing the service are deployed as virtualized applications in dedicated eDCs [66].

In the telecommunication industry, we are witnessing the rise of *"Telco-Cloud"* concept where telecommunication services are software-defined. This allows ICT operators to efficiently manage the deployment of their services in resource-constrained environments, and optimally respond to network demand fluctuations. In this context, NFV and SDN paradigms emerge as catalysts for the current transformation of the ICT infrastructure [67]. NFV is a concept where the development phases of network functions software (design, programming, and deployment), are decoupled from the physical, often proprietary, devices on which they run. This would decrease operational expenditure and bring more agility and flexibility into service development and deployment operations [68]. In addition, the SDN paradigm aims to decouple the control (packet forwarding logic) plan and data routing plan. The forwarding rules are software-defined and dynamically interface with commodity hardware allowing network operators to innovate more sophisticated protocols and adapt network behavior to dynamic QoS needs.

Meanwhile, cloud-native technologies are also key enablers for real-time control, power substation automation, and enhanced power-relay protection in SPG networks. That is, the high penetration of renewable energies is pushing EPI operators to innovate new control strategies to deal with bi-directional power flow and dynamic fluctuations [69]. From CIs resilience perspective, the migration towards a softwarized management of critical services has some drawbacks related to the high exposure to cyber-risks and cross-domain failure propagation [66]. This latter issue is illustrated for example by the need of ICT operators to densify their eDCs networks to meet the strict latency requirements of critical applications which would increase the need for a more stable power supply in the power distribution network. Thus, a failure in the power infrastructure may propagate causing service interruptions in the telecommunication domain. On the other side, the failure of telecommunication services may have a considerable impact on the stability of the SPG as studied in [70]. In order to mitigate cross-domain failure propagation, some opportunities in terms of coordination-based protection mechanisms must be established between interdependent ICT and EPI operators at the operational level. The convergence of ICT and EPI infrastructure toward the same operational

technologies [66], offers an opportunity to adopt interoperable cross-domain protection schemes. Some examples of such resilience actions are :

- Sharing failure events data at the eDC level, allowing interdependent operators to enhance preparedness and minimize the impact of propagated failures.

- Coordinating dynamic risk assessment to better estimate failure propagation dynamics.

- Orchestrating multi-domain resources in eDCs operated by interdependent CIs operators.

In order to deal with the aforementioned problems, we define the following research questions :

- ***RQ1*** : How to establish a cross domain dependability evaluation procedure to model the impact of cloud-native technologies integration into interdependent ICT and EPI networks from a risk perspective ?

- ***RQ2*** : How to design coordinated, cross-domain resilience strategies between ICT and EPI domains at the eDCs layer ? and how to quantify the effectiveness of such protection mechanisms ?

In this present work, we tackle ***RQ1*** by designing interdependent state-space models of ICT and power domain subsystems that capture the impact of interdependencies in terms of cascading failure. This represents the lower level of the hierarchical model. In the upper level, we construct a network where the nodes are the subsystems and the links are the different dependencies between them. This will allow us to tackle ***RQ2*** through the study of topology impact on service-oriented availability. The model is based on Stochastic Activity networks (SANs) formalism applied to an SDN-enabled Smart power Grid (SDN-SPG).

As illustrated in Figure 3.1, we assume that real-time control and monitoring of power substations are performed by EMS hosted as virtualized applications (green box) in eDCs (red box) operated by the power network operator. The EMS relies on network programmability to dynamically configure the monitoring and control data flow. This feature is assumed to be delivered as a service by a telecom network operator which (in the context of SDN), hosts the control plan as a virtualized application in eDCs as well. Due to geographical proximity, the eDCs hosting the control plane depend on the reliable opera-

tion of power substations (purple box) to ensure a reliable flow of power for eDCs operations via UPS (blue box).

For the rest of this chapter, we review related work on the dependability evaluation of complex cyber-physical systems of the ICT and EPI domains and explain how our contributions extend existing work on dependability evaluation of interdependent CPSs. Then, we propose an architecture of an SD-SPG where we highlight the critical subsystems to networking and power services dependability. Afterward, we present the modeling approach based on SANs formalism and the sub-models of each critical subsystem. Finally, we conduct simulations to quantify the impact of cross-domain protection mechanisms on Steady State Availability (SSA) measures of critical services.

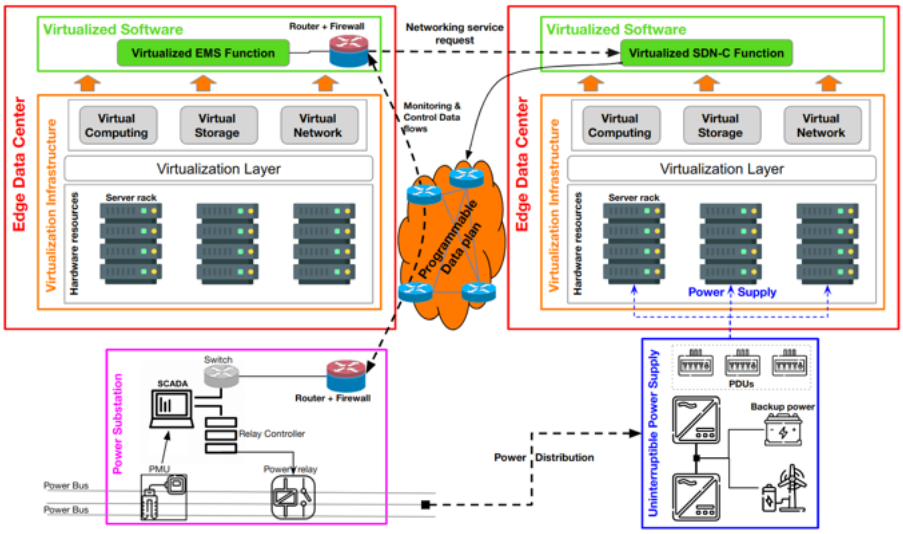


Figure 3.1 – Detailed view of the main components of an SDN-enabled Smart Power Grid and their interactions. EMS and SDN-Controller functions are running in eDCs as virtualized applications (green boxes) on top of a virtualization infrastructure (orange box) aggregating the physical servers and the virtualization infrastructure manager software. Note that, we assume that the eDCs (red boxes) hosting EMS applications are reliably supplied in power and we do not represent their respective UPS systems. The main service of the ICT subsystems is network programmability, i.e : the adaption of data plane forwarding rules w.r.t. client (in our case the EMS) requests.

3.2 . Related Work

CIs resilience has long been an active field of research due to the socio-economic impact of the interruption of such critical services [71, 72, 73]. As an example, the 2003 Italian grid blackout [74], shed light on the impact of

interdependencies and cascading failure phenomenon between the telecommunication and power domains. Consequently, modeling interdependencies and failure propagation dynamics was the first step into the design of efficient mitigation procedures. In [70], authors propose a framework to assess the reliability of power systems with a strong dependence on ICT infrastructure. A detailed analysis is conducted of different impacts of ICT failures on power systems operations including system monitoring interruption, computing incorrect control sequence, and information sharing disruption. Sequential Monte Carlo simulation is conducted to estimate the probability of blackout apparition taking into account both the failures of power and ICT systems. The results show that increasing the reliability of ICT leads to fewer load disconnections in the power domain. Despite the interesting results, realistic data on failure propagation are still needed to validate the results. In [75], authors propose a Mixed Integer Linear Program (MILP) to optimize service restoration in smart grids via the placement of protection resource while considering different scenarios of telecommunication services availability. Interdependencies between the two domains are captured by treating ICT components as loads and EPI substations as client in the ICT domain. However, the level of abstraction of the ICT components doesn't provide details into how failures manifest in the ICT domain and whether protection mechanisms are needed in parallel to the power domain ones. That is, understanding how operators respond to propagated failures is crucial to adopt an optimal coordinated protection action that could benefit both operators. In [76], authors present an interdependent Markov chain approach to model cascading failures between the telecommunication and power domains. This study suffers from the level of abstraction which omits the role of different components in the EPI and ICT infrastructures and doesn't take into consideration their heterogeneity. In [31], authors propose a heterogeneous interdependent networks model in order to study the dynamics of cascading failures between the power grid and the communication network. The proposed model considers different roles of different nodes in both networks when creating the interdependencies links. During a cascading failure event, a node is considered as failed if it doesn't belong the giant connected component of the graph. Dynamic network protection and self-healing mechanisms are not considered in this latter work. In [77], authors investigate the flexibility and automation brought the the SDN paradigm as an enabler for fast recovery of communication network by enhancing the reliability of teleprotection. In [78], authors propose a network coding framework based on p4 language to enhance the resilience of packet forwarding in critical infrastructures network. Other works investigating the integration of SDN-enabled capabilities into the power grid, focus on security assessment and enhance the cyber-resilience against cyber attacks [79, 80, 81].

Considering that the control plan of the SDN is more likely to be hosted as a set of VNF in dedicated eDCs, assessing the reliability and availability of eDCs is crucial to detect design faults, and increase the service (in our case network programmability) availability and reliability attributes [82]. In the context of virtualized eDCs, the dependability evaluation of NFV-based services is studied to enhance the robustness and availability of critical management components of the NFV architecture. That is, reliable power supply is studied due to its criticality in [83] where the authors present a framework called *Flex* which optimizes the DC's power supply to hosted services based on their criticality and tolerance to power outage during power interruption periods. In [84], authors develop a dependability evaluation framework based on SANs to assess the steady state availability of the Management and Orchestration (MANO) and the impact of different failure modes on overall system performance. In [85], a hierarchical modeling approach is proposed to evaluate the reliability and availability of cloud DCs. The hierarchical model is composed of Stochastic Reward Nets to capture the behaviors and dependency of the components in the subsystems in detail. In addition, a fault-tree is constructed to model the architecture of the subsystems, and Reliability graphs are constructed in the top layer to model the system network topology. In [86], a hierarchical model is developed to assess the availability of private cloud storage system using a combination of Continuous-time Markov Chains and Reliability Block Diagrams. In [87], the impact of different backup strategies on NFV infrastructure' availability are studied through SANs to assess the suitability of each backup strategy to different availability modes of the system. In [88], an availability model is developed for DCs network hosting redundant VNF with dynamic migration strategies. The model based on a network evolution approach, is capable of integrating multiple flow characteristics and different redundancy schemes. In [89], Monte Carlo simulations are carried out to estimate the reliability and availability attributes of a data center' UPS. In [90], authors provide an analysis of the dependability of power substation automation system based on *IEC 61850* standard with different redundancy strategies. In [91], a Stochastic Petri Net (SPN) based model is developed to analyze the dependability of control centers network in SPG while considering different backup strategies of critical components. In [92], a vulnerability analysis of the interdependencies between SCADA systems and controlled systems is carried to investigate hidden failure dynamics that could help to better design the interconnection between control centers and power substations in the power grid for example. In our work, we present a SANs model that captures the effects of complex interdependencies between the critical components of an SD-SPG spanning the EPI and ICT domains. A summary of previous works tackeling the problem of dependability evaluation in interdependent ICT and power infrastructres is represented in Table 3.1.

In summary, we reviewed previous research work tackling the problems of interdependencies and failure propagation modeling in interdependent ICT and EPI networks and dependability evaluation of SDN and NFV-enabled critical CPS. First, in terms of capturing the impact of cascading failure, these works present some gaps when modeling the impact on telecommunication services. That is, the service is considered unavailable if the communication node has failed without considering the possibility of self-configuration and self-healing which are key benefits of the migration towards SDN/NFV-based communication service provisioning. Secondly, in terms of dependability modeling of SDN/NFV-based CPS in the ICT and EPI domains, previous works limit their study to the virtualization and computing infrastructure without considering the power supply which is in reality a crucial factor in ensuring high availability in virtualized DCs [83]. This is understandable since the EPI and ICT infrastructures are heterogeneous in nature and operates at different timescales. However, as illustrated in Figure 3.1, assuming that the control function of both domains are provisioned in eDCs using the same virtualization technology, enables to adopt homogeneous, synchronized protection mechanisms at the virtualization level. Also, we propose to study the dependability of a smart-grid-ready(SG-ready) UPS [61] which, unlike tradition UPS systems whose functions are limited to backup batteries management and servers protection against power disturbance, SG-ready UPS are capable of (autonomously) interacting with the power distribution network by : supplying energy in a bidirectional power-flow scheme, and fast frequency response for renewable energy penetration. Our modeling approach uses the *shared place* feature of the *Möbius* tool [93] to implement the interdependency models between different subsystems defined in Figure 3.1 . In addition, the presented models capture the complex behavior of these components both at the power and eDCs levels which helps to design effective protection mechanisms. The contributions of this work are :

- Extending existing work on dependability evaluation of virtualized DCs by considering interactions with power domain subsystems (SG-ready UPSs and Power substations).

- Modeling complex behavior of these subsystems by capturing the cascading failure impact and self-configuration enabled via SDN and NFV technologies.

- Studying of the impact of topology on service-oriented availability of telecommunication and power control services and quantifying of the impact of different protection policies.

Paper	Studied System	Dependability Evaluation	Interdependencies Modeling
[70]	Power system with high reliance on ICT services	Reliability evaluation using Sequential Monte Carlo Simulations	The impact of interdependencies is defined as the delay of power network response due to ICT failure.
[76]	Interdependent ICT and power infrastructures	N/A	Using Interdependent Markov Chain approach to model cascading failures between the ICT and power systems
[94]	Medium-Voltage distribution grid while considering the overlying communication network	Evaluating the robustness of the power network to cascading failures	Capturing th impact of cascading failures by computing predefined structural proprieties of the two networks.
[89]	Data Center Uninterruptible Power Supply System	Reliability evaluation using Monte Carlo Simulation using failure data	N/A
[85]	Tree-based data center networks deploying virtualization technology	Evaluating Availability and Reliability using • stochastic reward nets to capture the behaviors and dependency of the components in the subsystems in detail. • fault-tree to model the architecture of the subsystems; • Reliability graphs in the top layer to model the system network topology.	N/A
[86]	Private cloud storage services	Evaluating Availability using • Continuous Markov chain • Reliability Block Diagram	N/A
[95]	Control centers network of a smart grid while considering different backup strategies of critical components.	Evaluating Availability and reliability using • Stochastic Petri Nets transformed into CTMCs • Time scale decomposition (TSD) method, to reduce the number of states of CTMC	N/A
[96]	Next generation distribution grid : ICT based control system and the power grid.	Evaluating System Average Interruption Duration Index (SAIDI) using Stochastic Activity Networks	Capturing the impact of interdependencies using the *shared place* feature of the *Möbius* tool

Table 3.1 – Literature review on dependability evaluation and interdependencies modeling in interdependent telecommunication and power grid networks.

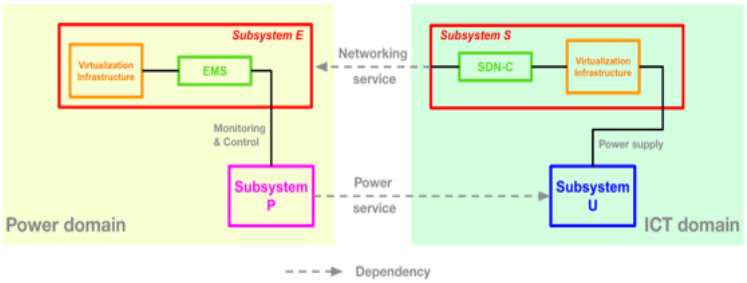


Figure 3.2 – Aggregated view of different subsystems involved in the functional dependencies between the ICT and power domains from the detailed view above. Note that, subsystems *E* and *S* are edge DCs that host different services as VNFs (EMS and SDN-C respectively). Note that, the *Power Service* dependency is defined assuming that the subsystem UPS relies on power lines controlled by the subsystem P and any disruption of the latter leads to cascading impact on the UPS.

3.3 . SDN-enabled Smart Power Grid Architecture

3.3.0.1 *S* subsystem

As illustrated in Figure 3.2, this subsystems relies on the reliable power supply ensured by the ***UPS***, and provides networking service via the programmable data plane. We assume this subsystem has three states :

- *Available* : the networking service can be requested by the dependent *EMS*, and delivered by means of nominal operation of the virtualization infrastructure, the control plane (SDN-C VNF) and the data plane components.

- *Compromised* : this state describes the inability to perform certain operations (auto-scaling) without impacting the service' availability. The switching from the available to compromised state is triggered upon the failure of the ***UPS*** managing the power supply of the eDC. Note that, this impact is not imminent and we still can ensure backup power supply for some servers. However, in case the service requires a scaling (increase servers usage), the operation might fails and the service becomes unavailable.

- *Unavailable* : the service is interrupted (SDN-C unable to handle upcoming requests to update the data plane) because of a software failure of the SDN-C itself or because of the failure of the virtualization infrastructure.

3.3.0.2 *UPS* subsystem

We assume this subsystem has three states :

- *Available* : the ***UPS*** operates in nominal mode and is able to reliably supply power to the virtualization infrastructure.

- *Compromised* : this state describes the inability to perform certain operations (charging backup batteries for example) without impacting the main service.

- *Unavailable* : the ***UPS*** is non operational (interruption of backup batteries charging operation, wrong handling of power fluctuations..) leading to eDC shut down.

3.3.0.3 *E* subsystem

This subsystems relies on the ***S*** subsystem to ensure reliable networking service to perform real-time monitoring and control of power substations. We assume this subsystem has three main states :

- *Available* : the service (monitoring and control of power substations) is performed as expected by means of nominal operation of the virtualization infrastructure and the EMS software.

- *Compromised* : the switching to this state happens upon the failure of the SDN-C that ensures monitoring and data transport from/to the controlled power substations. One effect of such event could be the delay monitoring data transfer, which leads to compute an inadequate control leading to power distribution interruption. EMS functions incorporate anomaly detection mechanisms that might correct wrong data and avoid the computing of wrong control. We refer to the time before the anomaly successfully impacts the EMS as the Mean Time To Compromise (MTTC).

- *Unavailable* : the monitoring and/or control functions are interrupted. This is might be because of the failure of anomaly detection when the system is in *Compromised* state. Or, the service might be unavailable because of the failure of the EMS software or the virtualization infrastructure hardware.

3.3.0.4 *P* subsystem

We assume the ***P*** subsystem has three states :

- *Available* : the power substation operates in nominal state.
- *Compromised* : this state describes a situation where the controlling EMS has failed and it is attempting to apply wrong control. In this case, the controlled power substation is considered as compromised. In such situation, anomaly detection mechanisms are frequently performed to detect abnormal controller state. If failed, the system switches to the unavailable state. Otherwise, it goes back to the available state.
- *Unavailable* : the power substation functions are interrupted. These functions are the collection and processing of power network state data via a network of sensors, and the application of EMS control via power relays. The interruption might happen because of a wrong EMS control, a failure of the sensors data aggregation function or the failure of power relays.

3.4 . Cross-domain Dependability modeling

A system's dependability is defined as *"its ability to deliver a service that can justifiably be trusted. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical, human) that interacts with the former at the service interface"* [97]. This incorporates the attributes of availability, reliability, security, and maintainability. We leverage SANs formalism due to their efficiency in capturing complex behavior in cyber-physical systems, which in our case will be used to capture the impact of interdependencies. This is done using the *"shared places"* feature in *Möbius*, allowing subsystems SANs models to share states during simulation. We start by defining atomic models of the four subsystems described above. Then, we create a network topology by connecting subsystems' atomic models using the *Composed Model* feature of *Möbius*. Also, we define reward functions which increment the time spent in a subsystem's state during simulation period. By doing so, we are able to compute a service steady-state availability by adding the mean times spent in available states. The number of simulation steps will be adapted between experiments to ensure the convergence of the results within the confidence interval.

3.4.1 . Atomic models

An Activity Network (AN) is a generalization of Petri nets that can be defined as an eight-tuple $AN = (P, A, I, O, \gamma, \tau, \iota, \varphi)$ where P is a finite set of all places, A is a finite set of activities (transitions in Petri nets vocabulary), I is the set of input gates, and O is the set of output gates. $\gamma : A \rightarrow \mathbb{N}^+$ is a mapping between the set of activities (transitions) and the number of cases associated with each activity. *Cases* are one of the differences between ANs and Petri Nets where an uncertainty about the next state is assumed upon the completion of the activity. $\iota : I \rightarrow A$ is mapping between input gates and activities. Also, $\tau : A \rightarrow \{Timed, Instantaneous\}$ specifies the type of each activity, and finally, $\varphi : A \rightarrow O$ is a mapping between the activities and output gates. As an extension to this formalism, a SAN can be defined as a five-tuple : $SAN = (AN, \mu_0, C, F, G)$ where :

- $AN = (P, A, I, O, \gamma, \tau, \iota, \varphi)$ is an activity network.
- $\mu_0 \in M_p$: is the initial marking of the network (M_p is the set of all markings of the network).
- C : is the case distribution assignment which maps functions to activities. For any activity α, $C_\alpha : M_{IP(\alpha) \cup OP(\alpha)} \times \{1, ..., \gamma(\alpha)\} \rightarrow [0, 1]$, where $IP(\alpha)$ is the set of input places connected to activity α, and $OP(\alpha)$ is the set of output places connected to α. If α is enabled in a certain marking $\mu \in M_{IP(\alpha) \cup OP(\alpha)}$, $C_\alpha(\mu, .)$ is a probability distribution that is referred to in the SAN formalism as the case distribution of α in μ .
- F : is the activity time distribution function that maps a continuous function to timed activities. For any activity α, and marking μ in which α is enabled, $F_\alpha : M_p \times \mathbb{R} \rightarrow [0, 1]$, and $F_\alpha(\mu, .)$ is a continuous probability distribution function with $F_\alpha(\mu, \tau) = 0 if \tau < 0$.
- G : is the reactivation function that maps functions to timed activities. For any activity α, and marking μ in which α is enabled : $G_\alpha : M_p \rightarrow \Psi(M_p)$, and $G_\alpha(\mu, .)$ is a set of reactivation markings of α in μ (with $\Psi(M_p)$ is the power set of M_p, i.e : the set of all subsets of M_p).

Considering that the SAN models are used to simulate discrete-event systems with complex operations, the triggering of an event and the start and completion of an operation is associated with an activity *completion*. An activity is enabled if all the conditions encoded in the input gates hold. The activation of a timed activity refers to the start of an operation, and is possible if the timed activity is enabled or it is still enabled after its completion. Once the timed activity is triggered, it will either complete (if it stays enabled through

the activity duration), or be aborted (if enabling conditions don't hold during the activity duration). The duration between the triggering and completion of an activity is specified via the activity time distribution function F. The distribution parameters might depend on the marking of the SAN at the activation time of the activity. Upon the completion of an activity, *case distribution function* C determines probabilistically which case to be chosen. Finally, a timed activity could be reactivated if the markings of the network permit the reactivation. To do so, a reactivation function G is associated with each timed activity to specify the sets of markings where the timed activity is reactivated (if enabling conditions hold).

In the *Möbius* tools, the graphical representations of the aforementioned primitives are depicted in Figure3.3 and used to construct the atomic SAN models of the SDN-SPG subsystems explained in the following subsection :

Figure 3.3 – Graphical representation of a SAN elements in *Möbius*.

- **Places** : represented graphically as circles, a place represents a system's state. A place contains a certain number of *tokens* referred to as the place's *marking*.

- **Activities** : which are actions (for example : moving a token from a place to another) that the system takes a certain amount of time to complete. There are two types of activities : *timed* and *instantaneous*. Timed activities (represented by thick vertical lines in the models below) have a time distribution function associated with the firing duration. Whereas, instantaneous activities (represented in thin lines) model actions that completes immediately if the input conditions are satisfied. Enabling conditions are specified in the *input gates*. In addition, case probabilities represented as thick circles may be defined to include the uncertainty associated with the completion of an activity. Each circle refers to a possible outcome, for example if a maintenance operation takes an exponentially distributed time to complete, case probabilities are defined to consider the possibility of faulty maintenance.

- **Input gates** : this primitive controls the enabling of activities by specifying the required conditions of firing. These conditions could be a function of marking of places and define also the new markings once

the activity is completed. Input gates are represented graphically as red triangles in Möbius.

- **Output gates** : this primitive defines the marking changes applied once an activity is completed. It is graphically represented as black triangle in Möbius.

3.4.1.1 Subsystem *S*

In Figure 3.4 we illustrate the SAN model of subsystem ***S*** where we highlight different events that may occur and their impact on the service availability which is defined as the ability of the systems to maintain the control of the data plane and the handling of EMS requests. This refers to the mean time spent in the *S_OK* state. The service is unavailable if it is in states *S_NOK* or *S_fc*.

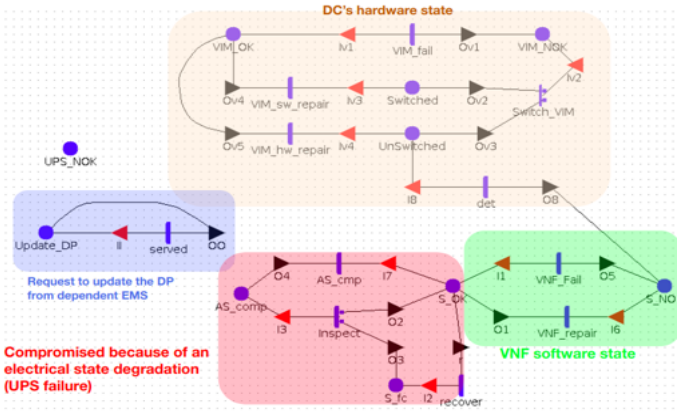


Figure 3.4 – SAN model of the ***S*** subsystem. The highlighted sub-models refer to independent dynamics that may affect the subsystem available state.

- **Virtualization Infrastructure (VI) failure** : to model the impact of the virtualization infrastructure failure on subsystem ***S***, we define the place *VIM_OK* for the available state of the virtualization infrastructure. This place is initiated with a number of tokens equal to the number of backups. In case of a failure of the VI software, the marking of the place *VIM_NOK* is incremented. Upon this event, a switching mechanism is triggered (this action is represented by the *switch_VIM* instantaneous activity) . To consider the failure of the switching mechanism, we define case probabilities which, depending on the success of the switching process, update the marking of one of the places *Switched* or *UnSwitched*. We assume that once the switching is successful, the VIM software is repaired (completion of activity *VIM_sw_repair*). Otherwise, a hardware repair must be done (activity *VIM_hw_repair*). In both cases, the *VIM_OK*

marking is incremented. Note that, if the number of tokens in the *UnSwitched* place is equal to the initial marking of *VIM_OK*, this means that all the servers are down, which imply the failure of the SDN application as well. This is represented by the deterministic activity *det*.

- **SDN-C software failure** : in this SAN sub-model highlighted in green, we model a virtualized application state. Note that, the service is available if the application is operational (represented here by place *S_OK*). A software failure event may occur due to a software bug and it was shown in the literature that the time distribution of software failure and repair can be approximated by exponential distribution [64]. Thus, we assume that the MTTF of the software application is exponentially distributed and is represented by activity *VNF_fail* which, once fired takes the system to state *S_NOK* (service unavailable). The repair event is dependent on the availability of the VIM. This condition is included in input gate *I6*. We assume that the MTTF is exponentially distributed and represented by the activity *VNF_repair*, which, once completed, will be bring the service to the available state.

- **Power supply interruption** : in the SAN sub-model highlighted by red in Figure3.4, we illustrate the impact of power supply interruption (represented by a place *UPS_NOK* marked with one token) on the networking service availability. The input gate *I7* contains the condition that if the ***UPS*** is interrupted, then the auto-scaling function is compromised. This means that, once in the *AS_comp* the networking service cannot scale to an increase in demand by increasing its computing capacity (turning on new servers). Note that, the service is always available even in this state. We assume that an inspection activity (represented by *inspect*) might take place. If the inspection succeeds, the auto-scaling is recovered. Otherwise, the system switches to a failed state denoted *S_fc* for failed-compromised to distinguish from internal failure state. Once in this latter state, the recovery process depends on the recovery of the ***UPS*** (the marking of *UPS_NOK* passes to zero token).

- **Data plane update requests arriving** : the place *Updata_DP* is shared with the dependent ***E*** subsystems. Once it is marked with more than one token (a request arrival), the request is served if the subsystem ***S*** is in state *S_OK*. In the output gate *OO*, the marking is decremented and the systems waits for the upcoming request. Note that, the request generation is highlighted in blue in Figure 3.5 below.

3.4.1.2 Subsystem *E*

The virtualization infrastructure and application software sub-models of the subsystem ***E*** are similar to subsystem ***S***. We detail the state-space sub-models for request generation and the impact of networking service interruption illustrated in Figure 3.5 :

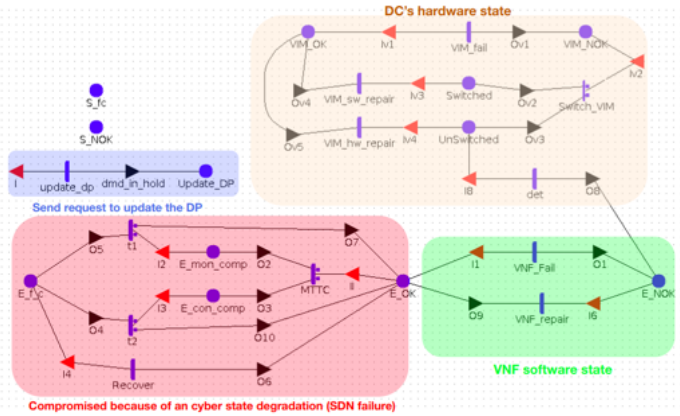


Figure 3.5 – SAN model of the ***E*** subsystem. The highlighted refers to independent dynamics that may affect the subsystem available state.

- **Networking service interruption** : this state-space model considers the failure states (*S_OK* and *S_fc*) of the subsystem ***S*** on which it is dependent. If the marking of one of these states is equal to one token (this condition is implemented in input gate *I1*), the monitoring or the control functions are compromised. We assume that the Mean Time To Compromise (MTTC) is exponentially distributed, and we define case probabilities to model on the uncertainty on whether the completion of this operation would impact the monitoring or the control functions of the EMS. Then, once the marking of one of the places *E_mon_comp* or *E_con_comp* is updated, an inspection operation is performed (activities t_1 and t_2), which will take the system back to state *E_OK* if succeeded. Otherwise, the service becomes unavailable and the system switches to state *E_fc*. Recovery procedure is performed in exponentially distributed periods (activity *Recover*) and takes the systems back to state *E_OK*.

- **Data plan request generation** : the sub-model highlighted in blue represents the process of generating a request to update the data plane when interfacing with the SDN-C. The request arrives in exponentially distributed time (activity *update_dp*) if the request queue is empty (the condition that the marking of the place *Update_DP* is equal to zero is implemented in input gate *I*). If the request is generated, the request is satisfied if the marking of *Update_DP* switches back to zero (activity *ser-*

ved in Figure 3.4 is fired).

3.4.1.3 Subsystem *P*

In the SAN model depicted in Figure 3.6, we assume that the service is available if the system is in states *P_OK* or *P_comp*. If the ***E*** subsystem is unavailable (in state *E_NOK* or *E_f_c*), a wrong control flow might compromise the controlled power substation (activity *p_mttc*). If the issue is detected, the system switches back to state *P_OK*. During the compromised state, load balancing control might be triggered (activity *LB_power*). If the control is corrected, the system switches back to state *P_OK*. Otherwise, the wrong control is applied and the system enters the *P_fc* state. To go back to available state, a recovery procedure is performed (activity *P_recover*).

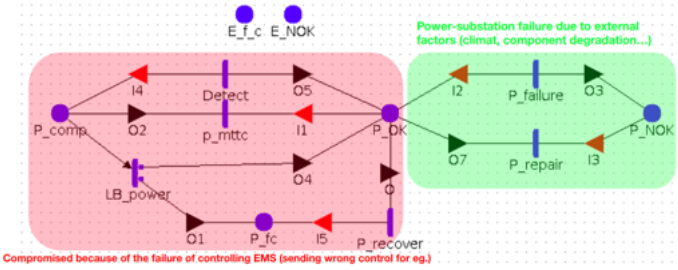


Figure 3.6 – SAN model of the ***P*** subsystem.

3.4.1.4 Subsystem *UPS*

In the SAN model depicted in Figure 3.7, we assume that the DC power supply service is available if the system is in states *UPS_OK* or *UPS_cmp*. If the power distribution network experiences a failure (states *P_fc* or *P_NOK* are marked with one token) , the impact is not imminent (due to backup batteries). Note that, a UPS is a reactive system that regulates incoming power flow and adapt it to eDC needs. The delay before the system is impacted is modeled as deterministic time (activity *impact*). Once this time is consumed, UPS capacity to recharge batteries or filter power fluctuations is compromised. Activity *AS_request* firing means that the DCs requires more power to respond to hosted services deployment needs (expressed by the shared states *VIM_OK, S_OK and S_NOK*). The success of the operation depends on the availability of the power substation on which the eDC is dependent.

3.4.2 . Composed models

As evoked previously, the atomic SAN models of the subsystems represent the lower level of the hierarchical model. The upper, network-level model is

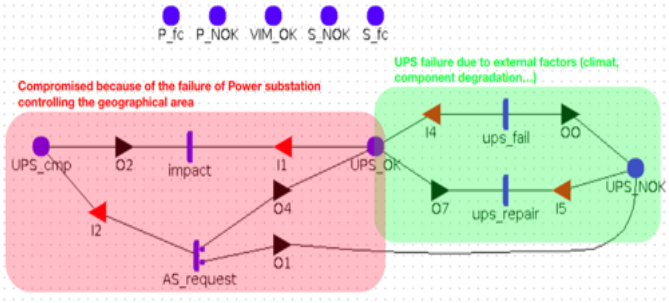


Figure 3.7 – SAN model of the ***UPS*** subsystem. The highlighted refers to independent dynamics that may affect the subsystem available state.

constructed by linking the subsystems to create a *dependency graph*. The previous atomic models are aggregated in *Möbius* using the *Composed Model* feature to construct the network to simulate. The objective is to study the different choices or strategies in terms of topology design and quantify the impact on steady-state availability of the virtualized services (subsystems ***E*** and ***S***). More precisely, we want to quantify the gain in availability when adopting different topologies (or different redundancy schemes). Therefore, we simulate the topologies illustrated in Figure 3.8 alongside their correspondent formalism in *Möbius*.

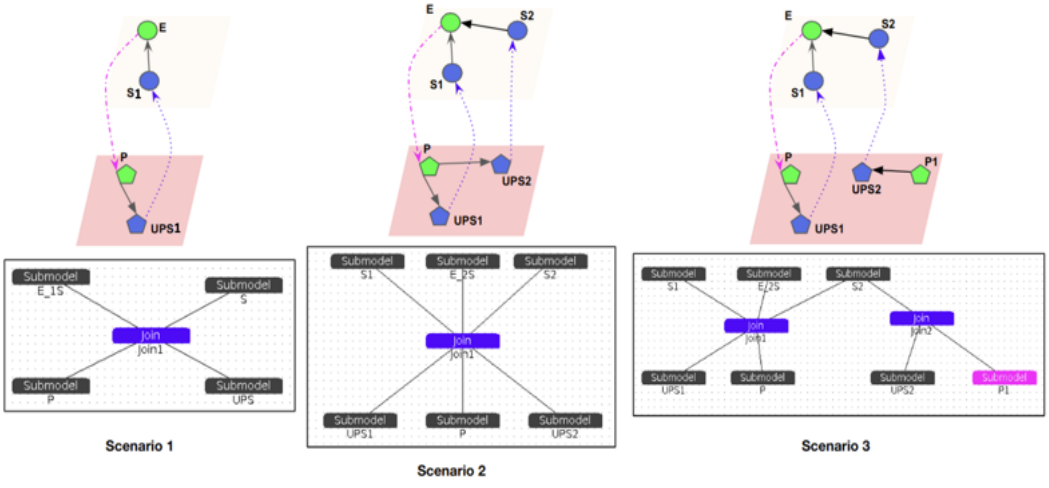


Figure 3.8 – Graph-Join Model of the different scenarios.

Note that in scenario 2 and 3, we must modify the atomic model of the ***E*** subsystem to include the state of ***S2*** alongside that of ***S1***. The choice of these topologies is done to highlight a situation where a copy of the SDN-C is distributed between two sites ***S1*** and ***S2*** in order to achieve higher redundancy. The difference between scenarios 2 and 3 lies in the power-domain interconnec-

tions where we assume that the power supply of the ***S2*** site is independent of the served EMS in scenario 3 compared to scenario 2 where the power supplies of both SDN-C sites relies on the same region controlled by the served EMS. The objective is to quantify and compare the gain in availability obtained when switching from scenario 1 to scenarios 2 and 3.

3.5 . Simulations

The values of failure and repair data parameters are adapted from different sources[98] [99] [100]) and presented in Table 3.2. We conduct experiments to study the sensitivity of the model to different variables as well as different service protection schemes depicted in Figure 3.8. In this figure, we show the simulated topologies with the correspondent implementation in *Möbius* using the Graph-Join model. We evaluate the Steady State Availability (SSA) of different subsystems in the network with a focus on virtualized services (subsystems ***S*** and ***E***). Note that, the passage from scenario 1 to scenarios 2 and 3 refers to a situation where a redundancy scheme of the communication services (***S1***) is created. The objective is to highlight the impact of integration of the knowledge about power domain interdependencies, into the decision process of where to instantiate the redundant copies of virtualized service in the data centers plane. That is, the problem of virtualized services placement is often modeled as an optimization problem where the constraints are formulated to deal with computing environment constraints (resources capacity, latency, and network bandwidth). However, the power supply of the eDCs composing the protection scheme is assumed to be reliable. In our work, we attempt to shed the light on the importance of adding power-domain information to the decision process in order to deal with the impact of power supply interruption due to specific failure propagation patterns. We argue that these patterns will be more frequent due to the high densification of the eDCs networks supporting CIs operations and because of the geographical proximity between interdependent telecommunication and power subsystems. This could be integrated into the eDCs dimensionning decision process whose objective is to determine the minimum amount of computing resources of eDCs and power backup batteries to be installed to reduce short-term (OPEX) and long-term (CAPEX) costs of running the virtualized eDCs while reducing service downtime. To this end, two parameters are of interest : a DC's ability to withstand power outages which is characterized by he UPS backup batteries capacity, and the power control frequency applied by the EMS on power substations under control. This latter parameter is an indicator of the sensitivity of the protection scheme to the degree of renewable energy resources penetration of a certain geographical area and how to include such observation into the protection scheme construction.

Subsystem/Parameter	Definition	Distribution	Value (h^{-1})
S-E/VNF_fail	VNF failure rate	Exponential	0.01
S-E/VNF_repair	VNF repair rate	Exponential	2.94
S-E/VIM_fail	VIM failure rate	Exponential	0.0005
S-E/VIM_sw_repair	VIM software repair rate	Exponential	0.02
S-E/VIM_hw_repair	VIM hardware repair rate	Exponential	0.048
S/AS_cmp	Compromised auto-scaling	Deterministic	2
S/recover	Recovery process after compromise	Exponential	0.125
S/served	Request handling rate	Exponential	3
S/switch/cases	Switch success probability	-	0.99
S/inspect	SDN software inspection rate	Exponential	2
S/inspect/cases	inspection success probability	-	0.6
E/MTTC	Mean time to compromise EMS	Exponential	0.5
E/t1-t2	Software inspection process	Exponential	3
E/recover	Recovery process after compromise	Exponential	0.125
UPS/UPS_fail	UPS failure rate	Exponential	0.004
UPS/UPS_repair	UPS repair rate	Exponential	0.125
UPS/impact	backup standby time	Deterministic	3
P/P_failure	*P* failure rate	Exponential	0.00005
P/P_repair	*P* repair rate	Exponential	0.03
P/p_mttc	*P*'s mean time to be compromised	Exponential	2
P/detect	*P*'s software inspection rate	Exponential	2
P/LB_power	power load balancing control event rate	Exponential	2
P/P_recover	*P*'s recovery process rate	Exponential	0.03

Table 3.2 – Failure and Repair data used in the reference scenario adapted from [98],[99], and [100].

For the next simulations we variate the parameters *UPS/impact* (which will be refered to as POD for Power Outage Delay in simulation) and *P/LB_power* (which will be referred to as PCR for Power Control Rate) to study the impact of UPS backup capacity and power control rate respectively. We conduct Monte Carlo simulation with 1000000 samples and the results converge within their respective confidence intervals. First, the steady state availability measures of each subsystems under the reference parameters defined in Table 3.2 are shown in Table 3.3.

Measure	Scenario 1	Scenario 2	Scenario 3
SSA^{E}	0.745605	0.984982	0.997858
SSA^{S1}	0.575937	0.972332	0.984771
SSA^{S2}	-	0.971048	0.996642

Table 3.3 – SSA measures for the reference parameters set.

We observe that the steady state availability measure of subsystems ***S1*** and ***E*** increases significantly (by 40.7% and 24.3% respectively) by increasing the redundancy of the communication service (the passage from scenario 1 to scenarios 2). This increase is more significant when switching to scenario 3 where the eDCs hosting the other redundant copy of the service is independent in the power domain of the power substation controlled by ***E***. In scenario 2, the SSAs measures of subsystems ***S1*** and ***S2*** are approximately

the same and both increase when ensuring power independency of ***UPS2*** in scenario 3. Overall, the obtained results are aligned with the initial assumptions of the efficiency of integrating power-domain knowledge to the choice of redundant sites. In addition to the virtualized environment constraints (computing capacity, bandwidth, memory), it is worth to make sure that the eDCs doesn't fall in the failure propagation path. In addition, we showed that emerging failure cascading events due to interdependencies between the EMS and SDN services need to be addressed with joint actions both at the virtualized DCs and power domains.

From a network dimensionning perspective, it is worth to study the trade-off between ensuring local power protection (captured by the parameter *UPS/impact*) and ensuring dynamic, redundant protection of virtualized services (passage from scenario 2 to scenario 3). Moreover, this procedure is more adequate to protect DCs in regions with high penetration of renewable energy (characterized with high control frequency captured by the parameter *P/LB_power*). In what follows, we provide a detailed study on the impact of both parameters.

3.5.1 . The impact of UPS' backup batteries capacity

We study the impact of power outage delay on eDC's services availability by varying the parameter *UPS/impact* which is a delay measured in hours. This parameter characterizes the capacity of the UPS to manage backup batteries and preserve its filtering functions during an abnormal electrical state. The power outage is caused by the application of the wrong EMS control. The results are shown in Figure 3.9. For subsystems *S1* and *S2*, an increase in UPS capacity to handle power distribution fluctuations, enhances the service availability. For scenario 1, and due to the reliance on only one UPS, the impact of backup capacity shortage is more apparent compared to scenarios 2 and 3 where a redundancy scheme is present. When comparing scenarios 2 and 3, we can see clearly that ensuring geographical decoupling of UPS power supply (as in scenario 3), leads to more stable service delivery, compared to scenario 2 where the two *S* subsystems ensuring the protection scheme, are geographically dependent on the same power substation. For subsystem *E*, the results shown in the graph of Figure 3.9a show similar behavior as the subsystems *S1* and *S2* due to high dependency. This means that wrong EMS control may have a cascading impact on the service itself due to specific failure propagation patterns. In Table 3.4, we show the results for incremental values of the POD (Power Outage Delay) for different subsystems and we notice that the behavior (increase in SSA measure) is common to all subsystems which suggests that failure propagation has been mitigated and that, the external impact on the availability is attenuated. In order to highlight to which extent external failures propagation impacts the SSA measure, we illustrate

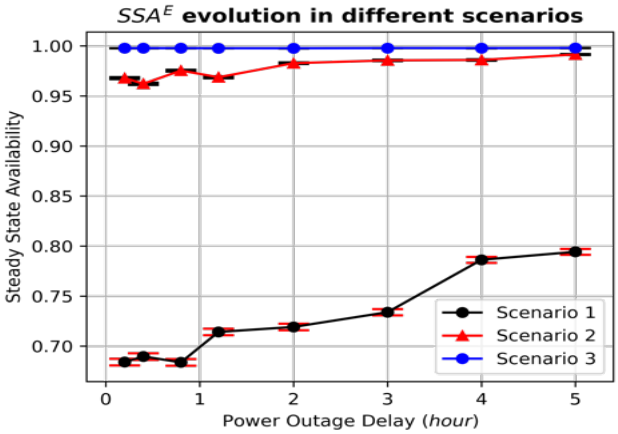
the frequency of external failures and their contribution to the unavailability in Figure 3.10, Figure 3.11, and Figure 3.12 for subsystems ***E***, ***S1***, and ***S2*** respectively. Note that, *Failure Mode 1* refers to service interruption caused by internal causes (VNF software failure, or shut-down due to eDC hardware failure). Whereas, *Failure Mode 2* refers to failure caused by external factor (***UPS*** failure for ***S*** subsystem and SDN-C failure for the ***E*** subsystem. We start by varying the time that the power UPS backup can sustain a power distribution failure. For the three subsystems and in different scenarios, the results are shown in figures 3.10, 3.11, and 3.12 where the confidence intervals of the results are also represented. We observe that for both subsystems ***E*** and ***S1***, in scenario 1, the steady state unavailability drops when increasing the POD (i.e power backup capacity) and that this unavailability is mostly caused by the cascading impact (frequency represented in orange bar). In scenario 2, both subsystems ***S1*** and ***S2*** show the same behaviour when varying the power backup POD. The unavailability of ***S1*** has dropped by a factor of 10 compared to scenario 1 and the impact of cascading failures decreases with the increase of the backup capacity. The same is observed for subsystem ***E*** whose steady state unavailability measure has decreased by a factor of 10 compared to scenario 1. Also, we observe that the latter subsystem becomes more resilient to cascading failures as the *Failure Mode 1* is more dominant over *Failure Mode 2* in scenario 3.

Measure	**Scenario 1**			**Scenario 2**			**Scenario 3**		
	POD=0.1	POD=3	POD=6	POD=0.1	POD=3	POD=6	POD=0.1	POD=3	POD=6
SSA E	0.66853	0.74560	0.81231	0.96787	0.98556	0.99023	0.99773	0.99786	0.99788
SSA S1	0.43660	0.57594	0.69951	0.93722	0.97354	0.97941	0.97539	0.98477	0.98830
SSA S2	-	-	-	0.94147	0.97189	0.98097	0.99624	0.99664	0.99716
SSA UPS1	0.52935	0.73555	0.85226	0.94762	0.98282	0.98815	0.98448	0.99188	0.99388
SSA UPS2	-	-	-	0.95789	0.98319	0.98975	0.99893	0.99922	0.99948
SSA P1	0.58061	0.66818	0.75256	0.95602	0.97686	0.97967	0.99034	0.99029	0.99072
SSA P2	-	-	-	-	-	-	0.99973	0.99970	0.99951

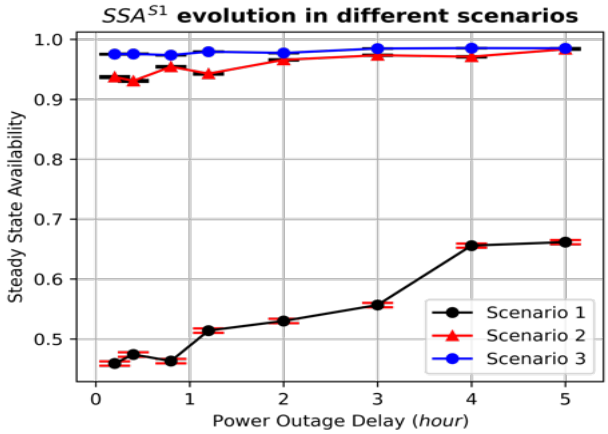
Table 3.4 – Evolution of SSA measures of different subsystems in different scenarios as a function of the UPS backup capacity (expressed as the maximum time before power supply interruption).

3.5.2 . The impact of power control rate

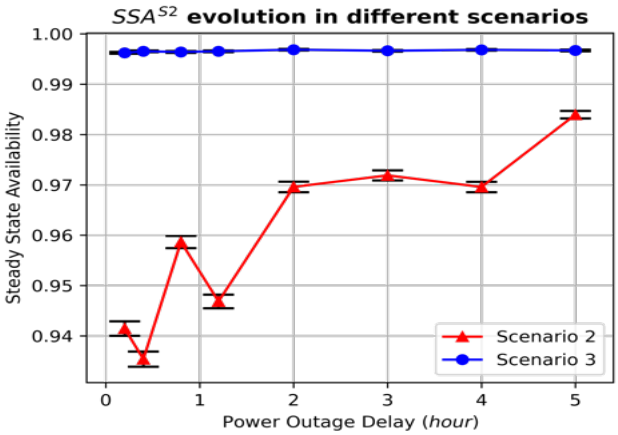
We study the impact of power control rate on eDC's services availability by varying the parameter *P/LB_power*. This parameter characterizes the frequency of event-triggered control which could be an indicator on high penetration of renewable energy sources in a particular area. Higher control frequency might correlates with EMS failure events leading to wrong control



(a) Evolution of the SSA of *E* as a function of UPS backup capacity of the *S1* subsystem on which it is dependent.

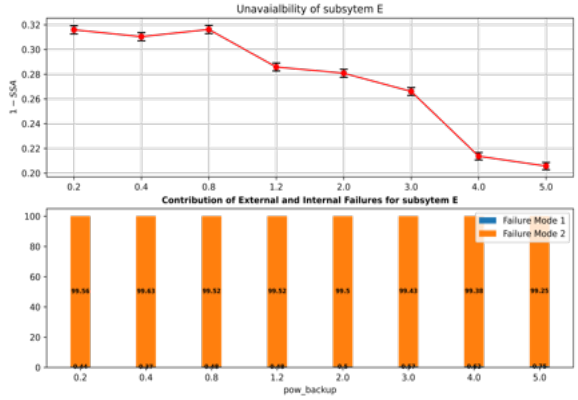


(b) Evolution of SSA measure of *S1* as a function of UPS backup capacity.

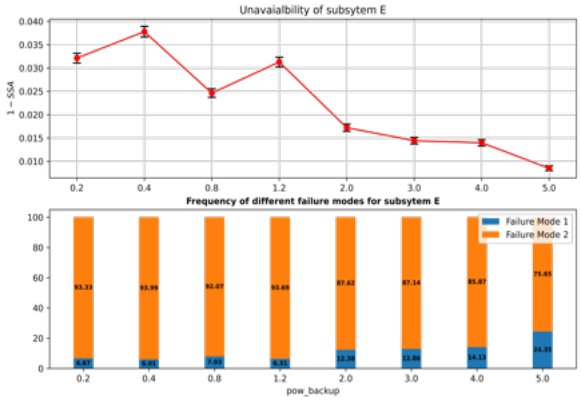


(c) Evolution of SSA measure of *S2* as a function of UPS backup capacity.

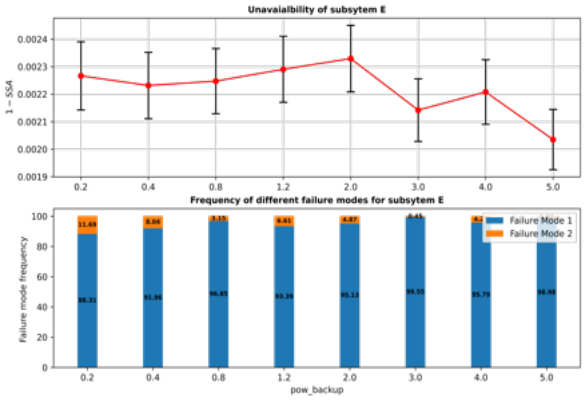
Figure 3.9 – SSA variation of subsystems *E*, *S1*, and *S2* for different scenarios as a function of power outage impact delay.



(a) Scenario 1

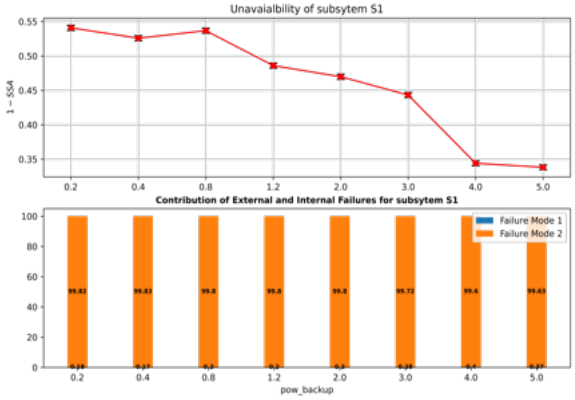


(b) Scenario 2

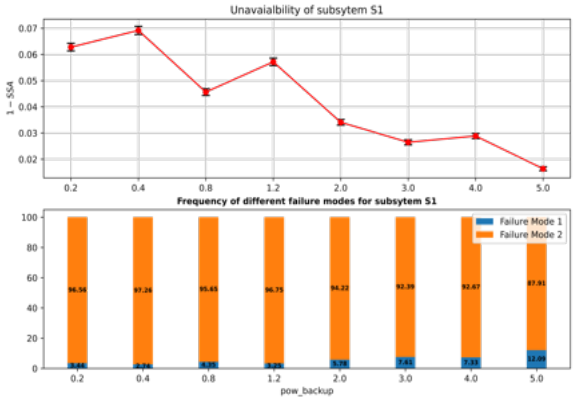


(c) Scenario 3

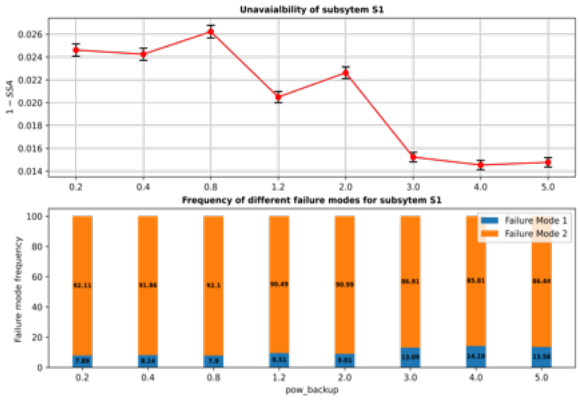
Figure 3.10 – $(1 - SSA)$ variation of subsystem *E*, and the frequency of failure modes for different scenarios as a function of **UPS** backup capacity (expressed in hours).



(a) Scenario 1

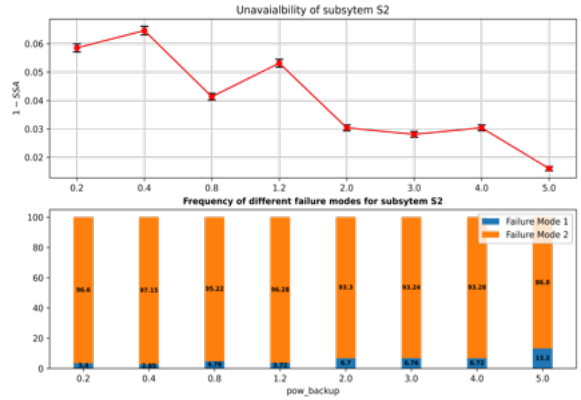


(b) Scenario 2

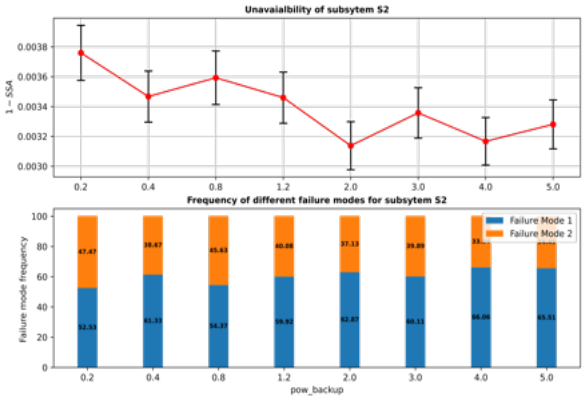


(c) Scenario 3

Figure 3.11 – $(1 - SSA)$ variation of subsystem *S1*, and the frequency of failure modes for different scenarios as a function of **UPS** backup capacity (expressed in hours)



(a) Scenario 2



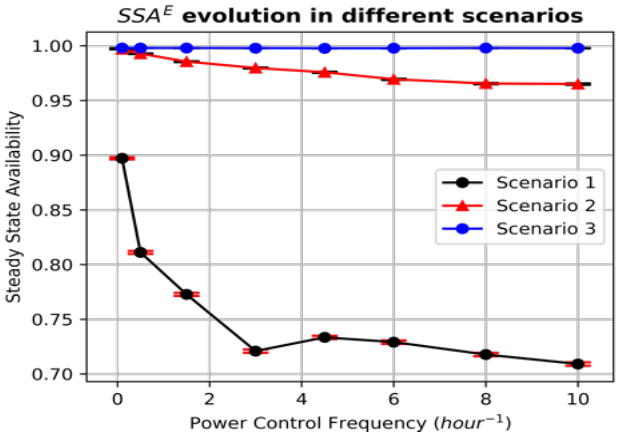
(b) Scenario 3

Figure 3.12 – $(1 - SSA)$ variation of subsystem *S2*, and the frequency of failure modes for different scenarios as a function of **UPS** backup capacity (expressed in hours)

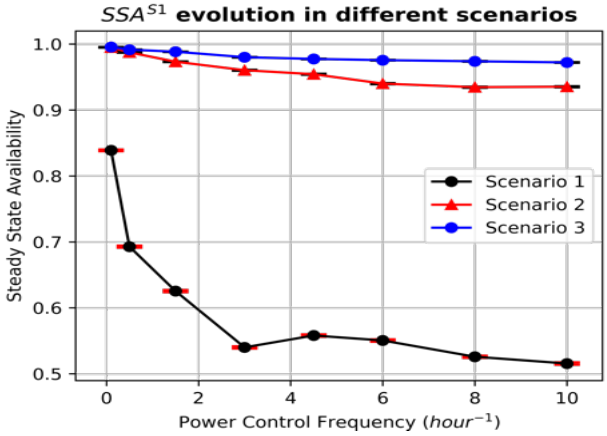
that initiates cascading failure events. In Figure 3.13 we notice that high power control frequency values decreases the SSA of virtualized services. We notice also, that redundancy may lead to better steady state availability comparing the topologies of scenarios 2 and 3. The obtained results suggest that in regions which require frequent power distribution control, the cascading failures are more frequent. Hence, a resilient protection scheme in the virtualized DCs domain should be distributed across regions with independent power control frequency. In Table 3.5, we show the SSA evolution for different subsystems when varying the power control (or load balancing) rate. We observe that the behaviour of the SSA measure is similar for the different subsystems which suggests that the failure propagation mitigation in one subsystem (or in one domain) has an impact on dependent subsystem's availability. For an in depth analysis of the failure propagation pattern, we illustrate the results depicting the frequency of different failure modes in figures 3.14, 3.15, and 3.16. We observe that for both subsystems ***E*** and ***S1***, in scenario 1, the steady state unavailability increases with high power control rate and that this unavailability is mostly caused by the cascading (external) impact (frequency represented in orange bar). In scenario 2, both subsystems ***S1*** and ***S2*** show the same behaviour when varying the power control rate parameter. The unavailability of ***S1*** has dropped by a factor of 10 compared to scenario 1 and the impact of cascading failures increases with the increase of the power control rate. The same is observed for subsystem ***E*** whose steady state unavailability measure has decreased approximately by a factor of 10 compared to scenario 1. Also, we observe that the frequency of external failure is approximately the same as in scenario 2 for subsystem ***S1*** which is still dependent on the same power substation controlled by ***E***. However, ensuring the decoupling as performed for subsystem ***S2*** in scenario 3 leads to less frequent external failures when comparing in Figure 3.16. Overall, a trade-off between the operational cost of the eDCs (installed UPS capacity) and the QoS (service availability) must be studied to determine the optimal dimensionning of the eDCs while dealing with resource shortage and the risk of failure propagation.

3.5.3 . Sensitivity Analysis

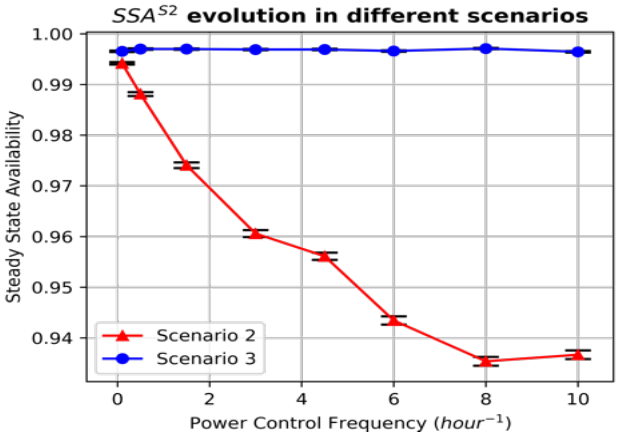
In this section, we perform a sensitivity analysis to study the parameters and their impact on the SSA measures of different virtualized subsystems. One of the drawbacks of model-based availability evaluation is the need to define many parameters whose real value is often unmeasured. The results of the analysis are shown in figures 3.17, 3.18, and 3.19 where the parameters are varied between -75% (inferior (Inf) value) and $+75\%$ (superior (Sup) value) of there reference value. We observe that for subsystem ***E*** in scenario 1,



(a) Evolution of SSA measure of the subsystem *E* as a function of power control rate.

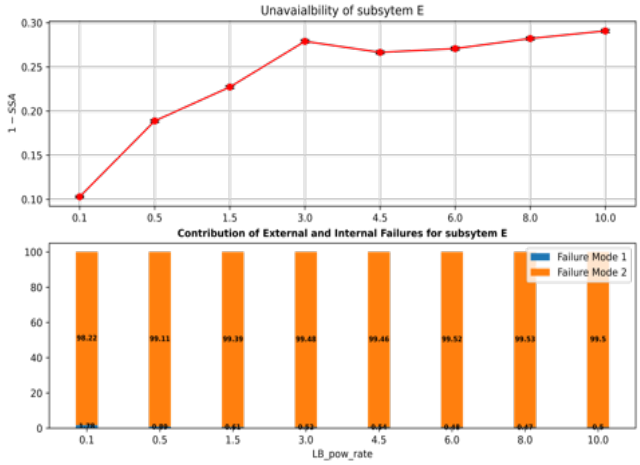


(b) Evolution of SSA measure of the subsystem *S1* as a function of power control rate.

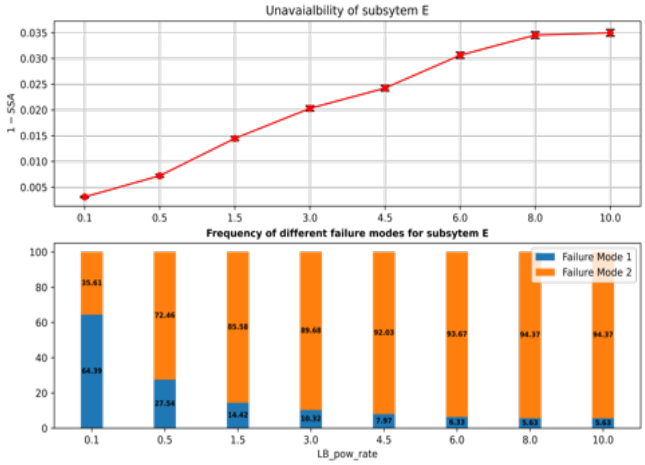


(c) Evolution of SSA measure of the subsystem *S2* as a function of power control rate.

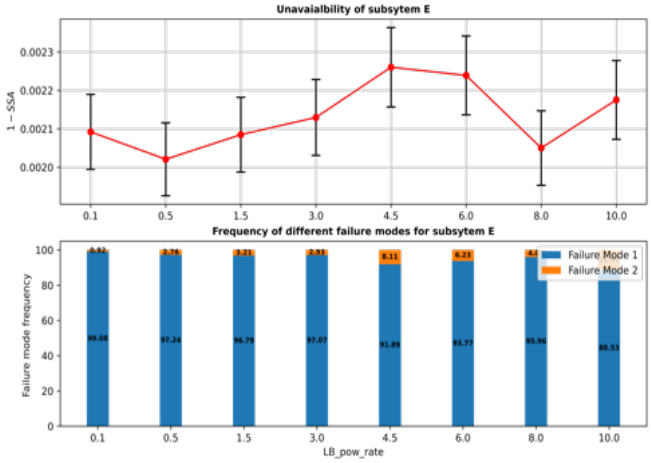
Figure 3.13 – SSA variation of subsystems *E*, *S1*, and *S2* for different scenarios as a function of power control rate.



(a) Scenario 1

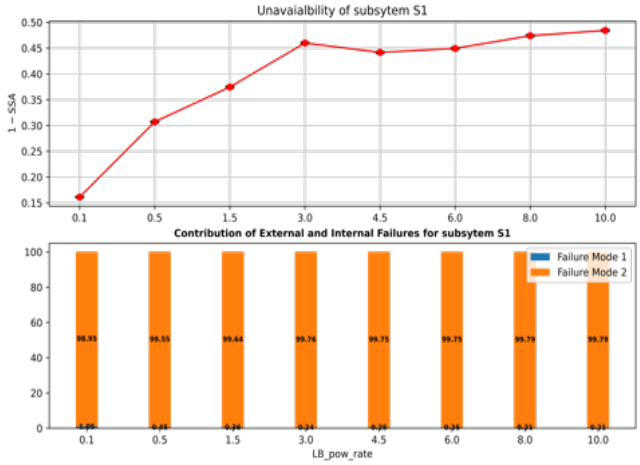


(b) Scenario 2

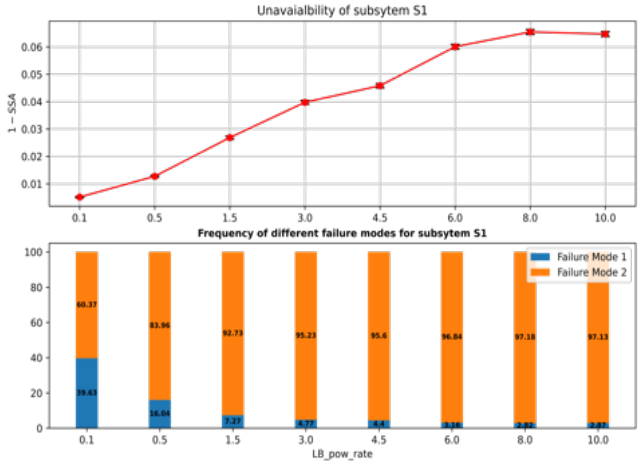


(c) Scenario 3

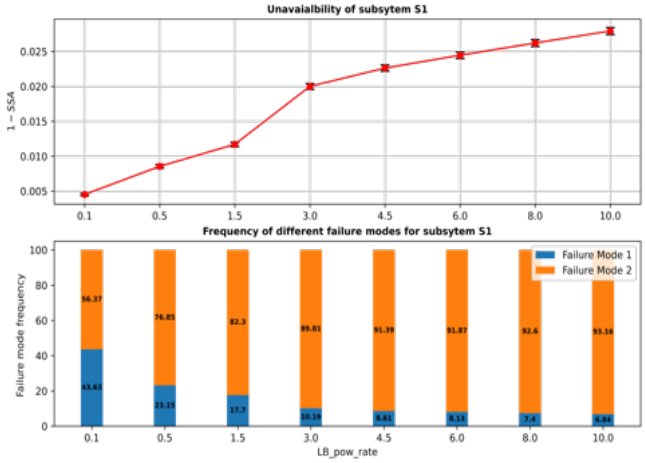
Figure 3.14 – $(1 - SSA)$ variation of subsystem *E*, and the frequency of failure modes for different scenarios as a function of *Power Control Rate (PCR)*.



(a) Scenario 1

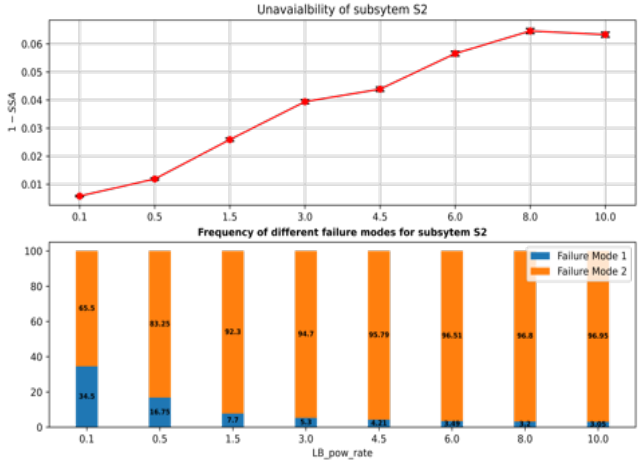


(b) Scenario 2

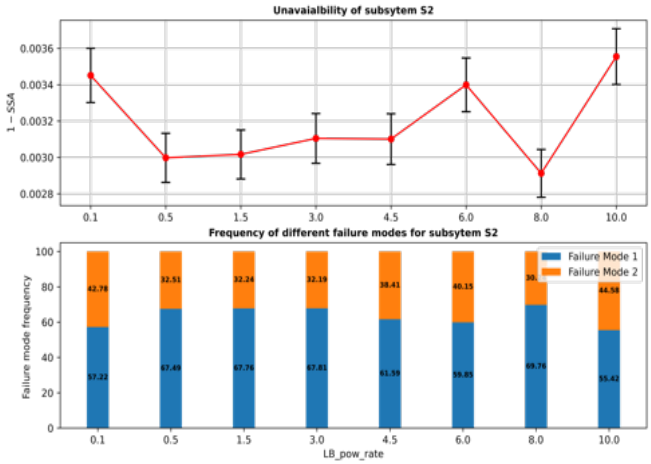


(c) Scenario 3

Figure 3.15 – $(1 - SSA)$ variation of subsystem *S1*, and the frequency of failure modes for different scenarios as a function of *Power Control Rate (PCR)*.



(a) Scenario 2



(b) Scenario 3

Figure 3.16 – $(1 - SSA)$ variation of subsystem *S2*, and the frequency of failure modes for different scenarios as a function of the *Power Control Rate (PCR)*.

Measure	Scenario 1			Scenario 2			Scenario 3		
	PCR=0.1	PCR=1	PCR=5	PCR=0.1	PCR=1	PCR=5	PCR=0.1	PCR=1	PCR=5
SSA E	0.87032	0.72092	0.72345	0.99472	0.98033	0.96948	0.99777	0.99781	0.99784
SSA S1	0.79678	0.54007	0.54061	0.99247	0.96216	0.94027	0.99401	0.97874	0.97557
SSA S2	-	-	-	0.99130	0.96339	0.94208	0.99643	0.99690	0.99665
SSA UPS1	0.89963	0.71181	0.70506	0.99581	0.97442	0.95835	0.99766	0.98772	0.98574
SSA UPS2	-	-	-	0.99654	0.97762	0.96261	0.99911	0.99940	0.99960
SSA P1	0.90725	0.62948	0.61930	0.99548	0.96828	0.94652	0.99826	0.98594	0.98445
SSA P2	-	-	-	-	-	-	0.99972	0.99982	0.99966

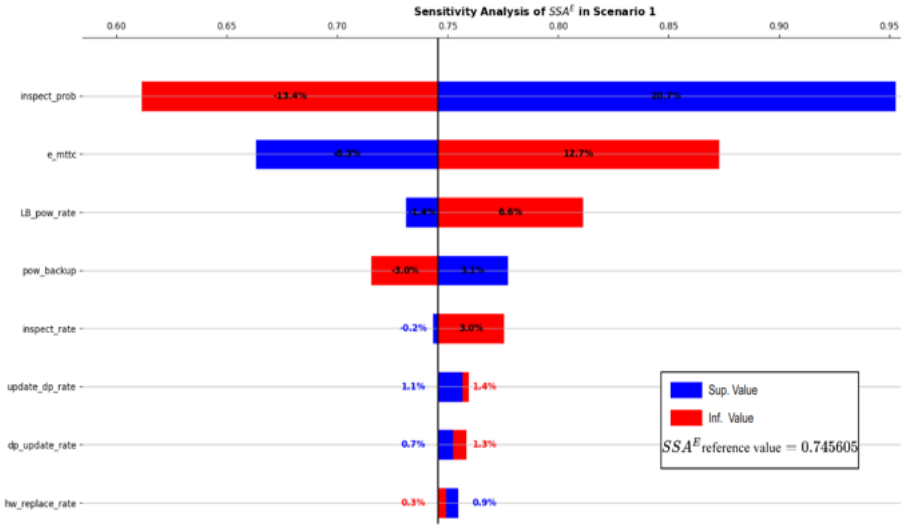
Table 3.5 – Evolution of SSA measures of different subsystems in different scenarios as a function of the power control rate (which we assume that it reflects the degree of penetration of renewable energies in particular region).

the inspection success probability is the most impacting parameter followed by the MTTC rate. Higher MTTC rate values result in increased vulnerability to the slightest changes in SDN service availability (this service is delivered by subsystem ***S***. Whereas, high inspection success probability means that the system is resilient against anomalies introduced to the misbehaviour of the SDN service. The same is observed for subsystem ***S1*** in scenario 1 because of the tight coupling between the subsystems. In scenario 2 however, the SSA measures become less sensitive to parameters variations. We observe that power outage delay and the power control rate are most impacting parameters and they are related to external dependent subsystems (***UPS*** and ***P*** respectively). In scenario 3, the variation is 10 times less than the scenario 2 and the model is robust to parameters value fluctuation. For subsystem ***S1***, the ranking of parameters based on their impact on the SSA measure is similar to subsystem ***E***. Also, we observe that the subsystem ***S2*** reacts the same way in scenario 2. However, in scenario 3 ***S2*** is more sensitive to *update_dp_rate* parameter which reflects the increase in data plane update requests. Also, this latter subsystem is also sensitive to switch preference probability which indicates the load balancing preference in terms of data plane update requests between the requesting subsystem ***E*** and SDN-C applications in ***S1*** and ***S2***.

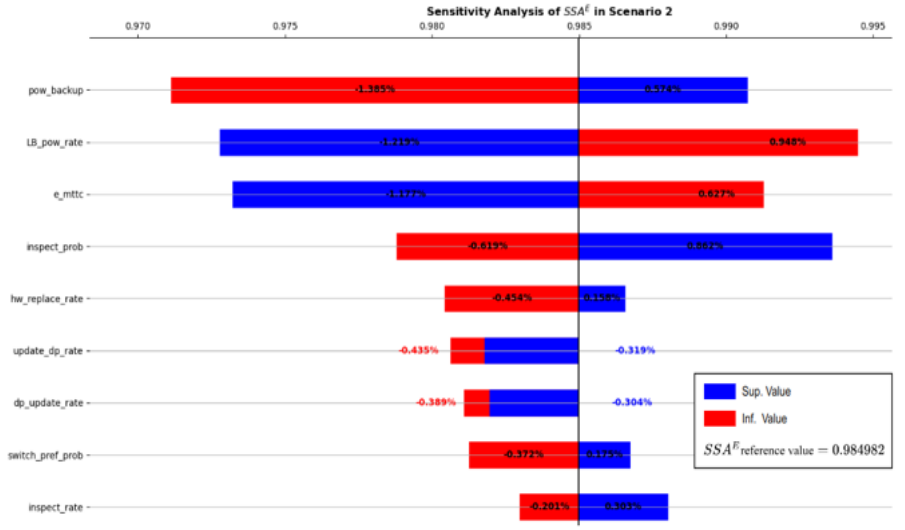
3.6 . Conclusion

In this chapter, we went through the problem of dependability evaluation in interdependent CIs integrating cloud-native management. The cloud-native management is illustrated by the deployment of edge data centers to host critical control applications by means of the vitualization technology. As an example of such CIs, we presented a reference architecture of an SDN-enabled Smart Power Grid in order to highlight emergent interdependencies between ICT and EPI services which may contribute to cross-domain cascading failure. The architecture is used to study the possibility of adopting vir-

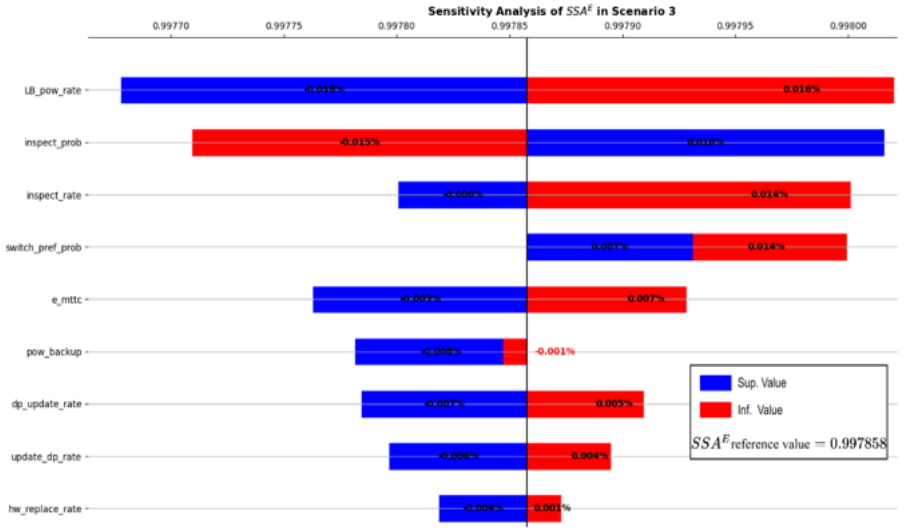
tualized services protection schemes while taking into account power-domain knowledge. To this end, we presented a hierarchical model based on Stochastic activity Network (SAN) formalism to model subsystems dynamics while capturing the impact of cascading failures, evaluate the availability of critical applications, and quantifying the impact of different protection schemes in the virtualization domain on steady-state service-oriented availability measures. The obtained simulation results suggest that ensuring the geographical decoupling of power supply systems feeding eDCs' hosting backup copies of critical virtualized services, leads to more robust protection schemes in the virtualization domain. Also, the installed power backup capacity and the power control rate (as an indicator of the high penetration of renewable energy) are key parameters in our model. These two parameters could be studied in the framework of eDCs dimensionning. That is, how to find an optimal trade-off between the installed power backup capacity of eDCs, the associated cost, the risk of failure cascades, and the performance of the hosted services (availability, latency,...). We suggest that it is possible for ICT and power operators to coordinate the installation of their eDCs infrastructure in particular geographical regions where the interdependencies patterns we modeled in this work are more relevant. As a perspective for this work, extending the modeling to real-world, network topologies with more subsystems (nodes) can be done to study more complex coupling patterns and failure propagation scenarios. Also, the virtualized services decision process, integrating the power-domain knowledge is to be formulated.



(a) Scenario 1

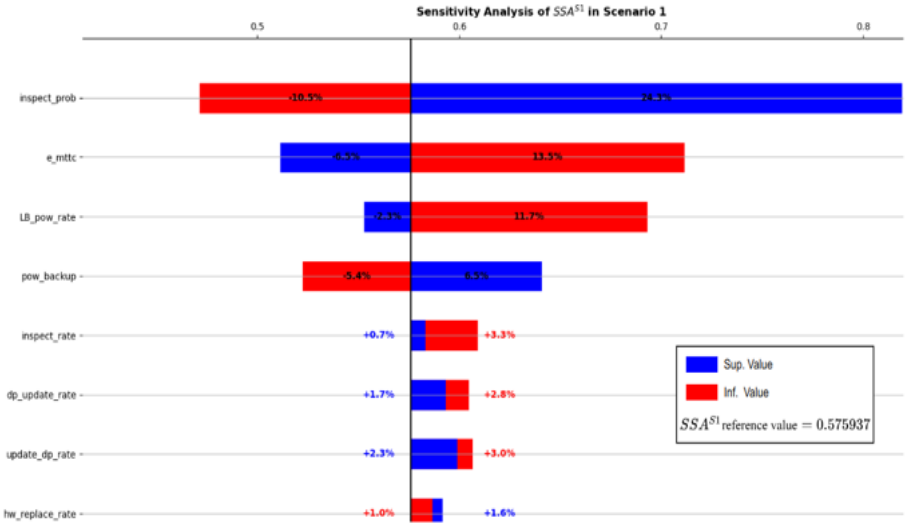


(b) Scenario 2

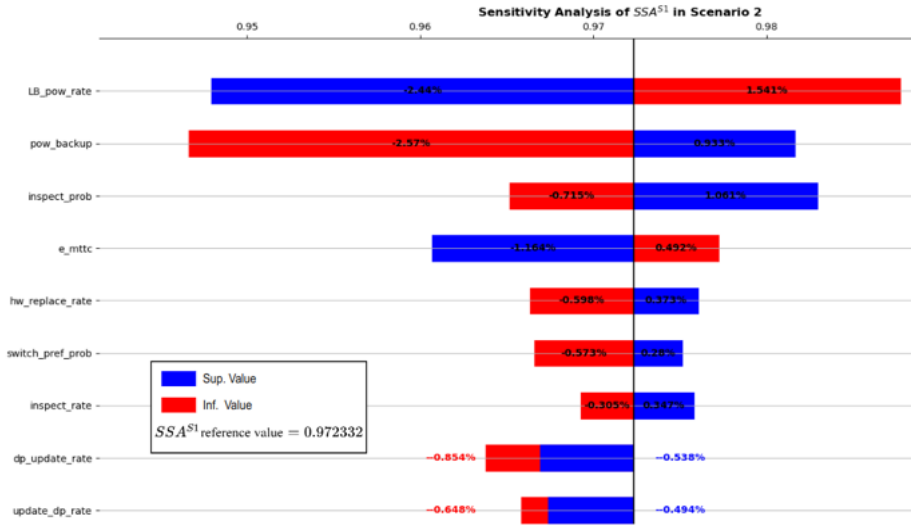


(c) Scenario 3

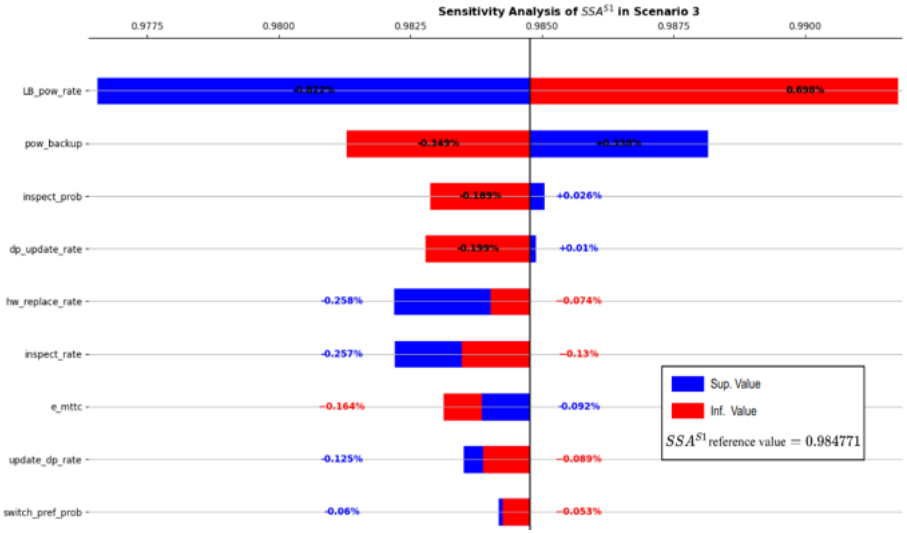
Figure 3.17 – SSA variation of subsystems *E* in scenarios 1,2,3



(a) Scenario 1

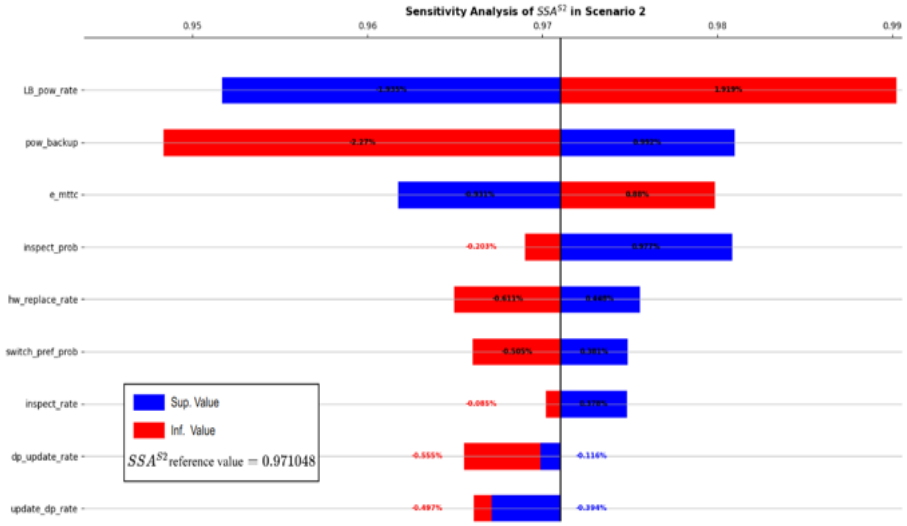


(b) Scenario 2

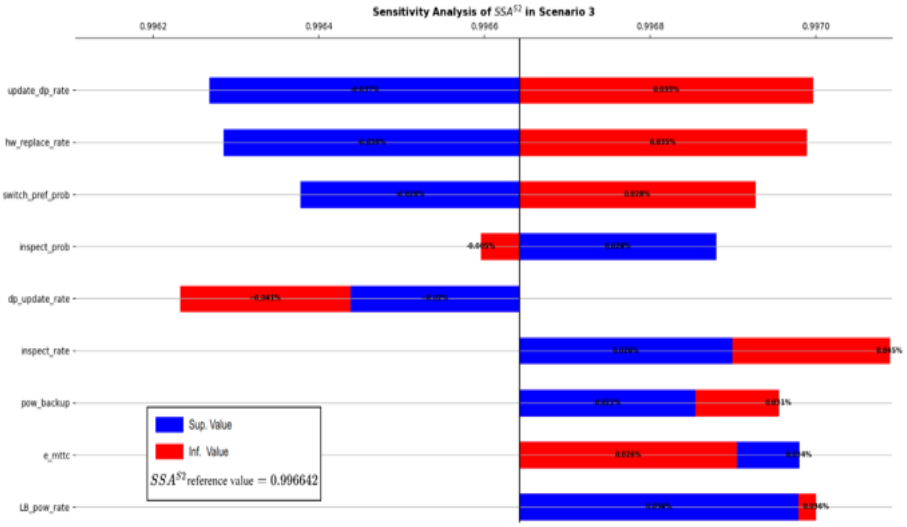


(c) Scenario 3

Figure 3.18 – SSA variation of subsystem *S1* in scenarios 1,2,3



(a) Scenario 2



(b) Scenario 3

Figure 3.19 – SSA variation of subsystem *S2* in scenarios 1,2,3

4 - Optimal orchestration of virtual resources for high availability of cloud-native critical services

In this section, we will go through the mathematical formulation of the resilient virtual resource orchestration problem. The environment is composed of (edge Data Centers) eDCs network hosting critical applications where copies of these applications are dynamically created to build redundancy schemes similar to those introduced in Chapter 3. The objective of this work is twofold. First, we want to formulate the problem of ensuring high service availability as an orchestration problem where eDCs resources are dynamically reserved and freed to run copies of selected applications whose hosting eDCs are more vulnerable to power failure cascade, all while dealing with resource shortage and application' performance constraints. The second objective is to show how risk information (the likelihood of eDC power supply interruption) can be embedded into the decision process as a constraint. To this end, we start by navigating existing works on resource orchestration in virtualized eDCs supporting CPSs networks applications. Then, we present the design principles and the optimization model formulation. The model is a Mixed Integer Non Linear Program (MINLP) with the objective to minimize the cost of protection scheme with respect to performance and availability constraint. Discrete-event simulation will be conducted to study the dynamic behaviour of the model while introducing the notion of "overbooking" as a solution to deal with resources shortage which characterizes edge environments.

4.1 . Introduction & Related Work

The flexibility resulting from using cloud-native and virtualization technologies to run software applications, is characterized by the wide range of control that could be applied into computing resources management to deal with dynamic applications needs. This leads to efficient and cost-effective resource management while respecting the service performability. Indeed, the edge computing paradigm is a key enabler of Ultra-Reliable Low-Latency Communications (URLLC) in the context of Fifth Generation of Mobile Telecommunication Technologies (5G) where service applications are deployed closer to the end customers which reduces end to end service latency. In [101] authors study the problem of VNF placement in multi access edge computing environment. The VNFs are assumed to compose a URLLC service where a trade-off between service availability and latency must be reached while mi-

nimizing the management cost. A genetic algorithm was developed to deal with the NP-hard complexity of the multi-objective function. In [102], a VNF placement optimization model was developed to ensure service provisioning that guarantees some QoS objectives in a telecommunication network where the core functions are virtualized. The authors introduce a fine-grained modeling of the impact of virtualization on the service latency leading to a more accurate modeling of delay constraints. The placement involves both the computing resources constraints as well as physical link constraints. Another use-case of NFV management in 5G networks is *Network Slicing* where a virtualized network is allocated to a particular customer to meet its particular QoS requirements. In [103], the problem of optimizing virtual resource allocation for network slicing applications is studied. The authors propose a queuing model to jointly optimize VNF placement and resource allocation for applications running on top of the same physical infrastructure. In [104], the authors propose a physical programming approach to deal with multi-domain service function chain placement. The optimization is part of a centralized orchestrator that inherits from the ETSI-NFV architectural framework to ensure service instantiation while dealing with limited visibility over the physical infrastructures due to operators' unwillingness to share private information about their assets.

Asides from the core telecommunication functions deployment, several works have investigated the use of virtualization to manage critical applications of monitoring and control of CPSs. In [105], authors study the problem of ensuring reliable service provisioning of VNFs supporting IoT-based smart grid while respecting QoS constraints. To tackle this problem, an optimization model is formulated with the objective to minimize CAPEX cost of ensuring VNF backup redundancy schemes to meet the reliability constraints. In [106], authors propose a framework to simultaneously perform VNF orchestration and power-disjoint traffic flow routing to enhance the robustness of SDN-enabled smart grid communication. A two-level hierarchical optimization scheme was developed to deal with the computational complexity of the original formulation with the objective to minimize VNF orchestration cost and maximize power-disjoint traffic routes.

In our work, backup copies of virtualized services are created in geographically distributed eDCs to mitigate failure cascades between the power and networking domains studied in Chapitre 3. The placement of the redundant copies must respect the service performance requirements in terms of latency, availability, and the amount of resources required to run the service. Also, in an eDCs network subject to cascading failures, the placement decision needs to be updated considering that some environment parameters (eDCs

availability for example) might change as well. In this framework, control theoretic approaches like Model Predictive Control (MPC) are gaining popularity due to their efficiency in dealing with the optimal resource orchestration while considering environment changes (VNFs requirements fluctuations) as system disturbances [107]. In [108], authors highlight the benefit of using MPC for VNF placement due to its efficiency in integrating future system state information to the optimization process. The author present a discrete-time dynamic model of resource utilization and developed an MPC whose cost function integrates a trade-off between energy consumption and QoS guarantees. In [109], authors extend the previous work in [108] by considering software and hardware interruption and security constraints.

Overall, in MPC an estimation of the state of the system to control for fixed time horizon is done where a cost optimization is performed which allows to treat real-time constraints as illustrated in figure 4.1. Once a pre-defined availability threshold is violated (high risk of failure propagation), an estimation of the future availability of all eDCs in the defined time horizon is performed. Based on this information, optimal resource orchestration is performed to build ephemeral redundancy schemes (in this scenario ephemeral means that the protection scheme will last at least for one time horizon). Estimated state may include : amount of available resources in eDCs, availability of hosted critical services, or the power supply state. In our work, we present a one-time optimization model formulation to show how the protection scheme' end-to-end availability can be jointly optimized with service performance requirement in terms of computing resources and latency.

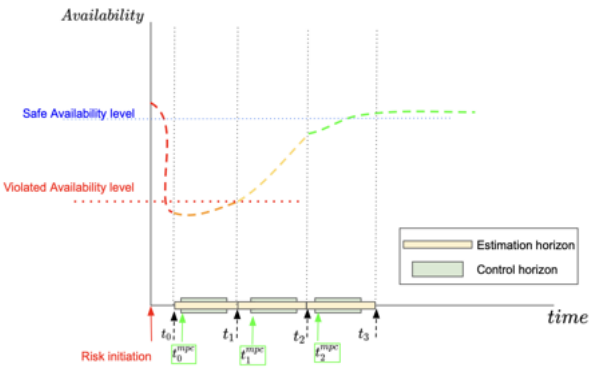


Figure 4.1 – An illustration of the MPC. Through consecutive predefined time windows, an estimation of the system state is performed. Based on which, eDCs resources are optimally orchestrated to enable the systems to meet its initial availability objectives.

4.2 . Problem Formulation

As mentioned in the previous chapter, the failure type we are considering is an ICT' eDCs power outage due to the failure of the power supply (EMS failure impacting power substations). Such event would require a maintenance operation to get the eDCs operation back to the nominal state (manual restart of hardware, hardware replacement..etc). Hence, in the context of a proactive procedure, hosted services are migrated to other eDCs fulfilling some requirements. The problem of resource migration is defined as the problem of finding the optimal mapping between a set of requests I and a set of possible eDCs J which can fulfill the requests requirements in terms of availability, computing resources, and latency. High availability is achieved through assignment redundancy. A selected, critical service k (VNFs forming the SDN-C service) is simultaneously migrated to a primary host eDC that may fails with a certain probability, and other eDCs forming an active-standby redundancy scheme as depicted in Figure 4.2. That is, the number of backups needed to ensure a certain availability of the protection scheme, is an output of optimization model. We define the model variables and parameters in Table 4.1.

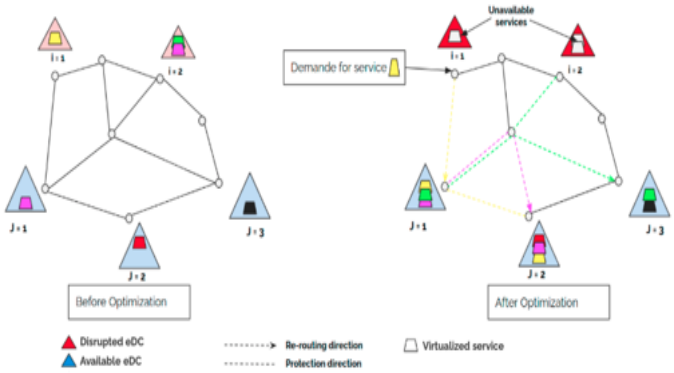


Figure 4.2 – An illustration of the redundancy scheme creation to host critical application originally hosted in eDCs subject to a power supply outage for example (eDCs $i = 1$ and $i = 2$). For the service in yellow for example, two copies are instantiated in hosts $j = 1$ and $j = 2$.

The decision is captured by the binary variables Y_{kijr}, with :

$$Y_{kijr} = \begin{cases} 1, \text{ if DC } j \text{ is chosen as } r^{th} \\ \text{ backup for demand } (k, i) \\ 0, \text{ otherwise} \end{cases}$$

In the service protection scheme, a service migration request (k, i) is assigned to more than one eDC. However, the service is running actively only in

parameter	definition
I	Set of DCs subject to maintenance intervention.
K^i	Set of services impacted by the maintenance of DC $i \in I$
J	Set of available hosts DC
c_{ki}	Resource amount request of service $k \in K^i$
θ_{ki}	Maximum latency violation allowed for service k
A_{ki}	Availability requirement of service $k \in K^i$
f_j	The setup cost of a DC j (energy consumption, rack and servers installation related costs)
λ_j	Resource usage cost (generated from renting one unit computing resource in DC j)
κ_j	The total capacity available of the host DC j.
q_j	Failure probability of DC j
t_{ij}	Data transmission latency between two connected DC i and j

Table 4.1 – Model Parameters notation

one eDC j as r^{th} backup and in standby mode in the other backups $m \in J/\{j\}$ ($Y_{kimx} = 1, x > r$), $r = 1$ is the primary assignment, $r = 2$ is the first backup and so on. Considering that a host j may fail with a probability q_j, we define the probability that a service $k \in K^i, i \in I$ is active in its r^{th} backup j :

$$\mathbb{P}_{kijr} = (1 - q_j) \sum_{m \in J/\{j\}} \frac{q_m}{1 - q_m} \mathbb{P}_{kim(r-1)} Y_{kim(r-1)} \tag{4.1}$$

This probability is calculated for an eDC j as r^{th} backup, assuming that the $(r-1)^{th}$ backup eDC m ($m \neq j$) fails with a probability q_m. The summation in (4.1) is reduced to one element (where $Y_{kim(r-1)} = 1$). If an eDC j is chosen to host two services, the setup cost f_j is computed for the two services. In addition, the cost of using the resources at full capacity in active mode (the product $c_{ki}\lambda_j$) is generated if the service is activated in eDC j at level r with probability $\mathbb{P}_{kijr}$. Note that, $\mathbb{P}_{kijr}$ is a decision variable as it is a function of $Y_{kij(r-1)}$. We formulate the optimization problem :

$$\min_{Y_{kijr}} \sum_{i \in I} \sum_{k \in K^i} \sum_{j \in J} \sum_{r=1}^{|J|} (f_j + c_{ki}\lambda_j \mathbb{P}_{kijr}) Y_{kijr} \tag{4.2}$$

$s.t$:

$$\sum_{r=1}^{|J|}\sum_{i\in I}\sum_{k\in K^i} c_{ki}Y_{kijr} \leq \kappa_j, \quad \forall j \in J \tag{4.3}$$

$$(\theta_{ki} - t_{ij})Y_{kijr} \geq 0, \forall k \in K^i, i \in I, j \in J, \forall r \tag{4.4}$$

$$\sum_{j\in J} Y_{kijr} \leq 1, \forall k \in K^i, i \in I, \forall r \tag{4.5}$$

$$\sum_{r=1}^{|J|} Y_{kijr} \leq 1, \forall k \in K^i, i \in I, j \in J \tag{4.6}$$

$$Y_{kijr} \leq Y_{kij(r-1)}, \forall k \in K^i, i \in I, j \in J, \forall r \tag{4.7}$$

$$\mathbb{P}_{kijr} = (1 - q_j) \sum_{m\in J/\{j\}} \frac{q_m}{1 - q_m} \mathbb{P}_{kim(r-1)} Y_{kim(r-1)} \tag{4.8}$$

$$\sum_{j\in J}\sum_{r=1}^{|J|} \mathbb{P}_{kijr} Y_{kijr} \geq A_{ki}, \forall k \in K^i, i \in I \tag{4.9}$$

$$Y_{kijr} \in \{0, 1\}, \forall k \in K^i, i \in I, j \in J, \forall r \tag{4.10}$$

Constraint (4.3) ensures that the sum of resource demands doesn't exceed the total capacity of the host j. Constraint (4.4) ensures that the latency between the chosen host j and affected eDC i doesn't exceed the latency violation threshold. Constraint (4.5) forces the process to choose at least one host eDC for each request. Constraint (4.6) ensures the assignment to one eDC j at each backup level r. Constraint (4.7) guarantees the service activation order in the eDCs forming the protection scheme (passing from standby to active mode). Constraint (4.9) guarantees the minimum number of backup to reach the desired availability for service k. Constraints (4.8) and (4.10) highlight the definition and domain of the decision variables. Note that, the process is forced to choose a minimum number of backups to satisfy the availability requirements with the minimum cost.

The objective function and constraint (4.9) are non linear as they include a product of two binary decision variables $\mathbb{P}_{kijr}$ and Y_{kijr}. We linearize them by introducing an auxiliary variable Γ_{kijr} as follows :

$$\Gamma_{kijr} = \mathbb{P}_{kijr} Y_{kijr} \tag{4.11}$$

$$\Gamma_{kijr} \leq Y_{kijr} \mathbb{P}^u \iff \Gamma_{kijr} \leq Y_{kijr} \tag{4.12}$$

$$\Gamma_{kijr} \leq \mathbb{P}_{kijr} \tag{4.13}$$

$$\begin{aligned} \Gamma_{kijr} \geq \mathbb{P}_{kijr} - (1 - Y_{kijr})\mathbb{P}^u \iff \\ \Gamma_{kijr} \geq \mathbb{P}_{kijr} + Y_{kijr} - 1 \end{aligned} \tag{4.14}$$

$$\Gamma_{kijr} \geq 0 \tag{4.15}$$

$\forall (k \in K^i, i \in I), j \in J, r \in \{1, 2, ...|J|\}$. With $\mathbb{P}^u = 1$ is the upper bound of the continuous variable $\mathbb{P}_{kijr}$.

4.2.1 . Interdependency-aware overbooking startegy

Interdependency is defined in our model as the degree of inoperability introduced in an eDC j due to the inoperability of a eDC hosting critical application i (for example the dependency of an EMS on a SDN-C as presented in Chapitre 3). That is, in a graph $G(V, E)$ of $|V|$ vertices and $|E|$ edges, two eDCs i and j are interdependent if the link $(i, j) \in E$. This link indicates the presence of dependencies between services hosted in both eDCs. We define the state of a DC i by S_i. If i lies in the estimated failure propagation path : $S_i = 1$, otherwise : i is available ($S_i = 0$). For two eDCs i and j in the network : if link $(i, j) \in E$ and $S_i = 1$, then j is vulnerable (failure may propagates from i to j captured by the state value $C_{ij} = 1$) with a probability $\mathbb{P}(C_{ij} = 1) = \tau = 1 - \mathbb{P}(C_{ij} = 0)$, where C_{ij} is a Bernoulli variable of parameter τ. We assume that $C_{ij} = C_{ji}$ and no possible recovery, so if an eDC experience a power supply disruption, then it will be out of service until a maintenance intervention is performed. Note that, we use the notation "*eDCs i and j are interdependent*" as equivalent to "*services K in eDCs i and j are interdependent*".

Resources reserved in backup eDCs are locked for new requests but might not be used if the primary assignment ($r = 1$) doesn't fail during the maintenance operation of the impacted eDCs. This would make the capacity constraint infeasible for upcoming requests, and hence, increase request rejection rate and accelerate failure propagation. To avoid this situation, we implement an overbooking strategy taking into account the probability of failure propagation impacting eDC j due to the failure of eDC i. The admission of a service (k, i) to an eDC j doesn't depend only on the availability of sufficient

Algorithm 1 Overbooking Policy

Require: $i, j, \kappa_j, guests$
Ensure: κ_j^{ob}
  $\kappa_j^{ob} \leftarrow \kappa_j$
  if $\mathbb{P}(C_{ij} = 1) > threshold$ **then**
    for $g \in guests$ **do**
      if j is not primary assignment **then**
        $\kappa_j^{ob} \leftarrow \kappa_j^{ob} +$ (reservation of g)
      end if
    end for
  end if
  return κ_j^{ob}

resources, but also on the dependency of services in j on service (k, i). We present the overbooking policy pseudo-code :

$guests$ contains all the anterior requests already fulfilled by j and not yet freed (ongoing maintenance in their original host eDCs). The resources reserved as standby by some requests are overbooked by j to host a interdependent service (k, i) where $\mathbb{P}(C_{ij} = 1)$ exceeds some threshold. This policy is applied to all $j \in J$, by doing so, the constraint 4.3 becomes feasible and request (k, i) is not rejected.

4.3 . Simulation

We implement our model in *Python* environment using CPLEX as an optimization engine. We design a discrete-time simulation using *SimPy* module to simulate request handling queue as depicted in Figure 4.3. We test several settings using different network topologies detailed in Table 4.2 below.

Network	$\|V\|$	$\|E\|$	Av ND
France	25	45	3.60
Atalanta	15	22	2.93
Di-yuan	11	42	7.64
Dfn-gwin	11	47	8.55

Table 4.2 – Networks characteristics [110]

For each setting, we compare different parameters values and the impact on the rejection rate. We fix the parameters f_j and λ_j and generate the ca-

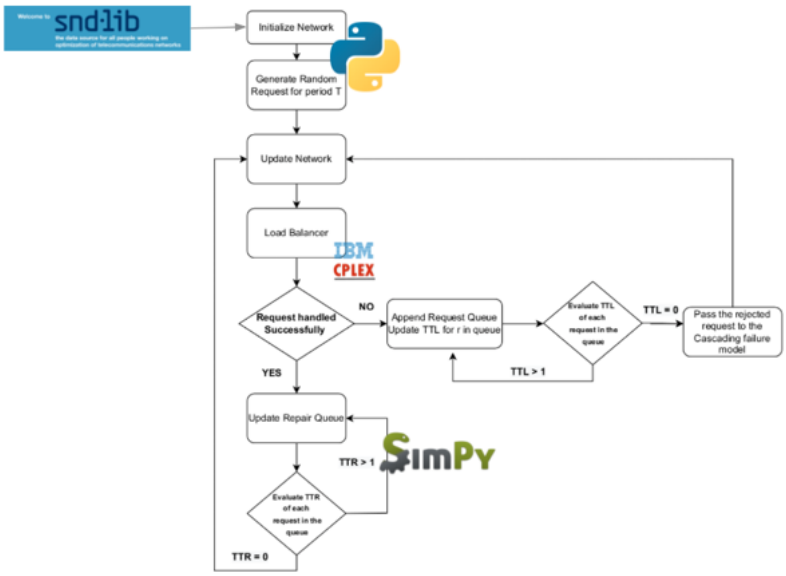


Figure 4.3 – Simulation setup.

pacities randomly using uniform distribution. We run the simulation for 30 demand periods. For each period a node (k, i) is chosen randomly for maintenance characterized by a demand tuple $\{c_{ki}, \theta_{ki}, A_{ki}\}$. We set the repair period to be equal to one i.e : resources are reserved and cannot be assigned for one period.

1. **Availability requirement :** In this setting we vary the availability requirement with a fixed cost and capacities for each node in the network. The failure probabilities of the hosts vary uniformly in the interval $[0.1, 0.3]$. We get the results depicted in Figure 4.4. As expected, high availability requirements require high redundancy, resulting in high resource reservation. For fixed DCs capacities, the optimization model becomes infeasible leading to a high rejection rate.
2. **Latency requirement :** In this setting we vary the latency requirement with a fixed cost and capacities for each node in the network. The objective is to test the impact of the topology on the migration process. we vary the latency between the minimum and maximum value of links latencies in the network .We get the results depicted in Figure 4.5. High latency makes the constraint 4.4 infeasible leading to request blocking.

Even though the redundancy scheme guarantees high service availability, it leads to resources under-usage. Resources which are reserved as backups might not be used during the maintenance intervention, preventing other services from using them leading to a higher rejection rate. One way to avoid such problem is to adopt an overbooking strategy allowing the assignment of

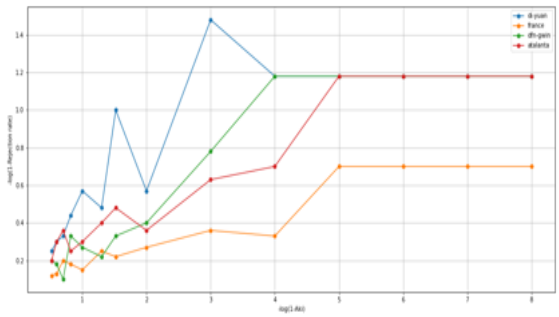


Figure 4.4 – The impact of the availability requirement on rejection rate

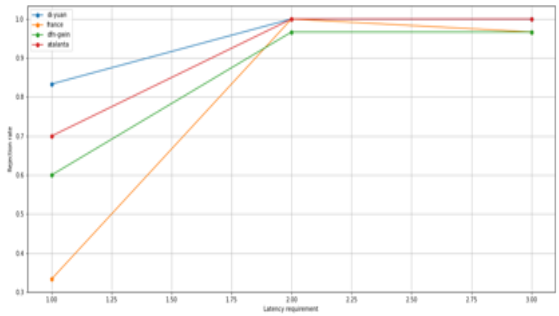


Figure 4.5 – The impact of the latency requirement on rejection rate.

reserved resources at higher backup levels. We implement the overbooking strategy introduced in 4.2.1 and study the dynamics of the ratio of impacted nodes and service rejection rate. We set the parameters A_{ki} and q_j so that each request is migrated to more than one DC. Furthermore, we set the repair period to be more than one to capture the impact of overbooking. We obtain the results illustrated in Figure 4.6a, for the two networks, *France* and *di-yuan*. The overbooking strategy increases resource usage in the network and thus, increases service migration rate.

To study the impact of critical information availability prior to the migration process, we compare the previous results with a setting where, the nodes with the highest betweenness centrality measure are considered to be critical and are protected (don't fail for a long period). Betweenness centrality quantifies the presence of the node in the shortest paths between all pairs of other nodes in the network :

$$B_c(v) = \sum_{s,t \in V} \frac{\sigma(s,t|v)}{\sigma(s,t)} \tag{4.16}$$

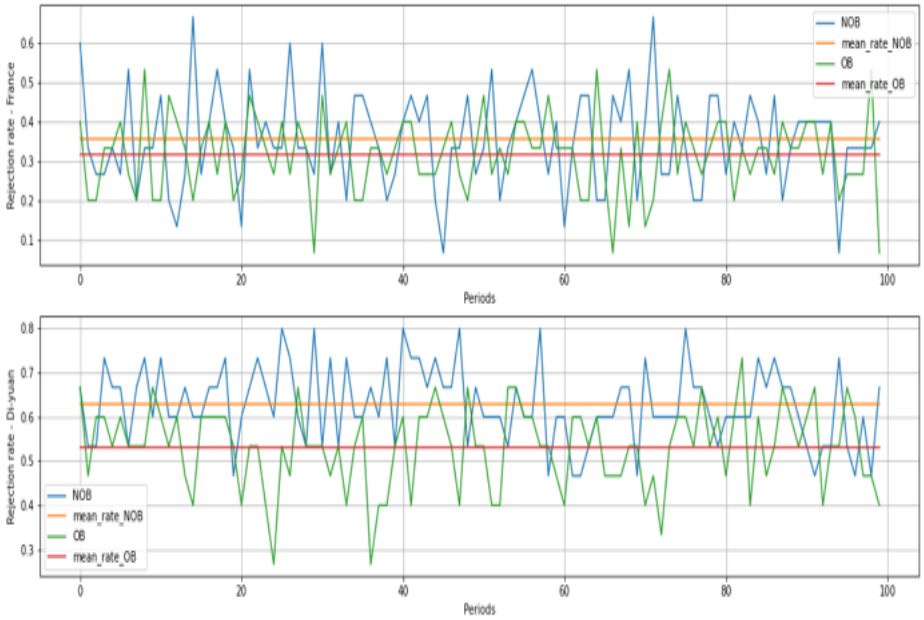
Where $B_c(v)$ is the Betweenness Centrality measure of node v in network with vertices set V. $\sigma(s,t)$ is the set of all shortest path between nodes s and t and $\sigma(s,t|v)$ is the subset that contains only the paths passing by v. We obtained the results illustrated in Figure 4.6b. The rejection rate has decreased compared to the "No protection" setting. The decrease is more important in the *France* network compared to the *Di-yuan* network. This is due to the number of nodes in each network and the node degree which is higher in the *Di-yuan* where all the nodes have approximately the same measure B_c. More detailed results obtained for all the networks are illustrated in Table 4.4 and Table 4.3. Comparing the protection and no protection settings, we notice a decrease in the rejection rate both when adopting an interdepdendency-aware overbooking strategy (mean and standard deviation of RR_{OB}) compared to the non overbooking scenario (RR_{NOB}). Also, the rate of impacted nodes obtained by the propagation model detailed above is computed for each setting. Similarly to the rejection rates, the impact of failure is decreased when protecting critical nodes and when adopting an overbooking strategy.

Network	Mean (RR_{NOB})	Std (RR_{NOB})	*Failure rate NOB*	Mean (RR_{OB})	Std (RR_{OB})	*Failure rate OB*
France	0.319	0.046	0.197	0.200	0.040	0.134
Atalanta	0.391	0.063	0.269	0.352	0.033	0.240
Di-yuan	0.612	0.071	0.503	0.571	0.074	0.477
Dfn-gwin	0.612	0.071	0.503	0.312	0.062	0.296

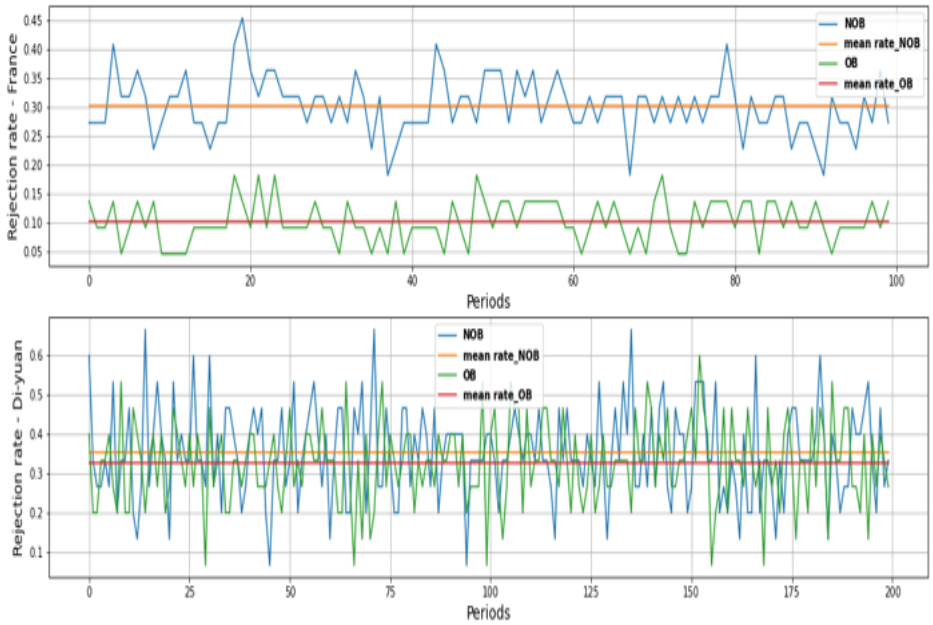
Table 4.3 – Simulation results - No Protection Setting

Network	Mean (RR_{NOB})	Std (RR_{NOB})	*Failure rate NOB*	Mean (RR_{OB})	Std (RR_{OB})	*Failure rate OB*
France	0.303	0.050	0.170	0.110	0.037	0.072
Atalanta	0.381	0.077	0.247	0.332	0.074	0.222
Di-yuan	0.499	0.070	0.372	0.525	0.057	0.375
Dfn-gwin	0.473	0.057	0.368	0.426	0.069	0.320

Table 4.4 – Simulation results - Protection setting



(a) The rejection rate dynamics in a "No Protection Setting"



(b) The rejection rate dynamics in a "Protection Setting"

Figure 4.6 – Rejection rate dynamics

4.4 . Conclusion

In this section, we presented a framework to study optimal resource orchestration as a tool to build resilient protection schemes in eDCs networks supporting SDN-SPG applications where a risk of cross-domain failure propagation is high. The class of failure we are considering is the power supply interruption of eDCs hosting critical networking application as VNFs. As demonstrated in Chapitre 3, ensuring power-supply-disjoint VNF placement may lead to better steady state availability. In this context, sharing eDCs resources between interdependent CIs has two main benefits. A first, long term benefit of reducing CaPEX resulting from expanding the eDCs network by installing new sites. The second benefit is short-term and concerns the ephemeral resource sharing scheme as a key to ensure high availability and avoid penalties resulted from service interruption. We studied the use case of planned eDC maintenance as a disruptive event. Critical services hosted in eDCs subject to a maintenance intervention due a power supply interruption, are pro-actively migrated to other reliable eDCs to ensure service continuity. A mixed integer non linear program was formulated to model the service migration process with respect to capacity, latency and availability constraints. We conducted simulations using real world network topologies. A propagation model was implemented to capture the dynamics of failure propagation. On top of it, an overbooking strategy is implemented with the objective of decreasing request rejection rate. Such approach might impact the QoS but mitigates failure propagation by ensuring the continuity of critical services characterized by some particular topological proprieties (significant betweeness centrality measure). A detailed study on the impact of such approach on the QoS and the formulation of the correspondent problem is in perspective of this work. We simulated a scenario where an information about critical eDCs in the network is available. eDCs with high criticality measure have very low failure probability. Compared to a no-protection scenario, the obtained results show a decrease in both migration request blocking and the impact of cascading failure. Thus, integrating eDCs availability information in the optimization framework as an input is crucial to ensure cross-domain, optimal orchestration. Such availability data must be shared in a continuous and secure manner in addition to eDCs' physical status data (computig capacity, interconnections, power supply data..) in order to achieve effective coordination. As a perspective for this work, the failure propagation estimation phase might be implemented to feed the optimizer with real time estimates of the network state. Also, a MPC formulation is expected to deal with dynamic optimization and changes in the environment.

5 - Trustful Resource Sharing

In previous chapters, we presented a cross-domain resilience strategy that relies on dynamic coordination between ICT and EPI operators based on virtual DCs resource sharing to guarantee the high availability of critical applications. Ensuring the active redundancy of these applications requires a continuous sharing of Life Cycle Management (LCM) data of the targeted applications between the current host and redundancy sites. However, sharing such data is subject to security, privacy, and sovereignty constraints. In this chapter, we study this problem in the framework of the data sovereignty concept which is an open issue in data-driven ecosystems and information systems management. More particularly, we propose a data and resource-sharing framework that exploits the convergence of International Data Spaces (IDS) principles and automation capabilities enabled by the SDN and NFV paradigms to guarantee trustful and proactive coordination.

5.1 . Challenges of Data Sharing in CIs Networks

Modeling and understanding dynamic interdependencies between ICT and EPI subsystems is key to mitigating the cascading impact of failures in SDN-enabled SPG networks and allows the adoption of proactive and sophisticated protection schemes. Indeed, CCPSs networks interdependencies are complex and the physical network is stochastic (subject to natural hazards, and the emergence of new states of operations). Thus, it is difficult to predict in advance the resources needed to stabilize the CCPSs's nominal operational condition in case of a disruptive event [111]. Also, this requires a continuous and real-time sharing of situational awareness data which is subject to several constraints, mainly trust, security, and sovereignty.

In the framework of European CIs, digital sovereignty is defined as the ability of a nation to control the digital infrastructure on its territory and the data generated from it. This concept comprehends the control over the digital assets hosting critical and valuable data [112, 113]. Whilst, the Data sovereignty, according to [22], is defined as the ability to determine who is allowed to access and use, and in which context, a data owner's data. This rush towards data is fueled by the advancements in artificial intelligence (AI) algorithms and big data analytics, and the opportunities in terms of business value creation and CIs resilience [114].

In the ICT domain, for example, the sixth generation of mobile telecommunication technologies (6G) is expected to be AI-driven. That is, the huge amount of data generated from the network elements can be processed and used to enable automation and self-organizing capabilities, improve QoS and security, and reduce OPEX [115]. From CIs interdependencies modeling perspective, data-driven approaches are gaining popularity due to their efficiency in overcoming existing physical, economic-based, and network-based models [116]. However, the multitude of heterogeneous data sources at the operational level brings additional overhead to data management and integration, in addition to real-time constraints of query handling in smart environments [117]. Overall, we summarize the main challenges to effective data sharing in CIs environments as follows :

1. **Sovereignty** : Creating value from the shared data, which in our case, has an objective of an enhancement of situational awareness, requires the use of a set of tools and computing resources to extract knowledge. In this context, ensuring data sovereignty refers to the ability to control how these tools operate on data at different levels (storage, collection, knowledge extraction, and usage). However, this is a difficult task, especially in dynamic and complex environments characterized by the heterogeneity, multi-tenancy, and sometimes conflicting objectives of interacting elements.

2. **Privacy** : CIs are majorly operated by private stakeholders who need to keep their business competitiveness. This prevents them from sharing information that may impact their economic status. In addition, private stockholders might want to keep control of their data by limiting who is eligible to exploit it and to what extent. This means that the data shared to enhance situational awareness shouldn't be exploited outside of that perimeter.

3. **Interoperability** : CIs operators manage different infrastructures from a technological perspective leading to an interoperability bottleneck. The underlying physical systems are heterogeneous in their operational procedures, timescale, and data management tools (different database systems, authentication, cyber security standards, and data integration tools). To deal with this issue, data brokers are required to ensure interoperability which might become hideous with the increase in the number of heterogeneous data sources. Thus, it is difficult to adopt a common resilience vocabulary during stress periods.

4. **Trust** : Operators are often reluctant when it comes to data sharing due to mistrust and privacy concerns. In the context of DCs resource sharing, trust can be viewed as the willingness of an operator to give privileges to another operator to deploy and run critical applications as a redundancy site.

5.2 . International Data Space Reference Architecture

5.2.1 . Overview of Data Space paradigm

The digital revolution of modern society has been a catalyst for the Industry 4.0 paradigm. This revolution is illustrated by the rapid growth of connected devices in the context of the Internet of Things (IoT), and the high reliance on cloud technologies to support communication, energy, and transportation services. Therefore, several protocols, standards, and tools have been developed to deal with huge volumes of heterogeneous data generated from a variety of connected devices.

From a data management perspective, the variety of data sources and formats requires the adoption of particular data integration tools for each class of data source [118]. This hindrance gave birth to the Data Space paradigm where the main objective is to overcome the limitations of traditional and domain-specific data management systems in dealing with heterogeneous data [117, 119]. This would prevent operators from investing in data integration tools, and enable fast data-driven service delivery. Moreover, a Data Space contains a set of rules and relationships between heterogeneous data from different sources and organizations. In Table 5.1, we provide a comparison between traditional Database Management System (DBMS) and Data Space concepts.

	Tradition DBMS	Data Space
Formats	Homogeneous	Heterogeneous
Scheme	Schema first, data later	Data first, schema later or never
Control	Complete	Partial
Leadership	Top-down	Top-down/Bottom up
Query	Exact	Approximate
Integration	Upfront	Incremental
Architecture	Centralized	Decentralized
Real-time data processing	No	Applicable

Table 5.1 – A comparison between the feature of traditional DBMS and the Data Space concept (taken from [74]).

The key differences between a traditional DBMS and a Data Space can be mapped into two dimensions from a data management perspective [120]. The first dimension is the *Administrative proximity* which refers to the degree of closeness between different data sources in terms of administrative control. The closest two data sources mean that they are managed by the same administrative entity (complete control as in the case of a traditional DBMS unlike the partial control of a Data Space), or at most coordinated administration by several actors. The level of administrative control over a group of data sources is a guarantee of consistency and permanence of the data management system, the closer the administrative control, the more robust these guarantees become. The second dimension concerns the *Semantic Integration* which is an indicator of the degree of matching between the schemas (types, units, names, and meanings of data) of different data sources. High *Semantic Integration* measure means that all the data conforms to a single agreed-upon schema, which is the case for a traditional DBMS. Whilst, a low High *Semantic Integration* measure indicates the non-existing of a unifying information schema which is the case for the Data Space paradigm. Overall, a Dataspace is a distributed data integration concept where a data producer (operator A) delivers its data to a data consumer (operator B) through an intermediary broker as indicated by the reference architecture depicted in Figure 5.1. The role of the federation entity is to provide services to ensure interoperability, security, and trustworthiness among the participants [121]. Some technical challenges of Data Spaces are being addressed in the research community. Namely, data models and querying, discovery, storage, indexing, and quality of answers guarantee [117].

5.2.2 . IDS Reference Architecture Model & Implementation

The International Data Space Association (IDSA) is a non-profit organization gathering numerous industrial actors with an objective of delivering a technology-agnostic, standardized, and Reference Architecture Model (RAM) description of a Data Space' distributed software architecture [122].

The architecture is divided into five layers : business, functional, process, information, and system. IDS participants are categorized into four categories and classified with respect to their role in the data exchange process [123]. In the business layer for example, we differentiate between core roles (data owner, data provider, data consumer and data user), and intermediate roles (identity provider, vocabulary intermediary, App store, and broker service provider).

A simplified architectural view of a data exchange involving the previously mentioned entities is illustrated in Figure 5.1. Note that, for taking part in the

Data Space, a per-role certification is required for the entity that desires to take part in the data exchange. In what follows, we provide a description of the main roles in the IDS architecture [1] :

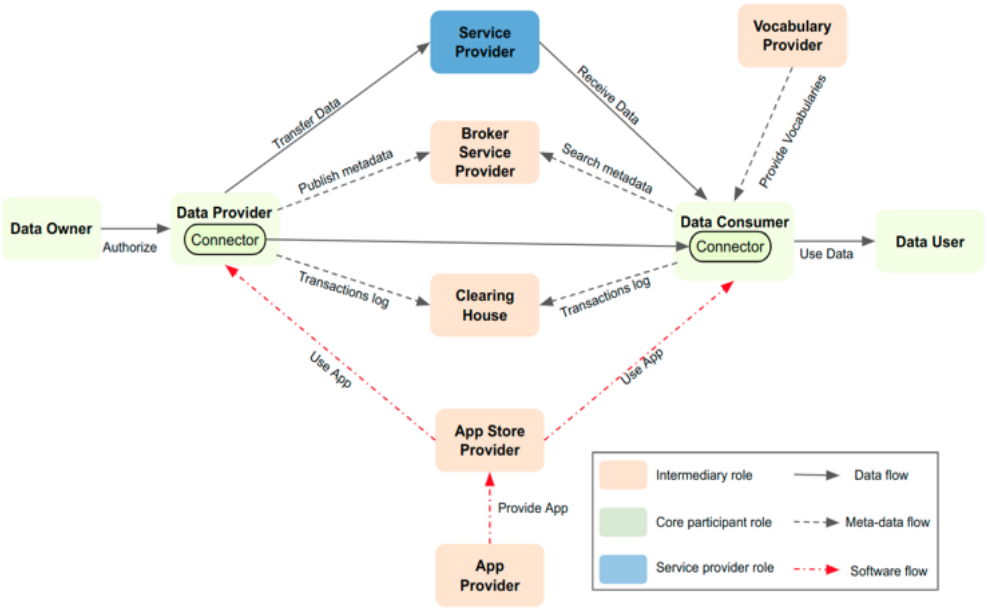


Figure 5.1 – IDS Reference Architecture Model.

- **Data Owner / Provider** : these roles can be assumed by the Data Supplier role. A Data Supplier induces data into the IDS ecosystem and assumes the roles of : Data creation (generating data from a sensor or accessing a system's logs for example), Data ownership (defining data usage contracts and policies), and Data provision (transmitting the data to the Data Customer).

- **Data Consumer / User** : these roles can be assumed by a single entity : a Data Customer which receives data from a Data Provider. If a the data is being processed by a third party service (Service Provider), then the Data Customer is both a Data Consumer and Service Consumer.

- **Broker Service Provider** : To enable data request from Data Customer, a Data Broker service is deployed by managing metadata about the information to exchange in the IDS. Thus, the Data Broker provider is assumed to fulfill the responsibilities of a Service Broker as well. This entity stores and manages information about the data sources available in the

1. The details can be found in https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0

IDS. Also, the metadata model is specified by the IDS information model along with the interface between the broker and the Data Consumers.

- **Service Provider** : this entity receives data from Data Provider and apply a transformation (data analysis, integration, cleaning...). Note that, in a IDS, data can be routed through several Service Providers. The output of the data transformation can be returned to the Data Provider or transferred to the Data Customer. Service provisioning is performed through apps that are installed in the IDS connector which can be developed by the participants or provided in "as a service" style by third party participants.

- **Identity Provider** : this entity provides services to manage identity creation, monitoring and validation for the participants. It consists of a certification authority, a dynamic attribute provisioning service, and dynamic trust monitoring service for authentication purposes.

- **Vocabulary Provider** : provides and manages vocabularies (ontologies, data models, metadata elements) which enable domain knowledge about the data assets and ensure machine readability and interoperability of the data.

- **Clearing House** : this is the main logging component which provides transactions recording for billing and quality of service analysis. After a data exchange, both the Data Provider and the Data Costumer confirm the data transfer by logging the operation's details. The logging information can be used to debug data exchange issues and resolve conflicts (for example, a data package is missing).

- **App Store Provider** : The App Store is responsible for distributing data apps. That is, data apps are downloaded to the IDS connector of the App Consumer (Data Provider/Customer or Service provider). Note that, a data app could be sensitive, hence it should be stored in the App Owner's premises. To this end, the App Store may comprise the role of App owner which has the app license.

The IDS defines a procedure to incorporate trust into data sharing, still, we need a digital infrastructure that hosts the tools to process and ensure data exchanges in *as a service* style. To fill such need, the Gaia-X project was launched in 2019 with the aim to provide data and infrastructure ecosystems to facilitate data sovereignty, trust, interoperability, and portability among participants [22]. The two ecosystems are linked via a set of federated services as

illustrated in Figure 5.2. These federated services refer to a network of data-related applications provided by various organizations participating in the data-sharing ecosystem. A detailed definition of this concept in the context of multi-domain network service provisionning is provided in [124, 125]. In the infrastructure ecosystem, services are provisioned, connected, or consumed as well as in the data ecosystem where the data, managed by the services, is the main asset. Overall, Gaia-X plays the role of an orchestrator and integrator in a cloud-native style.

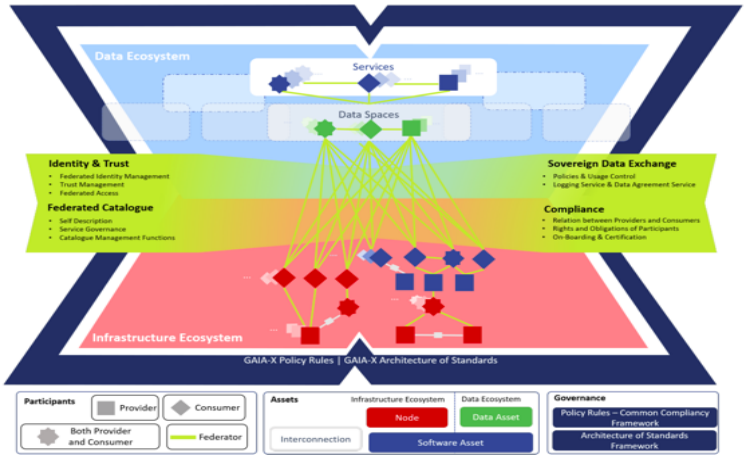


Figure 5.2 – Gaia-X architecture taken from [22].

A Gaia-X participant is whether a *Consumer*, *Provider*, or a *Federator*. A *Consumer* is a participant that uses the service offering provided by a participant of type *Provider*. A *Service instance* includes self-description and technical policies uses different infrastructure resources, and it possesses different assets. Finally, a *Federator* is responsible for providing federation services which are the core components of Gaia-X. These services belong to one of the four groups : Identity and Trust, Federated Catalog, Sovereign Data Exchange, and Compliance, covering all the possible interactions between participants, resources, assets, and policies in the ecosystem.

A logical mapping between the concepts of IDS and Gaia-X architectures, results in a number of intersections. That is, the IDS *Service Provider*, *App Provider*, and *Identity Provider* could be hosted in the Gaia-X infrastructure ecosystem. Also, the data ecosystem in Gaia-X could host *Data Provider* and *Data Consumer* roles in the IDS architecture [126]. Specific features of Gaia-X, mainly the federation services, are essential to enable interactions between the aforementioned roles. For example, when referring to Figure 5.2, a Data Provider application (blue square) in the data ecosystem uses federated services

(green line) to securely connect to a Gaia-X Service Provider in order to allow and control data (green square in the data ecosystem part) usage by a Data Consumer. This latter mapping is essential in the context of this work as it shows the convergence between the IDS architecture components and cloud-native service provisioning, and provides some insight into the design of a coordination framework for cross-domain resilience as it will be described in section 5.3.

Nevertheless, we still need to specify the technical tools to implement the IDS components in a cloud-native style to tackle real-world scenarios. In this context, several open-source projects are available with the objective of providing software implementation of the IDS Connectors and are summarized in Table 5.2. From which, the Eclipse DataSpace Components (EDC)[1] is an open-source project developed by the Eclipse Foundation providing a set of features (code, samples, and architectures) that align with the requirements of Gaia-X and IDS reference architecture model. The EDC is developed in *Java* using *Gradle* build tool, and it also includes a repository to set up a minimal viable Data Space in order to support technical adoption and onboarding of applications. Other open-source projects : Pontus-X[2], TRUE[3], TRUSTED[4], and Data Space Connector[5] are presented in the table. We focus on five main attributes : **usage control** to ensure sovereignty, **Identity Management** to ensure trust and security, **Data Model** to ensure interoperability, the **Architecture**, and the **implementation technology**.

We can observe from Table 5.2 that the IDS Information Model [130] is widely adopted by various implementations. Also, the adoption of containerization technology to run different services and data applications paves the way to flexible and effective service management using de-facto cloud-native orchestration software like *Kubernetes*. This latter observation is developed in table 5.3 below, where we show how the cloud-native management and IDS paradigms converge to tackle data exchange challenges in multi-domain CCPSs networks. Starting with the interoperability challenge, the IDS information model being adopted by the various real-world implementations, and the standardization of NFV-based operations in cloud-native environments, allow the ICT and EPI operators to exchange data at their virtualized layer easily. In addition, identity management in IDS environments reinforces the trust between participants in the data-sharing process by fixing rules and policies for data accessibility. Moreover, the automation brought by the cloud-native ma-

1. https ://projects.eclipse.org/projects/technology.edc
2. https ://github.com/deltaDAO/mvg-portal
3. https ://github.com/Engineering-Research-and-Development/true-connector
4. https ://github.com/Fraunhofer-AISEC/trusted-connector
5. https ://github.com/International-Data-Spaces-Association/DataspaceConnector

Project	Implementation Technology	Architecture	Data Model	Identity Management	Usage Control
EDC	Modular components built with Java programming language and Gradle	follows guidelines of Gaia-X architecture	Data model is based on the IDS Information Model.	Each participant is assigned a Decentralized Identifier (DID) and a Verifiable Credentials (VCs). In case of a centralized identity management authority, the credentials are verified by querying the authority. In a decentralized identity management, copies of a participant's VCs are shared among all other participants.	Data usage policies are based on Open Digital Right Language [127].
Pontus-X	Blockchain-based technology built on Ocean protocol using Ethereum Virtual Machine (EVM).	The architecture is based on Gaia-X ecosystem.	The usage of Ocean protocol allows to access data statically and dynamically and also enables the "compute-to-data" concept where computation is performed without accessing data.	Role-based Access Control and fine-grained permissions.	Usage terms are defined in *Smart Contracts* recorded in the blockchain, and automatically executed if an agreement is present between the resource provider and consumer.
TRUE	The connector can be accessible and configurable using APIs (REST) and protocols (HTTP, HTTPS, Web sockets..)	The architecture is based on three components : an Execution Core Container (ECC) for data exchanges within the IDS ecosystem, a Backed Data Application (BDA) fro data generation and usage, and a data Usage Control Application (UC) .	Data model is based on the IDS Information Model.	Identity management is ensured using IDS Dynamic Attribute Provisioning Service (DAPS). Various rules can be applied to data access : time-based interval, spatial(location)-based, purpose-based, and complex rules.	Usage of IDS Usage Control language via a REpresentational State Transfer API for getting, uploading, and deleting contract agreements.
Trusted	A platform built using *Spring Boot* for industrial IoT applications using *Apache Camel* for secure communication between connectors and *Docker* and *Trustme OS* for environment containerization.	The architecture is composed of a *Core Container* and Application containers with a support to data flow and usage control among connectors.	Data model is based on the IDS Information Model.	Each participant is assigned a unique identifier which is used by a DAPS to generate a Dynamic Attribute Token. This token is used to access data resources.	*LUCON* policy framework is used to control data flows between connectors by assigning a flow rule (conditions under which the policy is applied), and a service description (specify the services to which the rule is applied) to each data resource.
DS Connector	Modular component containerized using *Docker* and can be accessed using a RESTful API.	IDS Reference Architecture Model (RAM).	Data model is based on the IDS Information Model.	Use of Public Key Infrastructure (PKI) where a centralized authority, via a *Dynamic Attribute Provisioning Service* manages participants certificates.	Data usage policies are written in IDS User control Language based on Open Digital Right Language.

Table 5.2 – Data Space Connector implementation projects, a detailed view can be found in [128] and [129].

nagement of critical applications' LCM reduces human intervention, and thus, the risk of violation of data access rules is minimized which increases privacy. Finally, ensuring data sovereignty is done by hardening data usage control policies which, thanks to the flexibility of cloud-native management, can be updated and adapted to different situations.

Challenge	Description	Opportunity
Interoperability	Different virtualization technologies and service life-cycle management (LCM) tools.	Critical services virtualization following common NFV standards, and the shift toward COTS hardware, facilitate the coordination of LCM operations in heterogeneous CIs domains.
Trust	Uncertainty about the willingness of other parties to fairly collaborate and share their data	Identity management procedures can be managed effectively using cloud-native technologies.
Sovereignty	The use of mistrusted tools and platforms or data sharing and processing	IDS Usage Control Language based policies can be managed and adapted flexibly and on(-demand thanks to cloud-native management .
Privacy	Business competitiveness prevents an operator from sharing its data that could be used out of the shared resilience context.	The limitation of human-intervention by exploiting the automation tools powered by cloud-native management reduces the risk of rules violation and harden the established, agreed-upon policies.

Table 5.3 – The added values of Data Space paradigm combination with NFV-SDN characteristics to solve information sharing bottlenecks in multi-operators environments.

5.2.3 . Data Space use-cases

Several use-cases have been developed in different sectors to exploit the benefits of Data Space in order to build common data ecosystems to foster collaboration, innovation, and interoperability. Some examples of such use-cases are :

- **Telco Data Space :** the aim of a *Telco Data Space* as the one initiated by the TM-Forum [131], is to demonstrate the need to new data sharing mechanisms between Communication Services Providers (CSPs) in order to enable new business use-cases and innovate new services for customers. The data sharing mechanisms should be automated and respect the trust, privacy, and sovereignty requirements. Several use-cases are developed. As an example of use cases, we identify RAN energy saving based on resource sharing between ICT operators [132].

- **Energy Data Space :** the current transition of the energy sector characterized by the high penetration of renewable energies and the emergence of micro-grids and electrical mobility, led to an increased complexity into power network management that could be reduced by sharing data between different stakeholders through the *Energy Data Space*. A use case is developed in the field of predictive maintenance applied to wind farms, where the plant operator, maintenance service provider, and component supplier share different data to optimize their workflow in a trustful and interoperable way [133].

The migration of both the telecommunication and energy networks operators towards the same, standardized cloud-native management of their control applications, opens new opportunities for cross-domains resilience if data of the two domains can be accessed and interpreted easily. In the next sessions, we propose a use-case of cross domain resource orchestration based on a Data space in order to guarantee high application availability through on-demand redundancy.

5.3 . Use-case : IDSA-based Data Exchanges for Effective Cross-Domain Resilience in Interdependent ICT and EPI Networks

We propose to study a use-case of DCs resources sharing to ensure high availability of cloud-native applications. ICT and EPI operators must continuously share state data which is used to assess the risk of a DC power outage or a communication service interruption. Once the risk is assessed, an ephemeral redundancy scheme is created for services with high interruption probability. This scheme is determined through the optimal mapping presented in Chapter 4. In what follows, we present the set of data that could be shared considering current practices in virtualized functions migration as specified by standardization entities [134]. Also, we detail how the convergence of the cloud-native and Data Space paradigms can be leveraged to trustfully exchange data necessary to ensure cross-domain resilience.

5.3.1 . Design Principles : data set specification, and data exchange patterns.

Given that ICT and EPI operators are assumed to share situational awareness in the virtualized DCs infrastructure level, existing literature on multi-domain NFV services orchestration provides interesting insights and directives on choosing the minimal set of data required to perform the monito-

ring and migration of virtualized services while keeping a high level of privacy [135, 136, 137, 138]. Based on this, we identify two types of data to be shared between ICT and EPI operators at the virtualized DCs level : service-level (meta) data and VNF level data. The service-level (meta) data are gathered to assess the service availability and reliability attributes as the MTTF and MTTR for example. This data could be associated with meta-data of other services forming the network in order to quantify the impact of a service interruption on dependent services in the DCs network as well as the set of electrically-reliable DCs to be considered in the protection scheme. Non-functional data can also be associated with each participant in the data exchange process, an example is historical data of previous transactions assessing a trust level to the participant and its shared resources. In [**?**] authors present a *"Trust-by-Design"* concept to build cloud applications which can be trusted by the users. A set of trustworthiness evidences and metrics are presented among which : the re-use of already trusted software components, the .In addition, information about available capacity in DCs, network latency, and service connectivity are required to compute the optimal mapping in Chapter 4. Once the risk of failure propagation is assessed, an ephemeral redundancy scheme is created and VNF-level data are used to instantiate the application VNFs in selected hosts. An example of such data is a VNF Descriptor (VNFD) which specifies a VNF's required compute, storage, and networking resources, LCM data like auto-scaling policy, and affinity and anti-affinity rules.

Data exchange patterns refer to the possible architectures of request and sharing requests handling process. In our use-case, relying on one centralized authority to "fully" manage cloud-native services spanning EPI and ICT domain is not a feasible solution as it assumes that an operator will federate its own infrastructure management to a third party which is unrealistic. In this circumstances, adopting a fully decentralized, Peer-to-Peer (P2P)-based cooperative NFV framework seems to be an viable pattern. From NFV-resource sharing, existing work from the literature has demonstrated the feasibility of hierarchical, P2P multi-domain NFV resources orchestration [139, 138]. From trust and sovereignty perspective, blockchain-based identity and data usage-control management solutions are also proposed to deal with trust management [32, 137]. However, distributing functionalities of data usage control, identity management, and authorizations may introduce network overhead in terms of resources needed by each participant in the network to validate and prove the compliance of other participants in the network. Consequently, a hybrid approach where the monitoring of network status, and the management of identity and authorizations, can be federated to a centralized NFV-based entity. While the VNFs migration and active redundancy procedures are managed in a P2P network formed of different MANOs of considered DCs

spanning the ICT and EPI domains. In the following section, we specify the different operations handled by the centralized entity and the P2P network, and the different reference points between the elements and the interfaces that could be implemented following existing standards [140, 141].

5.3.2 . A Hybrid Framework for Trustful Coordination

In this section, we go through the steps to ensure dynamic virtual resources orchestration in the edge DC network spanning the power and telecommunication domains. The objective of the dynamic orchestration is ensure dynamic redundancy of critical services (EMS service for an EPI operator and SDN-C service for an ICT operator) and thus, achieve high availability. That is, the increasing demand for communication services, and the stochastic nature of service requests flows require the design of fast and robust service provisioning schemes. To this end, proactive resources provisioning in NFV environments has been studied in the literature as a promising solution to deal with dynamic flow fluctuations and resource constraints in the edge cloud [142, 143].

We make the assumption that the resource limitations present in the edge cloud, as well as the interconnections among various services in the NFV layer spanning the ICT and EPI domains, the CRO enables the sharing of edge DCs network resources as backups among ICT and EPI operators. Sharing resources between different operators is not a new trend, Radio Access Network (RAN) sharing is commonly performed between telecommunication operators with an objective to reduce costs and ensure high service availability. In [132], authors propose a reinforcement learning (RL) based collaborative framework allowing mobile operators to share their RAN infrastructure during low demand periods in order to reduce energy consumptions. The developed framework incorporates a distributed ledger technology (DLT) to share reports about the coordination performances. Indeed, resource sharing is key driver for innovation and resilience in multi-operator environments [144].

In order to achieve proactive failure recovery, VNFs placement is performed in two phases : first, predicting the availability of critical services, then, a reservation is made to instantiate standby VNFs as in an active-standby redundancy scheme. Predicting the availability of critical services in each node (DC) can be achieved using the current tools of life-cycle management (LCM) (active monitoring, health checks..) in NFV infrastructures [145]. These tools allow for example to detect issues at the hardware level (power supply shortage, disconnections..) and software level (request blocking, abnormal flows..).

In order to achieve network-level LCM, we build a hybrid framework com-

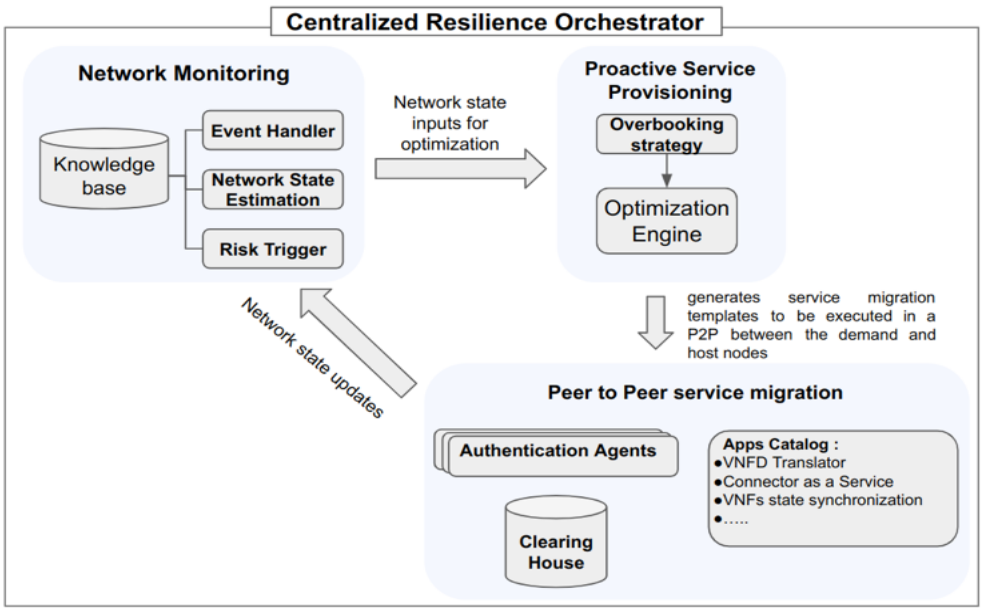


Figure 5.3 – Proposed architecture for the Centralized Resilience Orchestrator

posed of a centralized entity that we refer to as a the Centralized Resilience Orchestrator (CRO) for aggregating local information about the state of each edge DC in order to estimate the network status in case of a risk of failure propagation. The desired output to be monitored by the CRO is the service-oriented-availability of critical services in each node. In order to achieve such objective during stress events (failure propagation risk), dynamic resource orchestration is performed with respect to service level agreement metrics.

In Figure 5.3, a framework for managing risk events in the SDN-enabled smart power grids networks, is presented. High service availability is achieved through three main steps. First, an active monitoring of the network state (health checks, available computing resources for sharing per node...), depicted in the *Network Monitoring* block, is performed in an event-driven architecture style where a risk triggering agent is activated whenever an active redundancy scheme is required. Secondly, a *Proactive Service Provisioning* agent performs an optimal mapping between the set of demands for redundancy (standby backup instantiation) and the set of available DCs which form the redundancy scheme. Once the optimal redundancy scheme is computed, virtualized service migration is performed in the P2P network between the demand DC's MANO and the MANOs of chosen hosts. In general, from a modular view, the framework comprises :

- An **event handler** for receiving risk notifications from local management and orchestration (MANO) agents in each DC. For a DC hosting an

EMS instance, the notification is triggered if the EMS control or monitoring flows are delayed, which may cause a blind control situation of power substations in case of power demands fluctuations. Seamlessly, a SDN-C instance triggers the risk if the SDN-C is not able to auto-scale because of an abnormal power state of the DC hosting the SDN-C VNFs.

- A **network state estimation engine** in charge of local nodes' states aggregation and the calculation of failure propagation paths. This element's output is used by the optimization engine to perform the preselection of possible hosts to instantiate the standby backup of the critical services with high risk of failure.

- An **optimization engine** that implements the mapping between the set of requests and the available resources in the network. The mapping is performed with respect to latency, resource and availability constraints of the services.

- An **app catalog** containing apps that could be deployed at the orchestrator level or locally by the MANOs of each of the node involved in the peer to peer (P2P) service migration scheme. For example, an app for translating a VNF descriptor (VNFD) to enable VNF migration and instantiation between two platform using different orchestration technologies. In addition, VNF state synchronization can be provided in this catalog.

- **Authentication engine** that guarantees basic identification and security to lunch the service migration process between the demand node and the designated host in the P2P network.

- **Clearing house** for transactions recording where each migration operation is recorded to be analyzed and evaluated for future events.

5.3.3 . Proposed implementations of different interfaces between the CRO components

In this section, we perform a mapping between the components of the CRO and the roles of participants in IDSA and Gaia-X architecture. This qualitative approach allows us to propose guidelines and possible implementations of the interfaces between the different components based on existing IDS implementation presented in section 5.2.2 to integrate trust, privacy, and sovereignty into data exchanges process. In Figure 5.4 and Figure 5.5, we present the workflow diagrams of the monitoring and service migration operations, respectively.

Two main interfaces are present between the components of the CRO framework. The first interface is the network monitoring interface between the *Network Monitoring* module and the edge DCs' MANOs (EDC nodes in Figure 5.4). The implementation of such an interface could use the interfaces supported by the reference point *Os-Ma-NFVO* in the ETSI-NFV-MANO architecture [146]. Such reference point supports exchanges between the NFVO and the OSS to implement NS life-cycle management, fault management, and performance management. This requires the continuous sending of services status data in the form of events represented in the *Send_status_events()* call in Figure 5.4. Then a *Network State Estimator*, aggregates the status data of different critical services to build a unified situational awareness view and assess the risk of failure propagation via the *Verify_Risk_Threshold()* call to the *Risk Triggering* module. In case of the presence of a high risk of service interruption and failure propagation, a request to generate a new redundancy scheme for selected critical services (demand side), given a list of available DCs (Host side), is initiated through the *Demand_Host_List()* call to the *Optimization Engine* module. This latter module generates an optimal mapping specifying virtualized services migration patterns which is passed to the *Event Handler* via the *GenerateOptimalMapping()* call. The *Event Handler* publishes the notification of migration plans to each pair of demand and host nodes via the *Publish_P2P_MigrationPlans()* call.

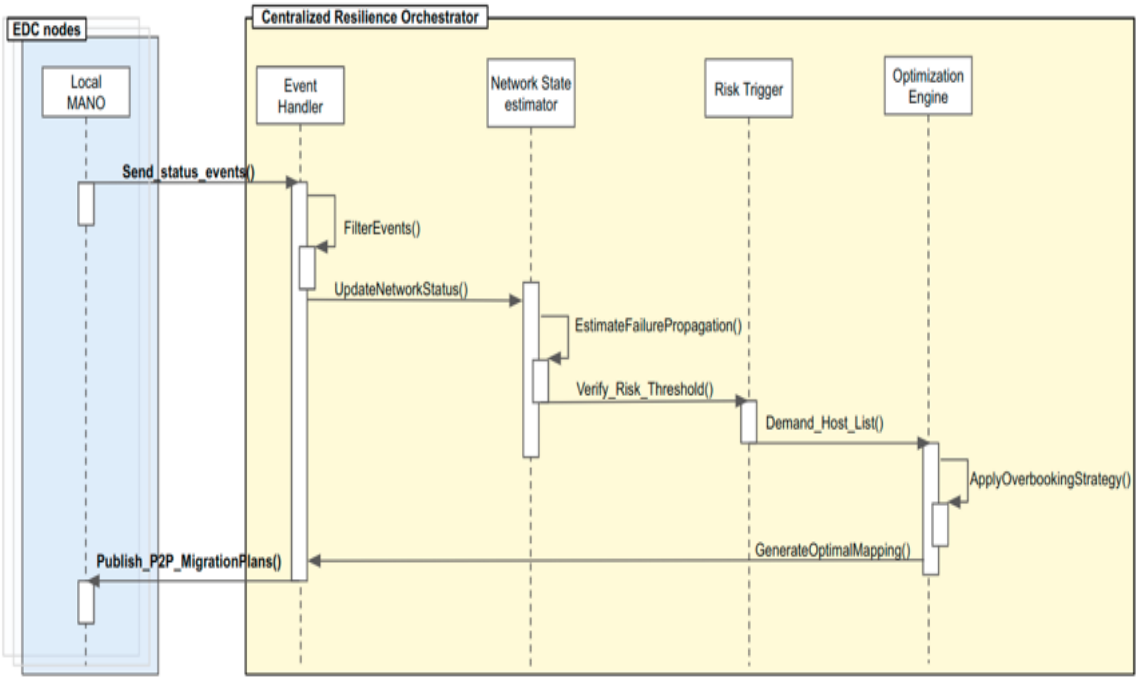


Figure 5.4 – Workflow for the monitoring of Edge-Data-Centers network services and the triggering of the dynamic redundancy scheme.

Once the targeted local MANOs are notified of the migration plan, the service migration process is initiated between the demand and host MANOs. In Figure 5.5, we present the workflow of the interaction between the MANO agent of the host node and the demand node. The CRO starts by notifying the *Demand MANO* of the migration plan initiation via the *Auth_Dmd_MANO()* call in order to obtain an agreement and confirm the adhesion to the sharing process via the *ConfirmMigration()* call. The same operation is repeated with the *Host MANO* via the *Auth_Host_MANO()* and *ConfirmHost()* calls. Between the last two calls, the *Host MANO* relies on a connector from the *App Catalog* required to process NS descriptors of other MANOs (**Data Consumption** role). Once the migration process is initiated, the *Demand MANO* requests a connector as well (via the *Request_connector()* call) to ensure the **Data Provider** role by adapting the data required to instantiate the service into an interoperable format in case the two MANOs use different virtualization technologies. An NS descriptor is generated via the *Generate_NSD()* call and then sent to be processed by the host via the *Send_NSD()* call. Once the service is instantiated in the location, the recovery of the demand DCs is initiated once finished a notification is generated via the *Recover()* call and a request to terminate the redundancy services is triggered via the *Terminate()* call. Finally, the operation is saved in the *Clearing House* via the *Save_transaction()* call, and the CRO is notified to update the network status via the *Notify_CRO()* call.

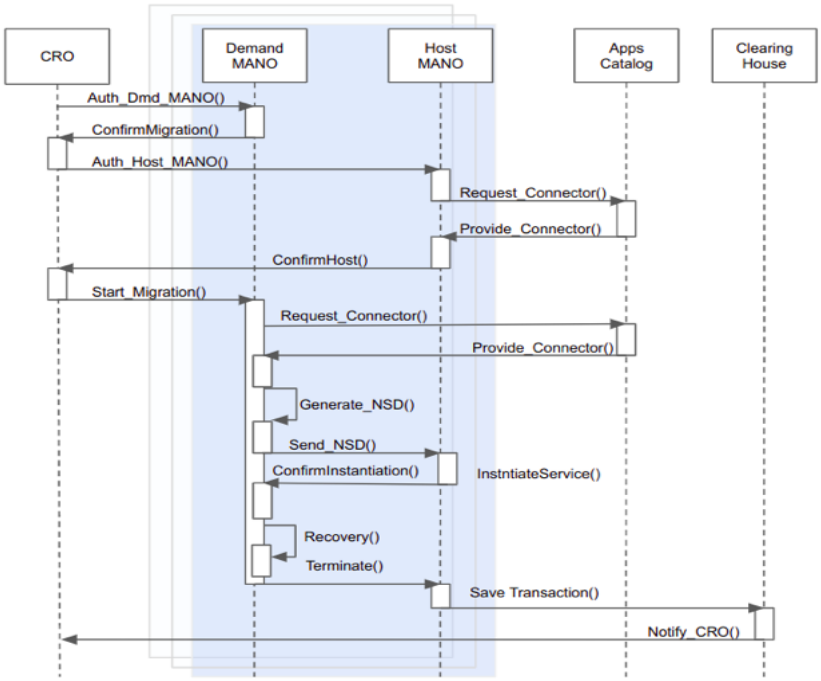


Figure 5.5 – Workflow for the Peer to Peer service migration process in the scope of IDSA architecture.

Note that, the CRO, through its authentication agents, ensures the peer-to-peer certificate generation. Also, it provides through the App catalog, connectors to ensure private and secure data exchanges. A node (eDC MANO) that requests an active redundancy scheme can be seen as fulfilling the **Data Provider** role of the IDS architecture. Whereas, the **Data Consumer** role is mapped to the host eDC that agrees to use its resources to increase the availability of demand's node services. The App catalog, Authorization, and Clearing House are considered as **Federated Services**.

5.4 . Conclusion

In this chapter, we reviewed the problem of information sharing between ICT and EPI operators from trust, privacy, interoperability, and security perspectives. We focused on the use-case of coordinated resilience in the cloud-native domain based on DCs resource sharing. First, we provided an overview of the main challenges preventing operators from sharing sensitive data. Then, we went through the Data Space paradigm in information management and the International Data Space Architecture whose objective is to establish secure, trustworthy, and standardized data exchanges between heterogeneous operators. We provided an overview of the IDS Reference architecture model along with the current state of the art of industrial implementations of this architecture. Afterwards, we presented a hybrid architecture composed of a centralized entity : Centralized Resilience Orchestrator, and distributed entities : Management and Orchestration (MANO) software of the DCs involved in the shared infrastructure between the EPI and ICT. In addition, we presented the detailed methodology to ensure resilient, and real-time orchestration of virtual resources as a response to fluctuating network state, and we performed a mapping between the different components of the proposed architecture and the IDS roles. Finally, as a future direction for this study, it would be logical to consider implementing a proof-of-concept. Additionally, it's crucial to focus on enhancing the efficiency of the data-sharing process to support sustained collaboration. This can be accomplished by optimizing the collaboration infrastructure (CRO) to accommodate diverse requests, ensuring that multiple participants can exchange data and services reliably and efficiently. Furthermore, the design of the P2P data exchange protocol should address the challenges posed by large-scale communications. Finally, specifying a pricing model of services provided between the participants involved in the data exchange environment would help stakeholders assess the worthiness of data and resource sharing from an economic point of view.

6 - General Conclusion

In this thesis work, we tackled the problem of CIs resilience in a era where cloud native technologies are increasingly integrated into the management layer of the cyber-physical systems networks providing the critical services essential for the socio-economic stability like telecommunication and power distribution services. The adoption of cloud-native technologies : Network Function Virtualization and Software Defined Networking, is due to their advantages in reducing the cost of services management, and enhancing the quality of services. However, this migration must go along with tools to assess the risk and vulnerabilities of such softwarized management paradigm on services' dependability. In addition, the presence of functional interdependencies between critical services of different domains might lead to cross-domain failure cascades with a risk of causing large scale service interruption.

We focused on two main interdependent services, telecommunication and power distribution. In the telecommunication domain, ICT operators are migrating towards the *Telco Cloud* where core communication functions are virtualized and run in a cloud-native style. This would pave the way to an efficient management of the infrastructure by reducing operational costs, enhancing the quality of service, and unlock new business opportunities through the support of new technologies like Industry 4.0, IoT, and Smart Grid. The second service we are considering is the power distribution in the framework of Smart power grid. More particularly, we focused our work around the monitoring and control applications that could be deployed in cloud-native style.

In Chapitre 2, we presented a conceptual framework of an SDN-enabled Smart Power Grid in order to study emerging interdependencies between ICT and power infrastructures at their cloud-native management layer. In this novel framework, control and monitoring applications of the power distribution network run as VNFs in edge data centers and rely on a programmable communication network to ensure data transport between the utility control center hosting the energy management systems and the controlled power substations. The communication network programmability is ensured by an SDN controllers hosted as virtualized functions in distributed edge data centers whose power supply rely on the reliable functioning of power substations. In order to study how failure propagates between different subsystems of the SDN-SPG, a failure mode and effect analysis was conducted to retrieve such events which would allow the design of effective protection mechanisms.

In Chapitre 3, a dependability evaluation was conducted to assess and

quantify the impact of different protection schemes in the virtualization domain on services' steady state availability. We presented a hierarchical modeling approach based on Stochastic Activity Networks to conduct the discrete-time simulations and test different protection scenarios. It turned out that increasing the redundancy of services in the virtualization domain by instantiating backup copies in other locations (eDCs) might not have a significant increase in availability if the eDCs composing the protection scheme are mutually dependent on the same power region. That is, the quantification of the impact of protection on services' steady state availability showed more gain in scenarios where the power supply of eDCs hosting backup copies relies on independent power substations.

In Chapitre 4, we tackled the problem of virtualized services orchestration in an eDCs network subject to power supply failure propagation. In order to proactively mitigate the impact of failure cascades, copies of virtualized services needs to be created in geo-distributed eDCs while satisfying performance (latency) and availability constraints. We formulated an optimization model with the objective to minimize the protection scheme cost where a multi-level placement strategy is computed to satisfy the availability requirement. To deal with the resource shortage which characterizes edge cloud environments, we studied the impact of overbooking on the rejection rate of requests to migrate services. As a perspective, this analysis can be extended in the framework of model predictive control where real-time estimation of the network state in terms of failure cascade vulnerability is dynamically associated with services placement optimization during disruption events.

The aforementioned network state estimation and service orchestration is only possible in the framework of cross-domain, coordination-based resilience. In this context, ICT and power operators must continuously share some information about the availability of their services in order to proactively respond to disruptive events. Chapitre 5, we studied the problem of information sharing from a data sovereignty perspective. We pointed out that data sharing between operators is subject to sovereignty, privacy and interoperability bottlenecks. To deal with it, we studied the convergence between the cloud-native paradigm benefits in terms of automation and the concept of DataSpace as an enabler for secure and effective, real-time data sharing. We presented a hybrid framework allowing the local orchestrators of virtualized eDC to communicate and share resources during the protection scheme building phase. We specified how each component involved in the protection scheme design is mapped to DataSpace reference architecture components in order to guarantee sovereign, secure, and interoperable coordination.

A - Paper A

Dynamic Orchestration of Communication Resources Deployment for Resilient Coordination in Critical Infrastructures Network

Khaled SAYAD[1,2] , Benoît LEMOINE[1], Anne BARROS[2], Yi-Ping FANG[2] , Zhiguo ZENG[2]

[1]*Dept. of Infrastructure Innovation and Engineering, Orange Labs Networks, 2 Avenue Pierre Marzin, 22300 Lannion, France*
E-mail: firstname.lastname@orange.com
[2]*Chaire Risk and Resilience of Complex Systems, Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, 3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France*
E-mail: firstname.lastname@centralesupelec.fr

In modern Critical Infrastructures (CIs) network, Smart Grid (SG) and Information & Communication Technology (ICT) infrastructures ensure security, as well as economic and societal well-being through a variety of services. Modern CIs rely on the fifth generation of mobile communication (5G) paradigm to incorporate new technologies, deliver new sophisticated services and adopt new business models. These models will shift the CI interdependencies towards a new dynamic paradigm where communication resources are deployed within the CIs operational scheme to reach performance and quality of service (QoS) objectives. Network Function Virtualization (NFV), Network Slicing (NS) and Software Defined Networking (SDN) are examples of 5G-enabling technologies used to reach the aforementioned objectives. However, due to the complex nature of CIs and the interdependencies between their components, the shift toward a dynamic operational scheme will increase the vulnerability and exposure to risks, impacting the network resilience. This requires the design of new resilience frameworks that consider the heterogeneity, privacy and self-interest nature of CIs and guarantee reliability and QoS objectives in such a constrained and dynamic environment. To tackle the resilience problem, we propose a framework to dynamically coordinate and manage the deployment of communications resources, based on NFV. This framework will ensure the availability of services, meet performance objectives during disruptive events and overcome constraints of interdependencies and heterogeneity. To illustrate our approach, we formulate the case of maintenance operations as a disruptive event in ICT hosting SG services.

Keywords: Critical Infrastructure, Resilience, ICT, Smart Grid, QoS, 5G, NFV, Optimization.

1. Introduction

Critical Infrastructures (CIs) play a major role in ensuring a continuous and resilient flow of services like mobility, energy, banking and telecommunications in modern societies Rinaldi et al. (2002). A critical infrastructure is defined by The Commission of the European Communities as: *"an asset, system of part thereof located in Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."*. Thus, Smart Grids (SG), Information and Communication Technology (ICT), and Transportation represent a complex network of interdependent CIs with an active research community focusing on interdependencies modeling, resilience and risk management. Rinaldi et al. (2002),Breor (2018), Murić et al. (2014), Ouyang (2014).

On the other hand, the fifth generation of communication technologies (5G) Shafi et al. (2017) will be a key player in the design and delivery of new sophisticated services within CIs network. Ultra Reliable Low Latency Communication (URLLC), Massive Machine Type Communication (mMTC) and Machine to Machine (M2M) are examples of high performance technologies whose integration in current infrastructures is being studied through real world use-cases.Yu et al. (2017)

The 5G networking services are deployed following a Service Level Agreement (SLA) specifying the reliability requirements and Key Performance Indicators (KPI). During disruptive events, critical services reliability and availability are aspects to be preserved. The resilience objectives are detailed in SLAs and differ from one application to another 3GPP (2021).

The ICT infrastructure will be in charge of delivering such high performance networking services through 5G enabling technologies like Network Function Virtualization (NFV), Software

Defined Networking (SDN) and Network Slicing. The deployment of these technologies in CIs network will lead to a shift towards a new dynamic paradigm introduced by the massive softwarization of CIs network functions where critical services run within the ICT premises Afolabi et al. (2018).

According to the World Economic Forum global risk report WEF (2021), information infrastructure breakdown and cyberattacks are expected to occur more frequently and have a significant impact on critical infrastructures. Following these expectations, mitigating the vulnerabilities brought by the 5G softwarization paradigm is primordial to guarantee the resilience of critical services in the 5G era. Moreover, the interdependencies that arise from the complex nature of CIs network would hinder the recovery process which would impact the quality of service (QoS) and cause economic loss to service providers.

Dynamic orchestration of cloud resources is performed to ensure a scalable and elastic management of service delivery in cloud environments in case of increased service demand or the delivery of new services. Dynamic orchestration is also primordial for a rapid and effective response against disruptive events. When a failure propagation process is taking place, the orchestration objective is to optimally place the affected resource to guarantee the availability and mitigate the failure propagation to other dependent infrastructures. Applying such process in CIs network is a difficult and little studied topic in the literature that we propose to investigate it through this paper.

In this paper, we demonstrate that, in the 5G dynamic paradigm, we can achieve such an unified resilience by performing a coordination process based on resources availability information sharing to guarantee both, the continuity of service and fast recovery following disruptive events. Our approach overcomes the heterogeneity of CIs and allows sharing resources in a dynamic and optimal scenario which would make resource allocation less complex and avoid additional costs. To illustrate our approach, we study the use case of maintenance operations in data-centers hosting CIs services. The ICT infrastructure deploy data centers to host Smart Grid applications. We use an architecture inspired by the one introduced in Cosovic et al. (2017) to develop a resilient virtualized infrastructure. We specify also, using Network Slicing (NS), Smart grid functions to be virtualized, namely, Smart Metering (SM) and State Estimation (SE).

This paper is organized as follow : in section 2, we highlight the problem targeted by this paper and introduce our approach. In section 3, we present related work about the use of 5G technologies in critical infrastructures. Then, we review the special case of maintenance operations in softwarized environments and it's impact on the QoS. Finally, we review some resource orchestration frameworks used in cloud environments. In section 4, we tackle the first problem of how to assess the resielence of 5G enabled critical infrastructure. Then, 5G enabling technologies and architectures will be presented. In section 5, we present our reference architecture used to host various CIs services with a focus on SG applications. A multi objective optimization framework is formulated to ensure the dynamic orchestration and resilient protection schemes during maintenance operations. Finally, conclusion and perspectives of the work are given at the end of this paper.

2. Problem Statement

Heterogeneity, timescale, geographical distribution and operational scheme, are main characteristics of the CIs network. CIs are known to be self-interested and greedy in nature in order to maximize their benefits and minimize expenditure. This represents a bottleneck while designing a shared resilience schemes for such systems. In addition, interdependencies between CIs make the problem even more complex.

The current adoption of cloud technologies by critical services providers paves the way to a more exposure to cyber vulnerabilities as a result of the massive softwarization of critical services. Software upgrades are a class of maintenance operations considered as a disruptive event that can lead to service interruption and downtime and therefore impacting the QoS. Moreover, the complexity of CIs represents a bottleneck toward achieving an optimal resource allocation during maintenance operations of interdependent infrastructures, due to the aforementioned characteristics. Traditional resilience schemes like resource redundancy are not effective because of the overwhelming deployment cost and complexity.

Orchestrating software maintenance operations in CIs while dealing with interdependencie and privacy constraints is a complex task. A trade-off between cooperation and self-interest should be considered while designing a coordination framework involving heterogeneous CIs.

3. Related Work

First, we review the use of cloud technologies in CIs. Then, we investigate a class of disruptive events in the new cloudification paradigm. We focus our study on maintenance operations of softwarized services. Finally, the application of multi-objective optimization for dynamic orchestration is investigated.

Critical services in modern infrastructures are increasingly immigrating to the cloud in order to enhance the QoS, decrease operational costs and guarantee a better response to dynamic changes

in services demands. The services are deployed as software instances in commodity off the shelf (COTS) hardware managed by the ICT infrastructure. The availability is defined as the readiness to deliver the critical services in compliance with the service level agreement (SLA). Reliability is defined as the ability of delivering the required services in a time interval Heegaard et al. (2015). In the literature, The term *Dependability* which encompasses the concepts of : Availability, Maintainability, Security and Reliability is commonly used when dealing with critical services resilience in softwarized environments Avizienis et al. (2004). In Niedermeier and de Meer (2016), a comparison between a traditional and a virtualized Smart Metering (SM) platform in SG have shown an interesting enhancement in reliability. In Vizarreta et al. (2018), a software defined network (SDN) controller maturity model is developed using historical release data to construct a stochastic model based on software reliability growth (SRG) to predict software failures occurrence during the testing phase.

Maintenance interventions in data centers are performed periodically in order to meet the growing customers demand, propose new services and correct software errors. Therefore, ensuring resilient services and achieving scalability Brewer (2001). The upgrade operations is an example of such interventions that present some resilience challenges like down time, data loss and even errors in the upgrading operation itself as explained in Dumitraş and Narasimhan (2009), which might cause QoS fluctuations and violation of the SLA Neamtiu and Dumitras (2011), and further lead to an escalating failure propagation due to the interdependencies between CIs. The reader is invited to take a look at Dumitraş and Narasimhan (2009), Neamtiu and Dumitras (2011) and Gramoli et al. (2016) for an in depth study of upgrades operation in large scale softwarized environments.

Industrial networked systems with limited computing resources are exposed to various cyberrisks. The problem of resource allocation can be treated as a multi objective optimization problem where nodes of the network cooperate to minimize failure propagation, fasten the maintenance operations and ensure a minimum continuity of service and therefor the resilience of the network. In Chantre and da Fonseca (2018), reliable facilities placement using failure probabilities was applied to edge devices placement to provision reliable broadcasting services. The framework was inspired by the Capacitated Facility-Location Routing Problem (cFLP) Melkote and Daskin (2001) where a subset of available facilities is chosen to fulfill dynamic service requests. In Cao et al. (2020), an optimal and reliable deployment of edge devices in 5G networks is achieved using many-objective evolutionary algorithm (MaOEA) to solve a Mixed Integer Programming (MIP) problem. The objective is to minimize cost of deployment, latency, failure probabilities and energy consumption of edge devices.

4. Resilience Assessment in 5G-enabled Infrastructure

The assessment of service resilience in the ICT infrastructure is crucial to mitigate the effect of failures in modern CIs network. Failure sources range from natural disasters to cyber-attacks and maintenance operations. In the 5G context, Management, control and operation functions are implemented as software in virtualized environment. We assume that, software failures occurrence trigger the need to maintenance intervention. Software upgrades are a special case of these interventions. To perform major upgrade operations, operators tend to shut down the concerned facility during the process leading to service interruptions and downtime. Thus, predicting the occurrence and impact of maintenance intervention will enhance the resilience of CIs network. A Software Reliability Growth Model (SRGM) can be used to perform such predictions and model failures occurrence dynamics. SRGMs are classified based the frequency of model testing into S-shaped and concave. In S-shaped models, we assume that failure intensity detection pace is slow at the beginning and improves as the test phase progress to reach a peak before decreasing. An example of such model is the Generalized Goel-Okumoto model Goel and Okumoto (1979):

$$\mu_{GGO}(t) = a(1 - e^{-bt}). \tag{1}$$

Concave models are exponential models assuming that the peak appears at the beginning and start decreasing exponentially. An example of such model is the Musa-Okumoto logarithmic model Musa and Okumoto (1984):

$$\mu_{GOL}(t) = a.ln(1 + bt). \tag{2}$$

Where $\mu(t)$ represent the mean number of failures at a time t. In Eq. (1) and Eq. (2) the parameters a and b are learned from historical data of failure apparition in different software releases.

4.1. *5G Enabling Technologies*

Network Function Virtualization (NFV) and Software Defined Networking (SDN) are two concepts designed to shift from a traditional, hardware-dependent network management towards a modern, software-based management. The softwarization concept aims to reduce costs of Capital and Operational expenditure by leveraging standardized common COTS hardware.

4.1.1. *Network Function Virtualization*

NFV is based on the concept of virtualized network functions (VNFs). Network function are implemented as software instances is a standardized hardware. To deliver an end to end service, distributed VNFs are incorporated into a Service Function Chain (SFC). NFV improves the network scalability and elasticity to dynamic service requests and thus represents a solid framework to design a resilient network.

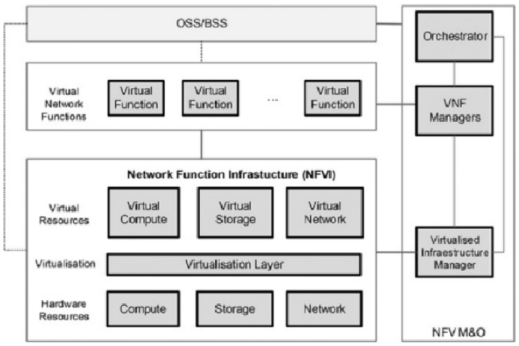


Fig. 1. NFV ETSI Architecture ETSI (2013)

As shown in Fig.1, the ETSI NFV architecture ETSI (2013) is composed of four building blocks: Management and Orchestration (MANO), VNF Manager, Virtualization Layer and Virtualized Infrastructure Manager (VIM). MANO is responsible for management and orchestration of software resources and virtualized hardware resources by attributing the necessary resources to deliver a service. VNF manager is responsible of the instantiation, scaling, termination of network functions and managing upgrades. Virtualization Layer abstracts the physical resources and assign VNFs to the virtualized infrastructure. VIM is responsible of managing the virtualized infrastructure by controlling its interaction with VNFs.

4.1.2. *Software Defined Networking*

In a traditional network, the control plane manages where to send an incoming packet. The data plane, on the other hand, performs the operation of forwarding the packets. As a result, the control and plane are superposed, that is, the data transport layer consists of nodes that are capable of forwarding data packets and learning and memorizing the addresses of other nodes simultaneously. However in the SDN paradigm, the control and data planes are decoupled. The control operations, learning and memorizing, are performed by a centralized controller that has a full overview of the data flow as depicted in Fig.2. SDN makes network control directly programmable via an open interface, while the underlying data transport nodes only forward the data packets.

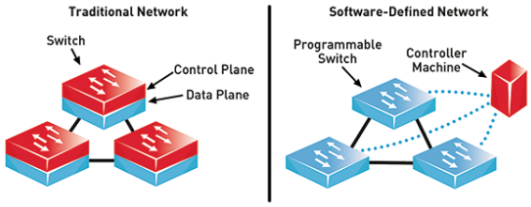


Fig. 2. Overview of Traditional and Software Defined-Network TECHNOLOGY (2021)

5. Use case : Maintenance of ICT

A maintenance scenario is depicted in Fig.3 OPNFV (2015) where different steps to be followed for a fast costumer notification and maintenance intervention, are represented. In this scenario, one of the servers dedicated to deliver a service to a consumer is planned to undergo a maintenance operation and therefore will be shut down. This service interruption propagates to affect other running VMs. The concerned consumer is notified by the VIM once the affected VM is identified. Consumer 3 in this case is informed about the maintenance process and switches to a standby VM. We propose to extend this use case by adopting an anticipation resilience mechanism based on information sharing. Using historical failure data, failure probabilities are calculated. Based on these probabilities, affected resources migrate to other infrastructure before the failure apparition. The migration process is steered by an dynamic optimization framework to optimally place resources with respect to cost, interdependencies and infrastructures capacity constraints.

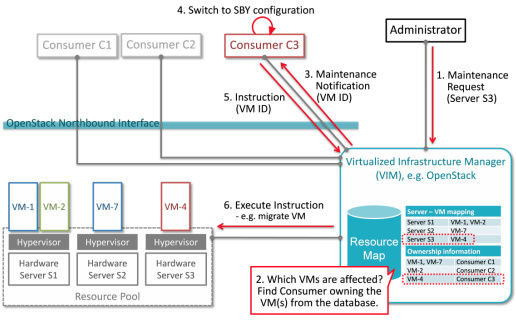


Fig. 3. Illustration of a maintenance use-case in a virtualization infrastructure OPNFV (2015)

We identify smart metering (SM) and State Es-

timation (SE) as potential functions to be virtualized. SE in SG is performed to extend real-time measurements due to the difficulty of implementing sensors in such environment. Available sensors measurements are treated to generate pseudo-measurements of the state of the SG. This type of applications requires low latency and high availability as in the URLLC standards to adequately fit the real data Cosovic et al. (2017). SM enables a real time monitoring of power generation and consumption. Smart meters are installed in residential areas of a city and allow, by transmitting consumption data, to real-time billing of power usage and propose new services by the service providers. SM requires a network capable of supporting large amount of connected devices and consumption data flows as in the Massive Machine Type Communication (mMTC) standards. Niedermeier and de Meer (2016).

5.1. *Resilient Infrastructure Architecture*

Our proposed architecture for SM and SE is based on ETSI architectures for NFV and SDN ETSI (2013). Field sensors measurements are transmitted to Points of Presence (PoP) which represents edge computing facilities. Depending on the service requirments, data may also be transmitted to Core Network (CN) data-centers. For example, SE requires low latency (ensured by URLLC). To this point, sensors measurements are only treated in PoPs. In contrast, for smart metering, CN and PoPs facilities are deployed to reach a trade-off between real time and long term services.

The exchange of availability information between CIs impacts the sensors data circulation and makes the data plane overloaded. We propose to use network coding on the transport layer to enhance the throughput of the network using a virtual network coding function (vNCF) Tan Do-Duy and Vazquez-Castro (2016). Fig.4 illustrates the softwarization paradigm where interdependent critical services of Smart Grid and other CIs run within ICT premises.

5.2. *Dynamic Resource Orchestration Based Resilience*

The use case presented in section 5 suggests that affected resources in an infrastructure are orchestrated before the maintenance intervention to guarantee resilience and continuity of service. This orchestration is anticipated based on degradation prediction of the 5G services. Dynamic resources allocation is performed considering sets of disrupted and non disrupted infrastructures. Non disrupted infrastructures cooperate to host the resources originally running in the disrupted infrastructures.

The URLLC and mMTC services provided to SG must have a high reliability. A dynamic protection scheme is thus calculated based on the

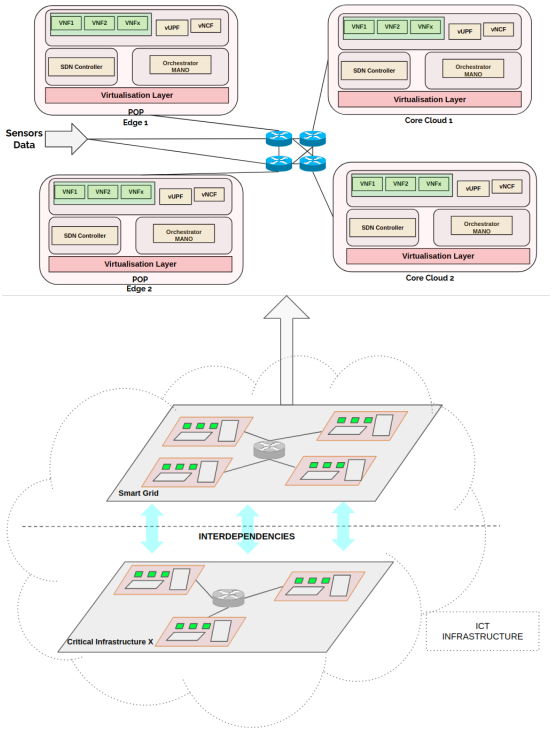


Fig. 4. Proposed architecture for the resilient virtualized infrastructure. Note that, the dependencies of ICT on other CI services are not represented. The virtualized services are hosted in private cloud owned by the SG operator

failure probabilities of hosting infrastructures. We assume that CIs have a uniform failure probability denoted q.

In a real case scenario, the switching from one service provider to another will introduce an additional data transport delay. We assume that the delay is smaller than the nominal delay guaranteed by an URLLC services (2-10 *ms*) Cosovic et al. (2017). A disrupted service is initially assigned to a CI fulfilling the cost, capacity and interdependency constraints. At the same time, a copy of the same service is assigned to back-up infrastructures.

This problem of reassigning critical services to available CIs considering cost and capacity constraints can be formulated as a capacitated reliable facility location problem Yu (2015). Critical services indexed by $k \in K$ in disrupted infrastructure $i \in I$, are hosted by a reliable infrastructure $j \in J$. k may refer to a VNF, a SDN controller or MANO. As depicted in Fig.5 below, we consider an example where $|J| = 3$ and $|I| = 2$. For $i = 1$, during the maintenace intervention, the demand of critical service represented by yellow is re-routed to the CI $j = 1$ with $j = 2$ as a

backup. The critical service represented by a green trapeze, initially fulfilled by CI $i = 2$ is re-routed to CI $j = 3$ with $j = 1$ as a backup.

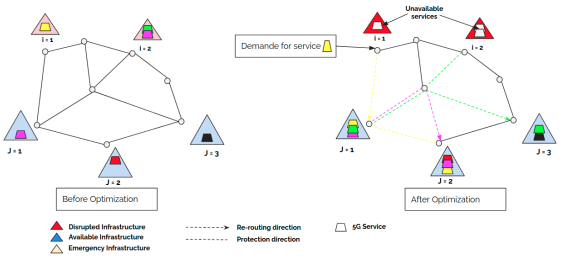


Fig. 5. Left: CIs network after the identification of failing CIs. Right: First assignment of disrupted services into available CIs.

We assume in our scenario, a hosting CI has two backups. If the primary assignment fails, critical services are ensured by the first backup. If the first backup also fails, we switch to the second backup. This is an adaptation of the level-r assignment strategy in classic cRFLP Yu (2015). In our case, cost and privacy constraints forbid a CI to share its services with a large number of other CIs.

We assume that the process has knowledge about resources distribution and availability status of CIs. Non-disrupted CIs may offer to share virtual resources based on the intensity of their interdependency with the affected CI. To this end, interdependence quantification metrics Casalicchio and Galli (2008) are included in the optimization process.

We define then the decision variables :

- $Y_{kijr} = \begin{cases} 1, \text{ service k of CI i is} \\ \text{ assigned to CI j at level r} \\ 0, \text{ otherwise} \end{cases}$
- $X_j = \begin{cases} 1, \text{ CI } j \text{ is slected} \\ 0, \text{ otherwise} \end{cases}$

We define also the process parameters :

- f_j: The cost of opening a CI j, represents the expense charged by a CI to allocate disrupted services in its computing infrastructure.
- κ_j : The available capacity of a CI j in number of computing resource units. An example of computing resource unit are virtual CPUs (vCPUs) or fraction of vCPUs.
- Λ_j : The cost of allocating one computing resource unit in CI j.
- c_{ki} : Computing resources demand in number of computing resource units by a service k of a disrupted CI i. This quantifies the required amount of computing resources. For example, SE requires more computing resources to treat data within a limited time-frame in order to ensure real-time estimations.
- $\tau_{kij} = \frac{T_j}{T_{ki}}$: The relative duration, which is a ratio between outage duration in two nodes, is used to measure the cascading effect from a disrupted service k in infrastructure i on a dependent CI j where T_j represents the duration of service unavailability in j caused by the failure of fraction of service (k, i).
- t_{ij} : The transmission time between two CIs i and j.
- θ_{ki}: The remaining time budget to transmit information for a service k from a CI i to a new hosting infrastructure after the failure apparition. For example, considering a SE application k where the CI i has a latency budget of $2ms$ to transmit data from sensors to the service k. If data transmission from sensors to CI i already takes $0.5ms$, then it remains $1.5ms$ to transmit data from CI i to another infrastructure hosting the service k after the failure.
- q_j: Failure probability of a CI j.

We assume that the optimization process is performed at a fixed time horizon where the parameters are stationary. The first step is to choose a subset of available infrastructures as candidates hosting CI. This is done based on provisioning cost, transmission time and the intensity of interdependence with of the hosting CI and the disrupted service. We formulate then the optimization problem:

$$\min_{X_j, Y_{kijr}} ECost(X_j, f_j, Y_{kijr}, \Lambda_j, c_{ki}, \tau_{kij}, q_j) \tag{3}$$

s.t. :

$$\sum_{j \in J} Y_{kijr} \geq 1 \tag{4}$$

$$Y_{kijr} \leq X_j \tag{5}$$

$$X_j, Y_{kijr} \in \{0, 1\} \tag{6}$$

$$(\theta_{ki} - t_{ij})\, X_j \geq 0 \tag{7}$$

$$\sum_{i \in I} \sum_{k \in K} c_{ki} Y_{kijr} \leq \kappa_j \tag{8}$$

$\forall \{k, i, j\} \in K \times I \times J$ and $\forall r \in \{0, 1, 2\}$.

The objective function Eq. (3) describes the Expected Cost (ECost) generated from the selection of a set of available CIs to host disrupted

services where each CI j has an opening cost f_j in addition to the cost of dimensioning in a hosting infrastructure where a billing system charges based on the amount of resources deployed to host the disrupted services. Note that, the amount resources is captured by c_{ki} and the correspondent sizing cost Λ_j. This objective also incorporates the expected cost of reassigning after the failure of the primary assignment. The dynamic allocation must fulfill the demand to host disrupted services while ensuring 5G performances. In our use-case, if a SE service is impacted in a CI i, it should be assigned to an available infrastructure j that can guarantee URLLC performances in term of latency. To ensure a reliable allocation, failure probabilities of a CI j denoted q_j are included. If the first assignment j fails, the demand is rerouted to a backup infrastructure with the higher reliability and so on. The choice of a hosting CI not only depends on meeting latency objectives but also the reliability requirements described by the failing probabilities q_j and the interdependency intensity τ_{kij}.

The constraint Eq. (4) forces the process to select at least one CI j to host a service k of a disrupted CI i. Constraint Eq. (5) forbids the assignment to an unselected facility. To highlight the binary nature of the decision variables, constraint Eq. (6) is added to the process. The selection of a set of hosting CIs j must respect the transmission time t_{ij} and the budget θ_{ki}, this is represented by the constraint Eq. (7). Finally, constraints Eq. (8) verify that the assigned demand doesn't exceed the capacity of the host.

We assume that a central decision making entity is operating on top of the CIs network. This entity has a holistic view of the state of each critical infrastructure and responsible for the optimal coordination process. However, it is more complicated in a real case scenario to ensure a continuous flow of critical information about the state of a CI due to privacy and security concerns. An example of these information are the aforementioned optimization process variables. Whereas, some parameters could be exchanged publicly like the amount of demand c_{ki} and sizing cost Λ_j, other parameters are confidential. An example of a confidential information are the location and number of computing nodes of a CI j which makes it difficult to estimate the capacity κ_j as well as the transmission time t_{ij} which depends on the network topology incorporating the disrupted CI i and the computing nodes of the hosting CI j.

In addition, due to strategic and business concerns, CI operators tend to hide the information about failure propagation and post-failure reports. This is problematic if one is trying to estimate the relative time τ_{kij} of cascading failure. The quantification of the interdependency is impossible as no information about the outage duration is available. The concern about the information sharing problem leads to rise questions about what information about the state of each CI is more relevant for the coordination process. Moreover, constrained by the availability of such data simultaneously, what is the minimum set of information that could be used to achieve an optimal CI coordination while respecting privacy and business constraints.

6. Conclusion and perspectives

In this paper, we tackled the problem of coordination in critical infrastructures network and highlighted the bottlenecks towards achieving such scenario. The flourishing of 5G enabled technologies in CIs paves the way to a new dynamic paradigm where critical services functions are hosted as software instances in virtualized environments, in the premises of ICT infrastructure. Even though this softwarization will make the network more vulnerable to risks, the unification of critical services delivery by mean of NFV and SDN, represents an opportunity to overcome the heterogeneity, privacy and greedy nature of traditional CIs while designing a coordination framework.

We argue that, in this paradigm, we can achieve a shared resilience scheme by anticipating maintenance interventions in CIs. Disrupted critical services are dynamically orchestrated to the computing facilities of available CIs to mitigate the effect of service interruptions and guarantee a continuity of service.

To illustrate our approach, we presented the use case of maintenance operations in a virtualized infrastructure hosting Smart Grid services. Maintenance operations cause fluctuations in service delivery which impact its quality. We propose a NFV/SDN based architecture to reach 5G performances required for the SG services. To design a resilient protection scheme, a multi objective optimization problem is formulated to overcome cost, reliability and interdependency constraints. However, developing such model is difficult due to lack of a transparent framework to share critical information due to confidentiality, security and concurrency aspects of CIs.

As a perspective to this work, the design of an information sharing framework to guarantee security, privacy and shared resilience of CIs, is envisioned. Also, on top of such framework, an implementation of the multi-objective optimization algorithm can be done to validate the robustness of the shared resilience scheme.

References

3GPP (2021). Service requirements for the 5G system. Technical Specification (TS) 22.261,

3rd Generation Partnership Project (3GPP). Version 18.1.1.

Afolabi, I., T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck (2018, 03). Network slicing & softwarization: A survey on principles, enabling technologies & solutions. *IEEE Communications Surveys & Tutorials PP*, 1–1.

Avizienis, A., J. . Laprie, B. Randell, and C. Landwehr (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 11–33.

Breor, S. (2018). Assessing critical infrastructure dependencies and interdependencies. In *Winter Simulation Conference (WSC)*, pp. 1–9.

Brewer, E. (2001). Lessons from giant-scale services. *IEEE Internet Comput. 5*(4), 46–55.

Cao, B., Q. Wei, Z. Lv, J. Zhao, and A. K. Singh (2020). Many-objective deployment optimization of edge devices for 5g networks. *IEEE Transactions on Network Science and Engineering 7*(4), 2117–2125.

Casalicchio, E. and E. Galli (2008). Metrics for quantifying interdependencies. Volume 290, pp. 215–227.

Chantre, H. D. and N. L. S. da Fonseca (2018). Multi-objective optimization for edge device placement and reliable broadcasting in 5g nfv-based small cell networks. *IEEE Journal on Selected Areas in Communications 36*(10).

Cosovic, M., A. Tsitsimelis, D. Vukobratovic, J. Matamoros, and C. Anton-Haro (2017). 5G Mobile Cellular Networks: Enabling Distributed State Estimation for Smart Grids. *arXiv:1703.00178 [cs, math]*.

Dumitraş, T. and P. Narasimhan (2009). Why Do Upgrades Fail and What Can We Do about It?: Toward Dependable, Online Upgrades in Enterprise System. In *Middleware 2009*, Volume 5896, pp. 349–372.

ETSI (2013). Network functions virtualization (NFV); architectural framework v1.1.1. Technical report, ETSI.

Goel, A. L. and K. Okumoto (1979). Time-dependent error-detection rate model for software reliability and other performance measures. *IEEE Transactions on Reliability R-28*(3), 206–211.

Gramoli, V., L. Bass, A. Fekete, and D. W. Sun (2016). Rollup: Non-Disruptive Rolling Upgrade with Fast Consensus-Based Dynamic Reconfigurations. *IEEE Transactions on Parallel and Distributed Systems 27*(9), 2711–2724.

Heegaard, P. E., B. E. Helvik, and V. B. Mendiratta (2015). Achieving dependability in software-defined networking : A perspective. In *7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, pp. 63–70. IEEE.

Melkote, S. and M. S. Daskin (2001). Capacitated facility location/network design problems. *European Journal of Operational Research 129*, 481–495.

Murić, G., D. Bogojevic, and N. Gospić (2014). Interdependencies of communication and electrical infrastructures.

Musa, J. and K. Okumoto (1984). A logarithmic poisson execution time model for software reliability measurement. In *ICSE '84*.

Neamtiu, I. and T. Dumitras (2011). Cloud software upgrades: Challenges and opportunities. In *2011 International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems*, pp. 1–10.

Niedermeier, M. and H. de Meer (2016). Constructing Dependable Smart Grid Networks using Network Functions Virtualization. *Journal of Network and Systems Management 24*(3), 449–469.

OPNFV (2015). Opnfv doctor project. `https://wiki.opnfv.org/display/doctor/Doctor+Home`. Accessed: 2021-03-24.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 43–60.

Rinaldi, S., J. Peerenboom, and T. Kelly (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*.

Shafi, M., A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder (2017). 5g: A tutorial overview of standards, trials, challenges, deployment, and practice. *IEEE Journal on Selected Areas in Communications*, 1201–1221.

Tan Do-Duy and M. A. Vazquez-Castro (2016). Network Coding function virtualization. In *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5.

TECHNOLOGY, J. (2021). Jerome software-defined networking.

Vizarreta, P., K. Trivedi, B. Helvik, P. Heegaard, A. Blenk, W. Kellerer, and C. M. Machuca (2018). Assessing the Maturity of SDN Controllers With Software Reliability Growth Models. *IEEE Transactions on Network and Service Management 15*, 1090–1104.

WEF (2021). World economic forum: Global risks report 2021.

Yu, H., H. Lee, and H. Jeon (2017). What is 5G? Emerging 5G Mobile Services and Network Requirements. *Sustainability 9*, 1848.

Yu, R. (2015). The capacitated reliable fixed-charge location problem: Model and algorithm. *M.S. thesis, Lehigh Univ., Bethlehem, PA, USA*.

B - Paper B

Towards Cross-Domain Resilience in Interdependent Power and ICT Infrastructures: A Failure Modes and Effects Analysis of an SDN-enabled Smart Power Grid

Khaled SAYAD[1,2], Benoît LEMOINE[2], Anne BARROS[1], Yi-Ping FANG[1] , Zhiguo ZENG[1]
[1]*Chaire Risk and Resilience of Complex Systems, Laboratoire Génie Industriel, CentraleSupélec, France*
email:firstname.lastname@centralesupelec.fr
[2] *Orange Innovation, France*
email:firstname.lastname@orange.com

***Abstract*—The adoption of cloud-native technologies like the Software Defined Networking (SDN) paradigm, into the management of Critical Cyber-Physical System (CCPS)'s monitoring and control functions, leads to the emergence of complex interdependencies between the cyber and physical domains, which would increase the risk of cascading failure, especially in the cyber-domain represented by edge Data Center (DC) networks. These Edge DCs host critical software services characterized by high dependability and performance requirements. The downtime of such services has a considerable impact that may destabilize socioeconomic well-being. In this work, we provide a failure modes analysis of an SDN-enbaled Smart Power Grid (SD-SPG) with a focus on the subsystems involved in cross-domain failure propagation. The objective of the analysis is to establish the causal effect between subsystem failure modes that may lead to cross-domain failure cascades. Then, we focus on the evaluation of Steady State Availability (SSA) metric under different interaction scenarios between the power and telecommunication subsystems. To this end, we propose a hierarchical modeling framework combining continuous-time Markov chains (CTMCs) and Reliability Block Diagram (RBD)s to capture both, subsystems and complex systems' steady-state behavior.**

***Index Terms*—NFV, SDN, Smart grid, Dependability evaluation, Failure mode analysis, Hierarchical modeling, Markov chain, Reliability Block Diagrams.**

ACRONYMS

CCPS Critical Cyber-Physical System
CIs Critical Infrastructures
DC Data Center
EMS Energy Management System
EPI Electrical Power Infrastructure
FMEA Failure Modes and Effects Analysis
ICT Information and Communication Technologies
NFV Network Function Virtualization
PMU Phasor Measurment Unit
RBD Reliability Block Diagram
SCADA Supervisory Control and Data Acquisitiony
SD-SPG SDN-enbaled Smart Power Grid
SDN Software Defined Networking
SDN-C SDN controller
SG Smart Grid
SSA Steady State Availability
UPS Uninterruptible Power Supply
VIM Virtualization Infrastructure Manager
VNF Virtualized Network Function

I. INTRODUCTION

Critical Infrastructures (CIs) are becoming more complex and vulnerable due to the integration of modern information and telecommunication technologies in the service management layer. Smart grids, intelligent transportation systems, and smart factories are examples of CIs that incorporate a programmable communication network [1] [2]. These CIs are implemented as distributed CCPSs where the physical assets are associated with software applications for sensing, supervision, and control. In a Smart Grid (SG), distributed power substations have local applications for control, and the global load balancing between distributed substations is ensured by an Energy Management System (EMS) that sends the control commands via a programmable communication network [3]. In our work, we assume that the communication network programmability is ensured by an SDN controller (SDN-C) managed as a service by the Information and Communication Technologies (ICT) operator. A standard SDN architecture is shown in Fig.1 where the EMS applications manager interfaces with the SDN-C to dynamically adapt the Data Plane to the power control needs in terms of load balancing, security, and resilience. In addition, to keep the pace with the increasing amount of data to process, and the low latency requirements of real-time EMS control, ICT and Electrical Power Infrastructure (EPI) operators must increase the geo-distribution of their edge DCs network. This geographical proximity implies that the DCs hosting SDN and EMS applications rely on a stable power supply to reliably manage the hosted virtualized critical services. In parallel, a reliable power supply depends on the high availability of critical control services hosted by the aforementioned DCs. In order to mitigate the risk of failure cascades due to the presence of these complex interdependencies, cloud-native technologies can be leveraged to

design proactive cross-domain resilience strategies respecting the privacy and resilience constraints of critical services. That is, novel network automation tools and procedures enable operators to integrate self-healing capabilities into networks of critical Virtualized Network Function (VNF)s. This would significantly reduce the response time and the risk of faulty human interventions [4]. Furthermore, the standardization of cloud-native technologies allows ICT and EPI operators to adopt a shared resilience mechanism at the DC layer. Even though this migration offers cost efficiency, increased up-time, and high redundancy support, there are still some bottlenecks in managing the networking to ensure real-time monitoring and control. Thus, evaluating the dependability of such a complex system has attracted special interest in the research community [5] [6]. A system's dependability is defined as *"its ability to deliver a service that can justifiably be trusted. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical, human) that interacts with the former at the service interface"* [7]. Dependability encompasses the attributes of reliability, availability, maintainability, performability, and safety, with the objective to ensure fault prevention, removal, tolerance, and forecasting.

To evaluate a system's dependability, efficient and simplistic combinatorial tools like RBD, Fault Trees (FT), and Dynamic Reliability Block Diagrams (DRBDs) are commonly used in the literature [8] - [13]. However, these models don't incorporate complex system behavior such as multiple failure modes, imperfect maintenance, and subsystems interdependencies [14]. To deal with these limitations, state-space models like Continuous-time Markov Chain (CTMC) and Stochastic Petri Networks (SPNs) can be effectively used to capture dependencies between different system's states and multiple failure modes, but their limitation becomes obvious when dealing with a large state space. Indeed, defining, storing, and computing state evolution in large-scale complex systems of multiple components might become intractable. Hence, a hierarchical modeling approach combining the state-space and the combinatorial tools offers trade-offs in terms of modeling and computational tractability [11] [15]. In this work, we focus on the evaluation of the steady state availability of the SD-SPG by means of a hierarchical model that combines CTMCs sub-models of the different subsystems at the lower level and RBDs at the upper level to aggregate subsystems steady states measures. To this end, we represent the SD-SPG as a network of connected and interdependent CCPSs of both the power and communication domains (noted CPS^{EPI} and CPS^{ICT} respectively).

This paper is organized as follows: in section II, we conduct a literature review on the integration of cloud-native technologies into EPI management and the motivation behind the need to establish a Failure Modes and Effects Analysis (FMEA). Then, we provide a preview of the state of the art on the dependability evaluation methodologies in SD-SPG and cloud environments. In section III, we present an SD-SPG architecture that separates the interactions between the ICT and EPI subsystems into three layers. A FMEA analysis is conducted to determine the failure mode of each component and the cross-domain impact. In section IV, we present the hierarchical model to evaluate steady state availability. Finally, we conduct numerical simulations and compare the computed dependability attributes for different scenarios of interactions between the power and telecommunication domains subsystems.

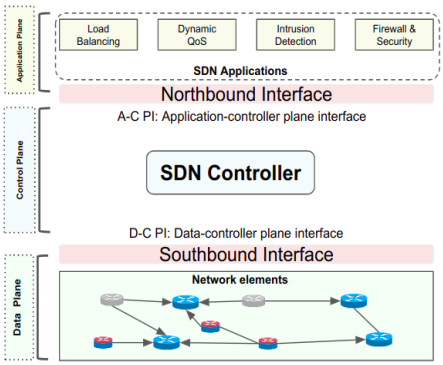


Fig. 1: SDN architecture.

II. Related work

A. Cloud native management of smart power grid

Monitoring and control applications in the EPI should evolve to keep pace with the increased complexity of the power grid both from the demand and supply sides. The communication network plays a major role in this transformation by enabling tele-operation, and real-time monitoring and control of power substations controlling the distribution network. This role is specified in the standard IEC 61850 which defines the protocols for power substations communications. Following this standards, new paradigms incorporating virtualization technology are gaining an interest as they are expected to be a key enabler for real-time, resilient monitoring and control as well as to enhance protection [18] [19]. In [20], the authors present a survey on modern solutions to switch from static to programmable control of the communication network. The authors provide a deep view into the existing and emerging communication technologies and their application to one of the subdomains of the SG like smart metering, substation automation, demand response...etc. In this framework, the cloud-native paradigm offers flexible, scalable, and reliable network management [21] [22]. In [23], the authors explore the opportunities brought by the Edge Computing (EC) paradigm into SG operations. The paper presents different architectures to integrate EC into SG fault monitoring, diagnosis, and asset management. In [24], the authors investigate the use of SDN to design a programmable communication network that guarantees access control, failure resiliency, and adequate bandwidth and delay for critical infrastructures. In [25], the authors propose a distributed SDN-C framework to deploy intrusion detection systems in order to mitigate malicious cyber-attacks on the smart grid. The proposed framework

presents enhanced performances compared to legacy security frameworks.

In general, a FMEA is conducted to enhance a system's reliability by first, identifying the failure modes and causes and then, calculating the (*RPN: Risk Priority Number*) to rank critical events and take corrective actions [26]. For complex systems spanning multiple engineering domains, such analysis becomes tedious as it requires heterogeneous expertise which would hinder the decision-making capability. However, in our work, the interoperability edge DCs infrastructure deploying the same virtualization technologies can be used to coordinate actions and share virtual computing resources to guarantee the high availability of critical services. Thus, the objective of FMEA in the context of this paper is to identify the subset of interactions between the power and telecommunication domain subsystems, that leads to cross-domain failure propagation. That is, identifying such critical events would help decision-makers to design cost-effective mitigation measures while considering the uncertainty associated with such events. In [27], authors quantitatively evaluate the resilience of a smart grid against cyber-attacks and the benefits of deploying enhanced protection devices. In our work, we study the benefit of sharing virtual computing resources between ICT and EPI DCs in order to avoid critical services downtime and failure propagation.

B. Dependability analysis & evaluation in SD-SPG

Dependability evaluation and analysis are conducted with the objective to investigate failure manifestation modes, their impact on the system or some subsystems, and how to efficiently mitigate failure events. This procedure is widely adopted to analyze mission-critical systems and extract dependability metrics. The choice of dependability attributes to study depends on the modeler choice and system specifications [28]. In Table.I, we present an overview of the prior works focusing on dependability modeling of Smart Grid and cloud-based complex systems. The proposed models focus on reliability, availability, and performance as main metrics to quantify using the transient and steady-state characteristics of time-dependent state-space stochastic models. In [6], the authors used stochastic activity networks (SANs) to model the availability of the next-generation power distribution integrating modern ICT infrastructure. A reward model is constructed to compute *System Average Interruption Duration Index (SAIDI)* which quantifies service downtime. In cloud-based systems, metrics like request rejection probability and mean response delay is studied in [13].

III. SDN-enabled Smart Power Grid Architecture & Functional Analysis

We propose the architecture depicted in Fig.2 for an SDN-enabled smart power grid. We separate the interactions between the components of ICT and EPI domains into three planes: control, data, and power :

A. Architecture

1) Control Plane: In this plane, we assume that the SDN-C and EMS applications are deployed over a virtualization infrastructure installed in the edge DCs following the same Network Function Virtualization (NFV) standards. The EMS performs monitoring of the power substations by receiving the monitoring data through the communication network (***link 3***) and ensures the dynamic and real-time control of the power relays to satisfy power loads demand fluctuations (***link 4***). In addition, the EMS interfaces with the SDN-C via the northbound interface to update the data routing paths in the data plane and expose the desired service level agreements (***link 1***). The SDN-C ensures the dynamic control of SDN-enabled routers in the data plane (***link 2***) to meet desired service level agreements (resilience, latency…), exposed via the interface with the EMS (SDN application interface: ***link 1***).

2) Data Plane: In this plane, we consider SDN-enabled routers connected via a southbound interface with their correspondent SDN-C. These routers apply the control setup imposed by the SDN-C (through ***link 2***) to the data flow. In addition, we consider the routers of EMSs and power substations as part of the data plane.

3) Power Plane: In this plane, we consider power substations composed of Phasor Measurment Unit (PMU) networks collecting sensory data and an electrical relays controller (a Supervisory Control and Data Acquisitiony (SCADA) system for example) responsible for aggregating sensor data, generating local control, sending monitoring data to the EMS and applying the global control imposed by the EMS. In addition, we assume that the DCs power supply systems (Uninterruptible Power Supply (UPS)) are considered as a load in this plane.

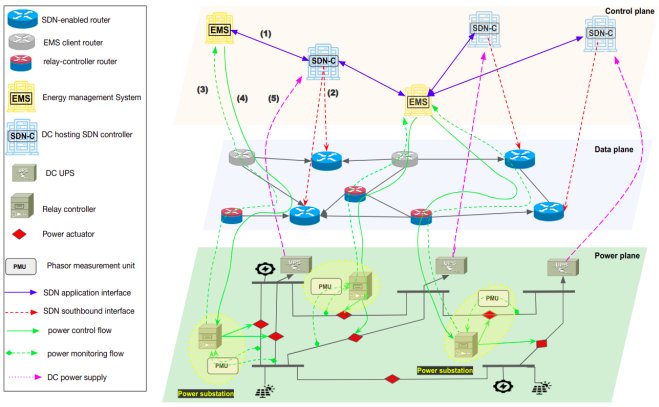


Fig. 2: Architecture of an SDN-enabled smart grid.

B. Functional Analysis

In Fig.3 and Fig.4, we represent the functional block diagrams of the CCPS in ICT and EPI domains respectively. We assume that the power supply of a DC hosting EMS instance is reliable and thus, it is not represented in the diagram. Also,

Paper	Studied System	Model	Dependability metrics
[5]	Control centers network of a smart grid while considering different backup strategies of critical components.	-Stochastic Petri Nets transformed into CTMCs to reduce the state-space.	Availability - Reliability
[6]	Next generation distribution grid with a focus on ICT-based control system and the power grid.	-Stochastic Activity Nets. -Composed Model using Möbius tool.	System Average Interruption Duration Index (SAIDI)
[17]	Tree-based data center networks deploying virtualization.	-Stochastic Reward Nets to model components. -Fault-Tree to model the architecture of subsystems; -Reliability graphs to model the system network topology.	Availability - Reliability
[16]	Private cloud storage services	-Continuous-time Markov chain -Stochastic Petri Nets -Reliability Block Diagram	Availability - Performance
[13]	A cloud IaaS system	-Stochastic Reward Nets	Performance

TABLE I: A preview of research papers treating the problem of dependability modeling in smart grid and cloud-based systems.

it is assumed that the southbound interface between the SDN-C and the data plane is reliable, and thus, is not considered as well. A FMEA to the components involved in ensuring the power and communication services is detailed in Table.II. Note that, the communication service is primordial input to the PMUs network in order to send sensor data to the EMS. Also, the EMS relies on the communication service to send real-time control to the power relays, which explains the double representation of communication service in Fig.4.

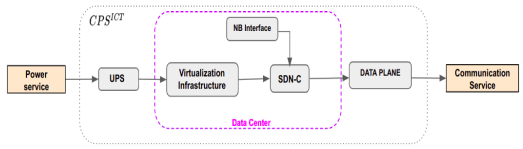


Fig. 3: Functional Block diagram of a cyber-physical system in the ICT domain whose main function is to provide communication service.

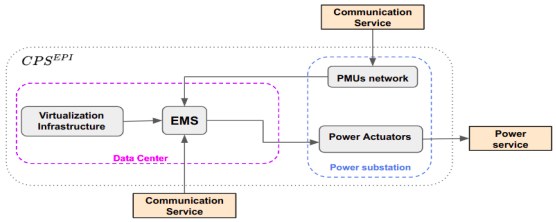


Fig. 4: Functional Block diagram of a cyber-physical system in the EPI domain whose main function is to provide power service. Note that, we assume that the power supply of a DC hosting EMS instances, is reliable and thus, it is not represented in the diagram.

IV. Dependability Modeling and Evaluation of SD-SPG

We assume that each CPS is composed of two subsystems: a virtualized DC (subsystems **E** and **S** of CPS^{EPI} and CPS^{ICT} respectively), and a power-domain subsystems: (subsystems **P** and **UPS** of CPS^{EPI} and CPS^{ICT} respectively). Based on the FMEA table above, we define the different states of each subsystem and construct the corresponding continuous-time Markov Chains (CTMCs). These models will be used to compute SSA measure of each subsystem. Then, the quantified measures will be aggregated to compute CPS availability using the RBD modeling.

A. Continuous-time Markov chains

In the state-space model of the **S** subsystem in Fig.5, we assume that this subsystem (a virtualized data center composed of virtualization infrastructure, SDN-C, and a programmable data plane), has four states :

1) **State S1**: all three components: virtualization infrastructure, SDN-C, and Data plane routers are available.
2) **State S2**: the SDN-C software experiences a failure mode (software bug, overloaded, software rejuvenation...) while the virtualization infrastructure and the data plane are available. In addition, we consider the absence of demands to update the data plane. The rate λ_{12}^S is the failure rate of the SDN-C software and μ_{21}^S is the rate of SDN-C software re-instantiation success on the same virtualization infrastructure (same hardware). Note that, the data plane might continue to work properly even if the SDN-C is out of service as long as there is no requests to update the routing tables.
3) **State S3**: If the subsystem is in *state 2* (failed SDN-C re-instantiation), and that a request arrives with a rate $\lambda_{23}^S = \frac{1}{MTTReq_{sdn}}$ with $MTTReq_{sdn}$ is the *mean time to request SDN-C service*, the VIM will attempt to instantiate the SDN-C on another available hardware. We assume that VIM will attempt to re-instantiate the SDN-C on other hardware resources available in the same DC with a rate μ_{31}^S. Otherwise, the data plane becomes unavailable with the rate λ_{34}^S.
4) **State S4**: if the SDN-C is not re-instantiated and the request persists, the data plane becomes out-of-date, and thus, unavailable and out of service with a rate λ_{34}^S. The rate μ_{31}^S models the success of restoring the SDN-C and the data plane. In this state, a restoring of the SDN-C and the controlled data plane may be conducted with a rate μ_{41}^S.
5) **State S5**: this state corresponds to the case where the virtualization infrastructure is down. The rate λ_{45}^S models the rate by which the VIM fails while re-instantiating the SDN-C and the data plane (faulty intervention). For example, instead of rebooting the VM of SDN-C software, a reboot of the whole virtualization infrastructure is performed instead. The rate λ_{15}^S characterizes the rate by which an abnormal electrical state of the DC leads

Component	Function	Failure Modes	Failure Cause	Failure Effect
SDN-C	Control the data plane.	1- Inability to handle incoming requests. 2-Inability to reconfigure the data-plane.	1-Failure of the NB interface . 2-Unavailability of the virtualization infrastructure.	1-Reject requests to configure the data plane 2-Non transmission of data from EMS to power substation (control flow) and from power substation to EMS (monitoring flow) .
Data plane	Apply the control plane configuration.	1-Forwarding the data flow to wrong destination 2-Physical equipment (links) failures	1-Wrong routing/forwarding rules. 2-Extreme weather conditions.	Communication service interruption
Virtualization Infrastructure	Provide dynamic computing, storage and networking resources to run VNFs.	1-Inability to instantiate VNFs and provide required resources.	1-Abnormal electrical state.	Perturbation of VNFs continuity and availability.
UPS	Provide uninterrupted power supply for physical servers	1-Inability to provide reliable power.	1-Power distribution network failure.	Inability to launch new servers in the DC.
EMS	Control and monitoring of power distribution network.	1-Reconstruct wrong state of the network. 2-Apply outdated control to the power network.	1-Delayed transmission of monitoring data. 2-Latency requirements not satisfied in the data plane.	1-Compute wrong control. 2- Destablization of power distribution network.
PMUs	Collect sensor data of power distribution network state.	1-Sensor fusion failure. 2-Send delayed measurements.	1-Error accumulation in the measurements. 2-Data plane failure.	1-Destabilize the monitoring function of the EMS.
Power actuators	Apply power network stabili--zation control sent by the EMS.	1-Electro-mechanical degradation	1-Heat, oxidation, acidity, and moisture	1-Inability to satisfy power demands in the power distribution network.

TABLE II: FMEA of main components involved in SDN-enabled smart power grid network.

to the failure of the virtualization infrastructure and thus causing the failure of the SDN-C and the data plane as well.

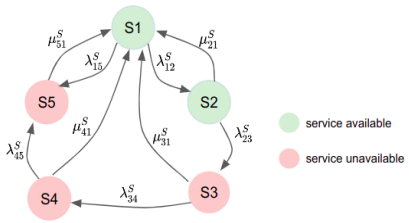


Fig. 5: continuous-time Markov chain describing the state of the **S** subsystem (a virtualized data center composed of: Virtualization Infrastructure Manager (VIM), SDN-C and a programmable data plane).

For the state-space representation of an **E** subsystem (a virtualized data center composed of VIM and an EMS) illustrated in Fig.6, we assume it has three states :

1) **State S1**: the two components: VIM and EMS software are available.
2) **State S2**: the EMS software experiences a failure mode (software bug, overloaded, software rejuvenation, or a refused connection by the SDN-C) while the VIM is still available. The rate λ_{12}^{E} is the failure rate of the EMS software and μ_{21}^{E} is the rate of EMS software re-instantiation success on the same virtualization infrastructure.
3) **State S3**: the VIM is required to request a data plane update to perform an EMS scaling, with a rate of λ_{13}^{E}. If the operation is successful (the requested updates are performed normally by the SDN-C), the system goes back to state **S1** with a rate μ_{31}^{E}. Otherwise, the VIM fails at ensuring the scaling and hence is considered to fail with a rate λ_{34}^{E}.
4) **State S4**: in this state, both components are unavailable. The rate λ_{14}^{E} characterizes the rate by which the VIM fails due to a hardware or software failure. This implies the immediate unavailability of the EMS. The rate μ_{41}^{E} models the success of the VIM and EMS recovery process. Note that, we assume that the recovery process of the VIM implies a successful re-instantiation process of the EMS.

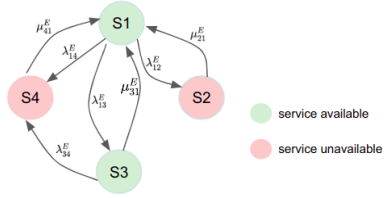
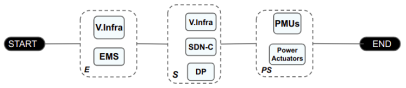
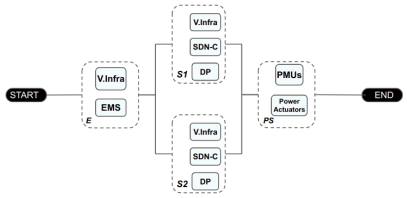


Fig. 6: continuous-time Markov chain describing the state of the **E** subsystem (a virtualized data center composed of : VIM and EMS)

We assume that the **UPS** supplying power to the **S** subsystem has two states: an available state if it is providing the requested power to the subsystem **S**. Otherwise, it switches to the unavailable state if a power request arrives with a rate λ_{pow} and the **P** subsystem is unavailable. For the **P** subsystem, we assume it can be in two states: an available state if it is fulfilling power distribution control when required. Otherwise, it switches to an unavailable state if power load fluctuations appear in the form of requests from the **UPS** with a rate λ_{ups} and if the controlling EMS (corresponding subsystem **E**) is unavailable.



(a) Reliability Block Diagram of a CPS^{EPI} without redundancy.



(b) Reliability Block Diagram of a CPS^{EPI} with networking redundancy.

Fig. 7: Reliability Block Diagram of a CPS^{EPI}.

B. Reliability Block Diagrams

The SSA of all the four subsystems are aggregated to calculate the SSA of CPS^{ICT} and CPS^{EPI}. Also, we conduct a sensitivity analysis to quantify the contribution of each subsystem to the availability of the CPS. Thus, this can be used to determine how the improvement of one subsystem's availability will impact the availability of the CPS. In Fig.7, we represent the RBD of a CPS^{EPI} with different networking redundancy. Let A_E, A_S, and A_{PS} be the steady state availability of subsystems E, S, and PS respectively. The steady-state availability of the CPS^{EPI} represented by the RBD in Fig.7a is:

$$A_{CPS} = A_E \times A_S \times A_{PS} \tag{1}$$

In case of redundancy of the networking service, the steady state availability of the CPS^{EPI} represented by the RBD in Fig.7b is:

$$A_{CPS}^{P} = A_E \times (1 - (1 - A_S)^2) \times A_{PS} \tag{2}$$

Assuming that the two S subsystems have the same availability attributes. In the next section, we simulate the CTMCs and evaluate the upper-level availabilities considering different redundancy schemes of a CPS^{EPI} on the networking service. In addition, we study the impact of request parameter variation on the system's availability.

V. Simulation & Numerical Results

We use the *Möbius* software [32] to implement the CTMCs of the different components and compute the steady-state availabilities. Note that, the aforementioned CTMCs in IV are modeled first as a Stochastic Activity Network (SANs) which

Component	MTTF	MTTR
UPS	250000h	8h
Virt. Infra	111050h	2h
SDN-C	18000h	0.34h
EMS	18000h	0.34h
Power substation	10000h	24h
Data plane	32000h	1h

TABLE III: Components failure data and sources

will be solved as CTMCs by the tool. The model parameters are aggregated from various sources [17] [31] and are showed in TABLEIII, we variate the request rate parameters λ_{23}^{S} and λ_{13}^{E} and study the impact on the DC subsystems (E and S). Also, we assume that the autoscaling success rate μ_{31}^{S} is the same as the rate μ_{31}^{E}. The obtained results are illustrated in Fig.10 and Fig.8.

For the S subsystem, the steady state availability increases with the autoscaling success rate which reflects the high availability of hardware resources and the power supply of the DC (subsystem UPS). note that, with fixing the SDN-C repair rate $\mu_{21}^{S} = 2.94h^{-1}$, for values of λ_{23}^{S}, we notice that the slope of the subsystem availability as a function of the parameter μ_{31}^{S}, increase significantly for values of $\lambda_{23}^{S} > \mu_{21}^{S}$. The fastest the repair of the SDN-C, the smallest the risk of unavailability.

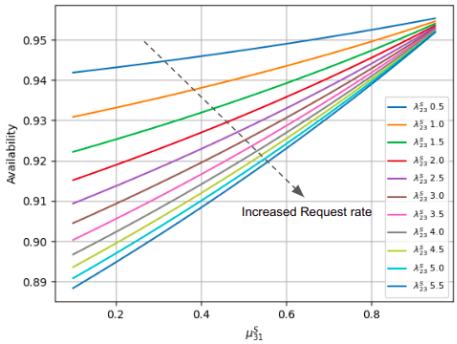


Fig. 8: Availability of subsystem S as a function of the rate μ_{31}^{S} for different networking request rate values.

Similarly, for the E subsystem, an increase in the autoscaling success rate μ_{31}^{E} is equivalent to a situation where the correspondent SDN-C is high available. An increased request rate λ_{13}^{E} may reflect a high dependency of the local power substations on global load balancing ensured by the EMS and thus, this increases the vulnerability of the EMS to the unavailability of S subsystem on which it is dependent. We also compute the rejection rates as the rate between the number of times the subsystem E requests a network update and the times these requests are rejected. This metric is illustrated as a function of the autoscaling success parameters. We notice that this metric converges to zero with an increase in the autoscaling success rate. However it doesn't depend on the request rate λ_{13}^{E}. Finally, the steady state availabilities for subsystems UPS and P are $A_{\infty}^{UPS} = 0.9241$ and $A_{\infty}^{PS} = 0.9786$ respectively. In Fig.9, we compute the availability of a CPS^{EPI} in two scenarios, with and without networking redundancy. As expected, the redundancy increases the availability of the CPS. However, it is worth to study a more realistic scenario where the UPS and PS subsystems state transitions depend on the state of the E and S subsystems.

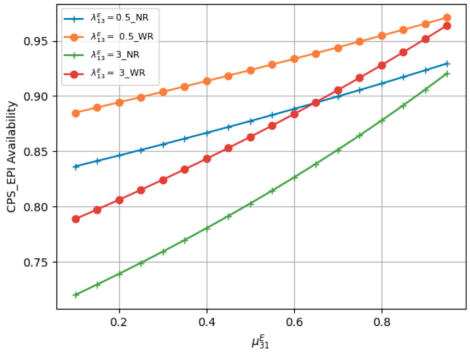


Fig. 9: Steady state availability of CPS^{EPI} in two scenarios: with redundancy (WR and without redundancy NR).

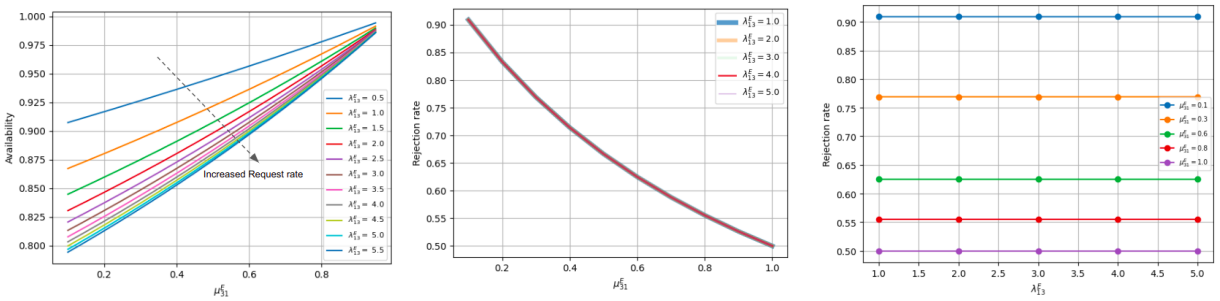
VI. Conclusion

In this paper, we presented a failure mode and effect analysis of an SDN-enabled smart power grid as an example of a critical cyber-physical system highly dependent on the modern cloud-native technologies. We focused on cross-domain failure propagation scenarios where the main components are hosted as virtual functions in data centers deploying the same virtualization technologies. In order to study the complex failure propagation scenarios, we presented a FMEA to separate in-domain, from cross-domain failure modes which lead to cascading failures. Detecting and mastering such interactions would help operators effectively evaluate the risk of such events and the optimal mitigation procedure. his also would allow operators to optimize their capital expenditures by reinforcing coordination in specific regions where the ICT and EPI networks are highly interdependent. To evaluate the availability of complex CPSs, we presented a hierarchical model composed of continuous-time Markov chains at the lower level and Reliability Block Diagrams at the upper level to capture complex interactions. The simulations showed that the increase in interactions between the subsystems of different domains, expressed by a higher service request rate, has a direct impact on the subsystems and the CPS steady state availability. Also, we showed that the increase of redundancy of the networking service leads to an enhancement of the availability of the CPS_{EPI}. As a perspective for this work, we propose to consider the complex interdependencies between all four subsystems to tackle the network-level subsystem's states and tackle the network-level dependability evaluation problem.

References

[1] F. Spinelli and V. Mancuso, "Toward Enabled Industrial Verticals in 5G: A Survey on MEC-Based Approaches to Provisioning and Flexibility," in IEEE Communications Surveys & Tutorials, vol. 23,

[2] Jianchao Zhang, Boon-Chong Seet, Tek-Tjing Lie and Chuan Heng Foh, "Opportunities for Software-Defined Networking in Smart Grid," 2013 9th International Conference on Information, Communications & Signal Processing, 2013.



(a) Availability of subsystem E as a function of the rate μ_{31}^{E} for different networking request rate values.

(b) Rejection rate as a function of μ_{31}^{E} for different request rate values.

(c) Rejection rate as a function of λ_{13}^{E} for different recovery rate values.

Fig. 10: Availability and Rejection rate evolution for different rate parameters for the subsystem E.

[3] P. Wlazlo et al., "A Cyber Topology Model for the Texas 2000 Synthetic Electric Power Grid," 2019 Principles, Systems and Applications of IP Telecommunications (IPTComm), Chicago, IL, USA, 2019.

[4] E. Coronado et al., "Zero Touch Management: A Survey of Network Automation Solutions for 5G and 6G Networks," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2535-2578, 2022.

[5] R. Zeng, Y. Jiang, C. Lin and X. Shen, "Dependability Analysis of Control Center Networks in Smart Grid Using Stochastic Petri Nets," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1721-1730, Sept. 2012, doi: 10.1109/TPDS.2012.68.

[6] T. Amare, B. E. Helvik and P. E. Heegaard, "A modeling approach for dependability analysis of smart distribution grids," 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 2018, pp. 1-8, doi: 10.1109/ICIN.2018.8401634.

[7] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[8] B. Silva et al., "ASTRO: A tool for dependability evaluation of Data Center infrastructures," 2010 IEEE International Conference on Systems, Man and Cybernetics, Istanbul, Turkey, 2010, pp. 783-790, doi: 10.1109/ICSMC.2010.5641852

[9] F. M. Alturkistani, S. S. Alaboodi and S. N. Brohi, "An analytical model for reliability evaluation of cloud service provisioning systems," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, Taiwan, 2017, pp. 340-347, doi: 10.1109/DESEC.2017.8073821.

[10] T. A. Nguyen, D. Min, E. Choi and T. D. Tran, "Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models," in IEEE Access, vol. 7, pp. 9273-9313, 2019, doi: 10.1109/ACCESS.2019.2891282.

[11] Trivedi, K., & Bobbio, A. (2017). Hierarchical Models. In Reliability and Availability Engineering: Modeling, Analysis, and Applications (pp. 577-630). Cambridge: Cambridge University Press. doi:10.1017/9781316163047.022

[12] S. Fernandes, E. Tavares, M. Santos, V. Lira and P. Maciel, "Dependability assessment of virtualized networks," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 2012, pp. 2711-2716, doi: 10.1109/ICC.2012.6363992.

[13] R. Ghosh, F. Longo, F. Frattini, S. Russo and K. S. Trivedi, "Scalable Analytics for IaaS Cloud Availability," in IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 57-70, Jan.-March 2014, doi: 10.1109/TCC.2014.2310737.

[14] M. Malhotra and K. S. Trivedi, "Power-hierarchy of dependability-model types," in IEEE Transactions on Reliability, vol. 43, no. 3, pp. 493-502, Sept. 1994, doi: 10.1109/24.326452.

[15] W. E. Smith, K. S. Trivedi, L. A. Tomek and J. Ackaret, "Availability analysis of blade server systems," in IBM Systems Journal, vol. 47, no. 4, pp. 621-640, 2008, doi: 10.1147/SJ.2008.5386524.

[16] Torres, E., Callou, G. & Andrade, E. A hierarchical approach for availability and performance analysis of private cloud storage services. Computing 100, 621–644 (2018). https://doi.org/10.1007/s00607-018-0588-7

[17] T. A. Nguyen, D. Min, E. Choi and T. D. Tran, "Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models," in IEEE Access, vol. 7, pp. 9273-9313, 2019.

[18] SASE and Edge Team, V. S. W. (2022, May 18). Journey Toward a Smarter Grid: Substation Virtualization Is Here and Now. VMware SASE and Edge. https://blogs.vmware.com/sase/2022/05/18/journey-toward-a-smarter-grid-substation-virtualization-is-here-and-now/

[19] Samara-Rubio & al. "Virtual protection relay a paradigm shift in power system protection", 2022, Intel Corporation.

[20] L. F. F. De Almeida et al., "Control Networks and Smart Grid Teleprotection: Key Aspects, Technologies, Protocols, and Case-Studies," in IEEE Access, vol. 8, pp. 174049-174079, 2020.

[21] A. Aydeger, K. Akkaya and A. S. Uluagac, "SDN-based resilience for smart grid communications," 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), (2015)

[22] J. Moura and D. Hutchison, "Resilience Enhancement at Edge Cloud Systems," in IEEE Access, vol. 10, pp. 45190-45206, (2022)

[23] Y. Liao and J. He, "Optimal Smart Grid Operation and Control Enhancement by Edge Computing," 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2020, pp. 1-6.

[24] R.Kumar, "Programmable Cyber Networks For Critical Infrastructure", PhD thesis, University of Illinois at Urbana-Champaign, 2019

[25] U. Ghosh, P. Chatterjee and S. Shetty, "A Security Framework for SDN-Enabled Smart Power Grids," 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2017, pp. 113-118.

[26] Di nardo, Mario & Murino, Teresa & Osteria, Gianluca & Santillo, Liberatina. (2021). "A New Hybrid Dynamic FMECA with Decision-Making Methodology: A Case Study in an Agri-Food Company." 10.20944/preprints202112.0394.v1.

[27] Netkachov, Oleksandr & Popov, Peter & Salako, Kizito. (2019). Quantitative Evaluation of the Efficacy of Defence-in-Depth in Critical Infrastructures. 10.1007/978-3-319-95597-1_5.

[28] K. S. Trivedi, D. S. Kim, A. Roy and D. Medhi, "Dependability and security models," 2009 7th International Workshop on Design of Reliable Communication Networks, Washington, DC, USA, 2009, pp. 11-20, doi: 10.1109/DRCN.2009.5340029.

[29] G. Andersson et al., "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," IEEE Transactions on Power Systems, vol. 20,no. 4, pp. 1922 – 1928, Nov. 2005.

[30] M. Rahnamay-Naeini and M. M. Hayat, "Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach," in IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 1997-2006, July 2016, doi: 10.1109/TSG.2016.2539823.

[31] Retterath, B. & Chowdhury, A.A. & Venkata, S.s. (2005). Decoupled substation reliability assessment. International Journal of Electrical Power & Energy Systems - INT J ELEC POWER ENERG SYST. 27. 662-668. 10.1016/j.ijepes.2005.08.008.

[32] Daly, David & Deavours, Daniel & Doyle, Jay & Webster, Patrick & Sanders, William. (2000). Mobius: An Extensible Tool for Performance and Dependability Modeling. 1786. 332-336. 10.1007/3-540-46429-8_25.

C - Paper C

Availability Modeling and Analysis of Cloud-native, Interdependent Cyber-Physical Systems: Application to SDN-enabled Smart Power Grids

Khaled SAYAD, Benoit LEMOINE, Anne BARROS, Yiping FANG, and Zhiguo ZENG

***Abstract*—The increasing adoption of cloud-native technologies in critical Cyber-Physical Systems (CPSs) like telecommunication and power infrastructures requires tools to assess and mitigate the impact of emerging failure modes as a result of the softwarization and reliance on geo-distributed virtualized edge Data Centers (eDCs). This work proposes a hierarchical modeling approach using Stochastic Activity Networks (SANs) formalism to evaluate the availability of interdependent ICT and power-distribution services in the framework of an SDN-enabled Smart Power Grid (SDN-SPG) . The optimal dimensioning of eDCs hosting critical applications in both the virtualization and power domains is critical to ensure high service availability and mitigate failure cascades. Thus, through our conceptual framework, we quantify the impact of different protection strategies on critical services' steady-state availability. The obtained results suggest that redundancy-based protection in the virtualization domain can be enhanced by integrating power-domain information which is crucial to design effective cross-domain resilience strategies.**

***Index Terms*—Cyber-physical systems, NFV, SDN, Smart Grid, Availability Modeling, Stochastic Activity Networks, Failure modeling.**

ACRONYMS

AN Activity Network
CAPEX Capital EXpenditure
CIs Critical Infrastructures
CPSs Cyber-Physical Systems
eDCs Edge Data Centers
EMS Energy Management System
EPI Energy and Power Infrastructure
ICT Information and Communication Technologies
MTTC Mean Time To Compromise
MTTF Mean Time To Failure
NFV Network Function Virtualization
OPEX Operational EXpenditure
QoS Quality of Service
SANs Stochastic Activity Networks
SCADA Supervisory Control & Data Acquisition
SDN Software Defined Networking
SDN-C SDN-Controller
SDN-SPG SDN-enbaled Smart Power Grid
SPG Smart Power Grid
SSA Steady State Availability
UPS Uninterruptible Power Supply
VNF Virtualized Network Function

Khaled SAYAD and Benoit LEMOINE are with Orange Innovation, 2 Av. Pierre Marzin, 22300, Lannion, France. (email: firstname.lastname@orange.com)

Khaled SAYAD, Anne BARROS, Yiping Fang, and Zhiguo Zeng are with Chair Risk and Resilience of Complex Systems, Laboratoire GÃ©nie Industriel, CentraleSupÃ©lec, 3 Rue Joliot Curie, 91190, Gif-sur-Yvette,France. (email: firstname.lastname@centralesupelec.fr)

I. INTRODUCTION

Cloud-native concepts like Network Function Virtualization (NFV), Software Defined Networking (SDN), and edge computing are being integrated into modern Critical Infrastructures (CIs) operations in order to enhance the Quality of Service (QoS) and provide more reliable critical services. For services with strict latency and availability requirements, this implies that the software applications composing the service are deployed as virtualized applications in dedicated Edge Data Centers (eDCs) [1]. In the telecommunication industry, we are witnessing the rise of *"Telco-Cloud"* concept where telecommunication services are software-defined. This allows Information and Communication Technologies (ICT) operators to efficiently manage the deployment of their services in resource-constrained environments, and optimally respond to network demand fluctuations. In this context, NFV and SDN paradigms emerge as catalysts for the current transformation of the ICT infrastructure [2]. NFV is a concept where the development phases of network functions software (design, programming, and deployment), are decoupled from the physical, often proprietary, devices on which they run. This would decrease operational expenditure and bring more agility and flexibility into service development and deployment operations [3]. In addition, the SDN paradigm aims to decouple the control (packet forwarding logic) plan and data routing plan. The forwarding rules are software-defined and dynamically interface with commodity hardware allowing network operators to innovate more sophisticated protocols and adapt network behavior to dynamic QoS needs.

Meanwhile, cloud-native technologies are also key enablers for real-time control, power substation automation, and enhanced power-relay protection in Smart Power Grid (SPG)

networks. That is, the high penetration of renewable energies is pushing Energy and Power Infrastructure (EPI) operators to innovate new control strategies to deal with bi-directional power flow and dynamic fluctuations [4]. From CIs resilience perspective, the migration towards a softwarized management of critical services has some drawbacks related to the high exposure to cyber-risks and cross-domain failure propagation [1]. This latter issue is illustrated for example by the need of ICT operators to densify their eDCs networks to meet the strict latency requirements of critical applications which would increase the need for a more stable power supply in the power distribution network. Thus, a failure in the power infrastructure may propagate causing service interruptions in the telecommunication domain. On the other side, the failure of telecommunication services may have a considerable impact on the stability of the SPG as studied in [5]. In order to mitigate cross-domain failure propagation, some opportunities in terms of coordination-based protection mechanisms must be established between interdependent ICT and EPI operators at the operational level. The convergence of ICT and EPI infrastructure toward the same operational technologies [1], offers an opportunity to adopt interoperable cross-domain protection schemes. Some examples of such resilience actions are :

- Sharing failure events data at the eDC level, allowing interdependent operators to enhance preparedness and minimize the impact of propagated failures.
- Coordinating dynamic risk assessment to better estimate failure propagation dynamics.
- Multi-domain resources orchestration in eDCs operated by interdependent CIs operators.

In order to deal with the aforementioned problems, we define the following research questions:

- ***RQ1***: How to establish a cross domain dependability evaluation procedure to model the impact of cloud-native technologies integration into interdependent ICT and EPI networks from a risk perspective?
- ***RQ2***: How to design coordinated, cross-domain resilience strategies between ICT and EPI domains at the eDCs layer ? and how to quantify the effectiveness of such protection mechanisms ?

In this present work, we tackle ***RQ1*** by designing a interdependent state-space models of ICT and power domain subsystems that capture the impact of interdependencies in terms of cascading failure. This represents the lower level of the hierarchical model. In the upper level, we construct a network where the nodes are the subsystems and the links are the different dependencies between them. This will allow us to tackle ***RQ2*** through the study of topology impact on service-oriented availability. The model is based on Stochastic Activity networks (SANs) formalism applied to an SDN-enabled Smart power Grid (SDN-SPG). As illustrated in Fig. 1, we assume that real-time control and monitoring of power substations are performed by Energy Management System (EMS) hosted as virtualized applications (green box) in eDCs (red box) operated by the power network operator. The EMS relies on network programmability to dynamically configure the monitoring and control data flow. This feature is assumed to be delivered as a service by a telecom network operator which (in the context of SDN), hosts the control plan as a virtualized application in eDCs as well. Due to geographical proximity, the eDCs hosting the control plane depend on the reliable operation of power substations (purple box) to ensure a reliable flow of power for eDCs operations via Uninterruptible Power Supply (UPS) (blue box). For the rest of this paper, we review related work on the dependability evaluation of complex cyber-physical systems of the ICT and EPI domains and explain how this present work extends existing work on . Then, we propose an architecture of an SDN-enbaled Smart Power Grid (SDN-SPG) where we highlight the critical subsystems to networking and power services dependability. Afterward, we present the modeling approach based on Stochastic Activity Networks (SANs) formalism and the sub-models of each critical subsystem. Finally, we conduct simulations to quantify the impact of cross-domain protection mechanisms on Steady State Availability (SSA) measures of critical services.

II. Related Work

CIs resilience has long been an active field of research due to the socio-economic impact of the interruption of such critical services [7]–[9]. As an example, the 2003 Italian grid blackout [10], shed light on the impact of interdependencies and cascading failure phenomenon between the telecommunication and power domains. Consequently, modeling interdependencies and failure propagation dynamics was the first step into the design of efficient mitigation procedures. In [5], authors propose a framework to assess the reliability of power systems with a strong dependence on ICT infrastructure. A detailed analysis is conducted of different impacts of ICT failures on power systems operations including system monitoring interruption, application incorrect control, and information sharing disruption. Sequential Monte Carlo simulation is conducted to estimate the probability of blackout apparition taking into account both the failures of power and ICT systems. The results show that increasing the reliability of ICT leads to fewer load disconnections in the power domain. Despite the interesting results, realistic data on failure propagation are still needed to validate the results. In [11], authors propose a Mixed Integer Linear Program (MILP) to optimize service restoration in smart grids via the placement of protection resource while considering different scenarios of telecommunication services availability. Interdependencies between the two domains are captured by considering that ICT components as loads and EPI substations as client in the ICT domain. However, the level of abstraction of the ICT components doesn't provide details into how failures manifest in the ICT domain and whether protection mechanisms are needed in parallel to the power domain ones. That is, understanding how operators respond to propagated failures is crucial to adopt an optimal coordinated protection action that could benefit both operators. In [12], authors present an interdependent Markov chain approach to model cascading failures between the telecommunication and power domains. This study suffers from the level of abstraction which omits the role of different components in the power and

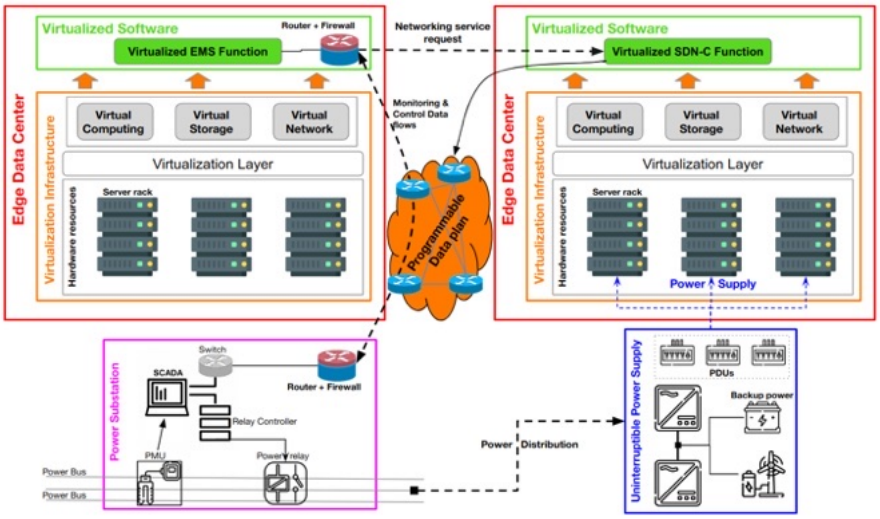


Fig. 1: Detailed view of the main components of an SDN-enabled Smart Power Grid and their interactions. EMS and SDN-Controller (SDN-C) functions are running in eDCs as virtualized applications (green boxes) on top of a virtualization infrastructure (orange box) aggregating the physical servers and the virtualization infrastructure manager software. Note that, we assume that the eDCs (red boxes) hosting EMS applications are reliably supplied in power and we do not represent their respective UPS systems. The part of this illustration involving the EMS and the power substation was adopted from [6]. The main service of the ICT subsystems is network programmability, i.e : the adaption of data plane forwarding rules w.r.t. client (in our case the EMS) requests.

ICT infrastructures and their heterogeneity. In [13], authors propose a heterogeneous interdependent networks model in order to study the dynamics of cascading failures between the power grid and the communication network. The proposed model considers different roles of different nodes in both networks when creating the interdependencies links. During a cascading failure event, a node is considered as failed if it doesn't belong the giant connected component of the graph. Dynamic network protection and self-healing mechanisms are not considered in this latter work. In [14], authors investigate the flexibility and automation brought the the SDN paradigm as an enabler for fast recovery of communication network by enhancing the reliability of teleprotection. In [15], authors propose a network coding framework based on p4 language to enhance the resilience of packet forwarding in critical infrastructures network. Other works investigating the integration of SDN-enabled capabilities into the power grid, focus on security assessment and enhance the cyber-resilience against cyber attacks [16]–[18].

Assuming that the control plan of the SDN is hosted as a set of Virtualized Network Function (VNF) in dedicated eDCs, assessing the reliability and availability of eDCs is crucial to detect design faults, and increase the service (in our case network programmability) availability and reliability attributes [19]. In the context of virtualized eDCs, the dependability evaluation of NFV-based services is studied to enhance the robustness and availability of critical management components of the NFV architecture. That is, reliable power supply is studied due to its criticality in [20] where the authors present a framework called *Flex* which optimizes the eDC's power supply to hosted services based on their criticality and tolerance to power outage during power interruption periods. In [21], authors develop a dependability evaluation framework based on SANs to assess the steady state availability of the Management and Orchestration (MANO) and the impact of different failure modes on overall system performance. In [22], a hierarchical modeling approach is proposed to evaluate the reliability and availability of cloud data-centers. The hierarchical model is composed of Stochastic Reward Nets to capture the behaviors and dependency of the components in the subsystems in detail. In addition, a fault-tree is constructed to model the architecture of the subsystems, and Reliability graphs are constructed in the top layer to model the system network topology. In [23], a hierarchical model is developed to assess the availability of private cloud storage system using a combination of Continuous-time Markov Chains and Reliability Block Diagrams. In [24], the impact of different backup strategies on NFV infrastructure' availability are studied through SANs to assess the suitability of each backup strategy to different availability modes of the system. In [25], an availability model is developed for data-centers network hosting redundant VNF with dynamic migration strategies. The model based on a network evolution approach, is capable of integrating multiple flow characteristics and different redundancy schemes. In [26], Monte Carlo simulations are carried out to estimate the reliability and availability attributes of a data center' UPS. In [27], authors provide an analysis of the dependability of power substation automation system based on *IEC 61850* standard with different redundancy strategies. In [28], a Stochastic Petri Net (SPN) based model is developed to analyze the dependability of control centers network in SPG while considering different backup strategies of critical components. In [29], a vulnerability analysis of the interdependencies between Supervisory Control & Data Acquisition (SCADA) systems and controlled

systems is carried to investigate hidden failure dynamics that could help to better design the interconnection between control centers and power substations in the power grid for example. In our work, we present a SANs model that captures the effects of complex interdependencies between the critical components of an SDN-SPG spanning the EPI and ICT domains.

In terms of capturing the impact of cascading failure, these works present some gaps when modeling the impact on telecommunication services. That is, the service is considered unavailable if the communication node has failed without considering the possibility of self-configuration and self-healing which are key benefits of the migration towards SDN/NFV-based communication service provisioning. Secondly, in terms of dependability modeling of SDN/NFV-based Cyber-Physical Systems (CPSs) in the ICT and EPI domains, previous works limit their study to the virtualization and computing infrastructure without considering the power supply which is in reality a crucial factor in ensuring high availability in virtualized data-centers [20]. This is understandable since the EPI and ICT infrastructures are heterogeneous in nature and operates at different timescales. However, as illustrated in Fig. 1, assuming that the control function of both domains are provisioned in eDCs using the same virtualization technology, enable to adopt homogeneous, synchronized protection mechanisms at the virtualization level. Also, we propose to study the dependability of a smart-grid-ready(SG-ready) UPS [30] which, unlike tradition UPS systems whose functions are limited to backup batteries management and servers protection against power disturbance, SG-ready UPS are capable of (autonomously) interacting with the power distribution network by: supplying energy in a bidirectional power-flow scheme, and fast frequency response for renewable energy penetration. Our modeling approach uses the *shared place* feature of the *MÃ¶bius* tool [31] to implement the interdependency models between different subsystems defined in Fig. 1 . In addition, the presented models capture the complex behavior of these components both at the power and eDCs levels which helps to design effective protection mechanisms. The contributions of this work are:

- Extending existing work on dependability evaluation of virtualized eDCs by considering interactions with power domain subsystems (SG-ready UPSs and Power substations).
- Modeling complex behavior of these subsystems by capturing the cascading failure impact and self-configuration enabled via SDN and NFV technologies.
- A study of the impact of topology on service-oriented availability of telecommunication and power control services and quantification of the impact of different protection policies.

III. SDN-enabled Smart Power Grid Architecture

1) S subsystem: As illustrated in Fig. 2, this subsystems relies on the reliable power supply ensured by the ***UPS***, and provides networking service via the programmable data plane. We assume this subsystem has three states:

- *Available*: the networking service can be requested by the dependent *EMS*, and delivered by means of nominal operation of the virtualization infrastructure, the control plane (SDN-C VNF) and the data plane components.
- *Compromised*: this state describes the inability to perform certain operations (auto-scaling) without impacting the service' availability. The switching from the available to compromised state is triggered upon the failure of the ***UPS*** managing the power supply of the eDC. Note that, this impact is not imminent and we still can ensure backup power supply for some servers. However, in case the service requires a scaling (increase servers usage), the operation might fails and the service becomes unavailable.
- *Unavailable*: the service is interrupted (SDN-C unable to handle upcoming requests to update the data plane) because of a software failure of the SDN-C itself or because of the failure of the virtualization infrastructure.

2) UPS subsystem: We assume this subsystem has three states:

- *Available*: the ***UPS*** operates in nominal mode and is able to reliably supply power to the virtualization infrastructure.
- *Compromised*: this state describes the inability to perform certain operations (charging backup batteries for example) without impacting the main service.
- *Unavailable*: the ***UPS*** is non operational (interruption of backup batteries charging operation, wrong handling of power fluctuations..) leading to eDC shut down.

3) E subsystem: This subsystems relies on the ***S*** subsystem to ensure reliable networking service to perform real-time monitoring and control of power substations. We assume this subsystem has three main states:

- *Available*: the service (monitoring and control of power substations) is performed as expected by means of nominal operation of the virtualization infrastructure and the EMS software.
- *Compromised*: the switching to this state happens upon the failure of the SDN-C that ensures monitoring and data transport from/to the controlled power substations. One effect of such event could be the delay monitoring data transfer, which leads to compute an inadequate control leading to power distribution interruption. EMS functions incorporate anomaly detection mechanisms that might correct wrong data and avoid the computing of wrong control. We refer to the time before the anomaly successfully impacts the EMS as the Mean Time To Compromise (MTTC).
- *Unavailable*: the monitoring and/or control functions are interrupted. This is might be because of the failure of anomaly detection when the system is in *Compromised* state. Or, the service might be unavailable because of the failure of the EMS software or the virtualization infrastructure hardware.

4) P subsystem: We assume the ***P*** subsystem has three states :

- *Available*: the power substation operates in nominal state.

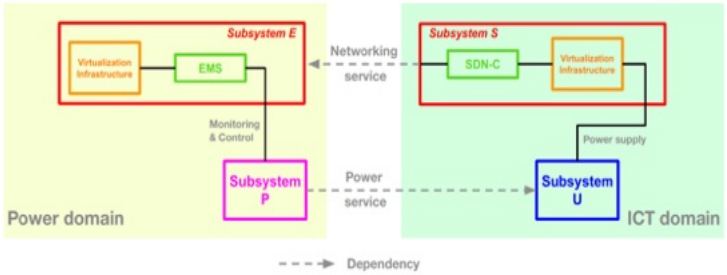


Fig. 2: Aggregated view of different subsystems involved in the functional dependencies between the ICT and power domains from the detailed view above. Note that, subsystems *E* and *S* are edge data-centers that host different services as VNFs (EMS and SDN-C respectively). Note that, the *Power Service* dependency is defined assuming that the subsystem UPS relies on power lines controlled by the subsystem P and any disruption of the latter leads to cascading impact on the UPS.

- *Compromised*: this state describes a situation where the controlling EMS has failed and it is attempting to apply wrong control. In this case, the controlled power substation is considered as compromised. In such situation, anomaly detection mechanisms are frequently performed to detect abnormal controller state. If failed, the system switches to the unavailable state. Otherwise, it goes back to the available state.
- *Unavailable*: the power substation functions are interrupted. These functions are the collection and processing of power network state data via a network of sensors, and the application of EMS control via power relays. The interruption might happen because of a wrong EMS control, a failure of the sensors data aggregation function or the failure of power relays.

IV. Cross-domain Dependability modeling

A system's dependability is defined as *"its ability to deliver a service that can justifiably be trusted. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical, human) that interacts with the former at the service interfaceâ* [32]. This incorporates the attributes of availability, reliability, security, and maintainability. We leverage SANs formalism due to their efficiency in capturing complex behavior in cyber-physical systems, which in our case will be used to capture the impact of interdependencies. This is done using the *"shared places"* feature in *Mobius*, allowing subsystems SANs models to share states during simulation. We start by defining atomic models of the four subsystems described above. Then, we create a network topology by connecting subsystems' atomic models using the *Composed Model* feature of *Mobius*. Also, we define reward functions which increment the time spent in a subsystem's state during simulation period. By doing so, we are able to compute a service steady-state availability by adding the mean times spent in available states. The number of simulation steps will be adapted between experiments to ensure the convergence of the results within the confidence interval.

A. Atomic models

An Activity Network (AN) is a generalization of Petri nets that can be defined as an eight-tuple $AN = (P, A, I, O, \gamma, \tau, \iota, \varphi)$ where P is a finite set of all places, A is a finite set of activities (transitions in Petri nets vocabulary), I is the set of input gates, and O is the set of output gates. $\gamma : A \rightarrow N^+$ is a mapping between the set of activities (transitions) and the number of cases associated with each activity. *Cases* are one of the differences between ANs and Petri Nets where an uncertainty about the next state is assumed upon the completion of the activity. $\iota : I \rightarrow A$ is mapping between input gates and activities. Also, $\tau : A \rightarrow \{Timed, Instantaneous\}$ specifies the type of each activity, and finally, $\varphi : A \rightarrow O$ is a mapping between the activities and output gates. As an extension to this formalism, a SAN can be defined as a five-tuple: $SAN = (AN, \mu_0, C, F, G)$ where: $\mu_0 \in M_p$: is the initial marking of the network (M_p is the set of all markings of the network), C: is the case distribution assignment which maps functions to activities, F: is the activity time distribution function that maps a continuous function to timed activities, G: is the reactivation function that maps functions to timed activities.The triggering of an event and the start and completion of an operation is associated with an activity *completion*. An activity is enabled if all the conditions encoded in the input gates hold. The activation of a timed activity refers to the start of an operation, and is possible if the timed activity is enabled or it is still enabled after its completion. Once the timed activity is triggered, it will either complete (if it stays enabled through the activity duration), or be aborted (if enabling conditions don't hold during the activity duration). The duration between the triggering and completion of an activity is specified via the activity time distribution function F. The distribution parameters might depend on the marking of the SAN at the activation time of the activity. Upon the completion of an activity, *case distribution function* C determines probabilistically which case to be chosen. Finally, a timed activity could be reactivated if the markings of the network permit the reactivation. To do so, a reactivation function G is associated with each timed activity to specify the sets of markings where the timed activity is reactivated (if enabling conditions hold).

Fig. 3: Graphical representation of a SAN elements in *Mobius*.

In the *Mobius* tools, the graphical representations of the aforementioned primitives are depicted in Fig.3 and used to construct the atomic SAN models of the SDN-SPG subsystems explained in the following subsection. Places are represented as circles which represent the modeled system state. Timed and instantaneous activities are represented by thick and thin lines respectively. Finally, input and output gates are represented graphically as red and black triangles respectively.

*1) Subsystem **S**:* In Fig. 4 we illustrate the SAN model of subsystem ***S*** where we highlight different events that may occur and their impact on the service availability which is defined as the ability of the systems to maintain the control of the data plane and the handling of EMS requests. This refers to the mean time spent in the *S_OK* state. The service is unavailable if it is in states *S_NOK* or *S_fc*.

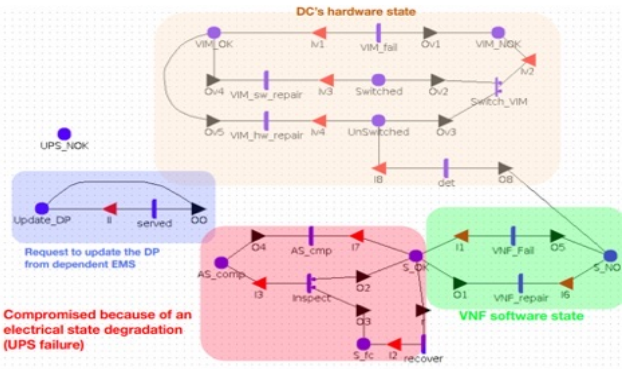


Fig. 4: SAN model of the ***S*** subsystem. The highlighted sub-models refer to independent dynamics that may affect the subsystem available state.

- **Virtualization Infrastructure (VI) failure**: to model the impact of the virtualization infrastructure failure on subsystem ***S***, we define the place *VIM_OK* for the available state of the virtualization infrastructure. This place is initiated with a number of tokens equal to the number of back-ups. In case of a failure of the VI software, the marking of the place *VIM_NOK* is incremented. Upon this event, a switching mechanism is triggered (this action is represented by the *switch_VIM* instantaneous activity) . To consider the failure of the switching mechanism, we define case probabilities which, depending on the success of the switching process, update the marking of one of the places *Switched* or *UnSwitched*. We assume that once the switching is successful, the VIM software is repaired (completion of activity *VIM_sw_repair*). Otherwise, a hardware repair must be done (activity *VIM_hw_repair*). In both cases, the *VIM_OK* marking is incremented. Note that, if the number of tokens in the *UnSwitched* place is equal to the initial marking of *VIM_OK*, this means that all the servers are down, which imply the failure of the SDN application as well. This is represented by the deterministic activity *det*.
- **SDN-C software failure**: in this SAN sub-model highlighted in green, we model a virtualized application state. Note that, the service is available if the application is operational (represented here by place *S_OK*). A software failure event may occur due to a software bug and it was shown in the literature that the time distribution of software failure and repair can be approximated by exponential distribution [**?**]. Thus, we assume that the Mean Time To Failure (MTTF) of the software application is exponentially distributed and is represented by activity *VNF_fail* which, once fired takes the system to state *S_NOK* (service unavailable). The repair event is dependent on the availability of the VIM. This condition is included in input gate *I6*. We assume that the MTTF is exponentially distributed and represented by the activity *VNF_repair*, which, once completed, will be bring the service to the available state.
- **Power supply interruption**: in the SAN sub-model highlighted by red in Fig.4, we illustrate the impact of power supply interruption (represented by a place *UPS_NOK* marked with one token) on the networking service availability. The input gate *I7* contains the condition that if the ***UPS*** is interrupted, then the auto-scaling function is compromised. This means that, once in the *AS_comp* the networking service cannot scale to an increase in demand by increasing its computing capacity (turning on new servers). Note that, the service is always available even in this state. We assume that an inspection activity (represented by *inspect*) might take place. If the inspection succeeds, the auto-scaling is recovered. Otherwise, the system switches to a failed state denoted *S_fc* for failed-compromised to distingue from internal failure state. Once in this latter state, the recovery process depends on the recovery of the ***UPS*** (the marking of *UPS_NOK* passes to zero token).
- **Data plane update requests arriving**: the place *Update_DP* is shared with the dependent ***E*** subsystems. Once it is marked with more than one token (a request arrival), the request is served if the subsystem ***S*** is in state *S_OK*. In the output gate *OO*, the marking is decremented and the systems waits for the upcoming request. Note that, the request generation is highlighted in blue in Fig. 5 below.

*2) Subsystem **E**:* The virtualization infrastructure and application software sub-models of the subsystem ***E*** are similar to subsystem ***S***. We detail the state-space sub-models for request generation and the impact of networking service interruption illustrated in Fig. 5:

- **Networking service interruption**: this state-space model considers the failure states (*S_OK* and *S_fc*) of the subsystem ***S*** on which it is dependent. If the marking of one of these states is equal to one token (this condition

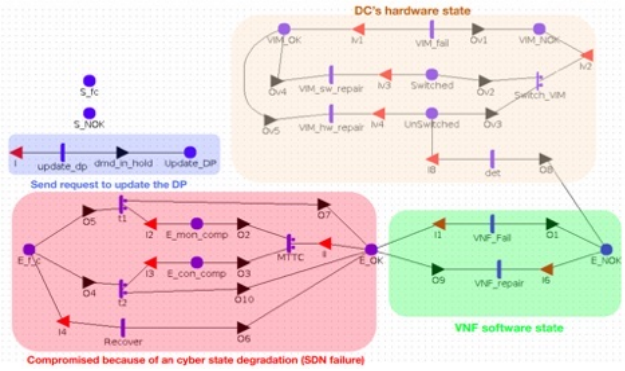


Fig. 5: SAN model of the ***E*** subsystem. The highlighted refers to independent dynamics that may affect the subsystem available state.

is implemented in input gate *II*), the monitoring or the control functions are compromised. We assume that the Mean Time To Compromise (MTTC) is exponentially distributed, and we define case probabilities to model on the uncertainty on whether the completion of this operation would impact the monitoring or the control functions of the EMS. Then, once the marking of one of the places *E_mon_comp* or *E_con_comp* is updated, an inspection operation is performed (activities *t1* and *t2*), which will take the system back to state *E_OK* if succeeded. Otherwise, the service becomes unavailable and the system switches to state *E_fc*. Recovery procedure is performed in exponentially distributed periods (activity *Recover*) and takes the systems back to state *E_OK*.

- **Data plan request generation**: the sub-model highlighted in blue represents the process of generating a request to update the data plane when interfacing with the SDN-C. The request arrives in exponentially distributed time (activity *update_dp*) if the request queue is empty (the condition that the marking of the place *Update_DP* is equal to zero is implemented in input gate *I*). If the request is generated, the request is satisfied if the marking of *Update_DP* switches back to zero (activity *served* in Fig. 4 is fired).

*3) Subsystem **P**:* In the SAN model depicted in Fig. 6, we assume that the service is available if the system is in states *P_OK* or *P_comp*. If the ***E*** subsystem is unavailable (in state *E_NOK* or *E_f_c*), a wrong control flow might compromise the controlled power substation (activity *p_mttc*). If the issue is detected, the system switches back to state *P_OK*. During the compromised state, load balancing control might be triggered (activity *LB_power*). If the control is corrected, the system switches back to state *P_OK*. Otherwise, the wrong control is applied and the system enters the *P_fc* state. To go back to available state, a recovery procedure is performed (activity *P_recover*).

*4) Subsystem **UPS**:* In the SAN model depicted in Fig. 7, we assume that the eDC power supply service is available if the system is in states *UPS_OK* or *UPS_cmp*. If the power distribution network experiences a failure (states *P_fc*

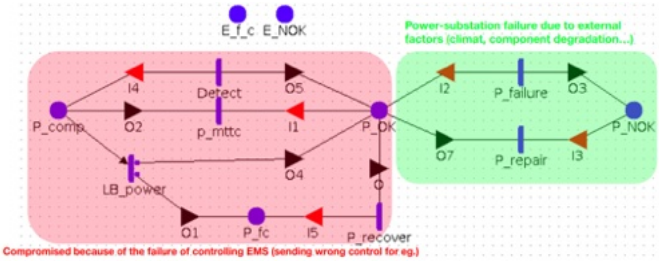


Fig. 6: SAN model of the ***P*** subsystem.

or *P_NOK* are marked with one token) , the impact is not imminent (due to backup batteries). Note that, a UPS is a reactive system that regulates incoming power flow and adapt it to eDC needs. The delay before the system is impacted is modeled as deterministic time (activity *impact*). Once this time is consumed, UPS capacity to recharge batteries or filter power fluctuations is compromised. Activity *AS_request* firing means that the eDCs requires more power to respond to hosted services deployment needs (expressed by the shared states *VIM_OK, S_OK and S_NOK*). The success of the operation depends on the availability of the power substation on which the eDC is dependent.

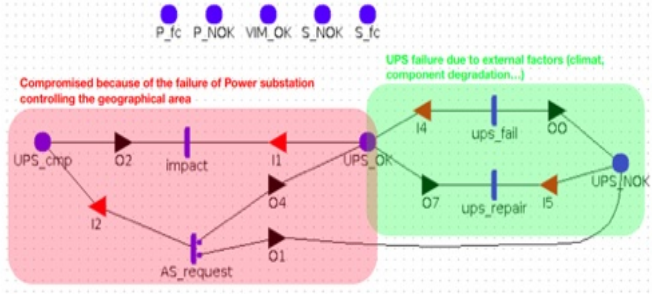


Fig. 7: SAN model of the ***UPS*** subsystem. The highlighted refers to independent dynamics that may affect the subsystem available state.

B. Composed models

As evoked previously, the atomic SAN models of the subsystems represent the lower level of the hierarchical model. The upper, network-level model is constructed by linking the subsystems to create a *dependency graph*. The previous atomic models are aggregated in *MÃ¶bius* using the *Composed Model* feature to construct the network to simulate. The objective is to study the different choices or strategies in terms of topology design and quantify the impact on steady-state availability of the virtualized services (subsystems ***E*** and ***S***). More precisely, we want to quantify the gain in availability when adopting different topologies (or different redundancy schemes). Therefore, we simulate the topologies illustrated in Fig. 8 alongside their correspondent formalism in *Mobius*. Note that in scenario 2 and 3, we must modify the atomic model of the ***E*** subsystem to include the state of ***S2*** alongside that of ***S1***. The choice of these topologies is done to highlight a situation where a copy of the SDN-C is distributed between two sites ***S1*** and ***S2*** in

order to achieve higher redundancy. The difference between scenarios 2 and 3 lies in the power-domain interconnections where we assume that the power supply of the ***S2*** site is independent of the served EMS in scenario 3 compared to scenario 2 where the power supplies of both SDN-C sites relies on the same region controlled by the served EMS. The objective is to quantify and compare the gain in availability obtained when switching from scenario 1 to scenarios 2 and 3.

V. Simulations

The objective of simulations is to highlight the impact of integration of the knowledge about power domain interdependencies, into the decision process of where to instantiate the redundant copies of virtualized service in the data centers plane. That is, the problem of virtualized services placement is often modeled as an optimization problem where the constraints are formulated to deal only with computing environment constraints (resources capacity, latency, and network bandwidth). However, the power supply of the eDCs composing the protection scheme is assumed to be reliable. In our work, we attempt to shed the light on the importance of adding power-domain information to the decision process in order to deal with the impact of power supply interruption due to specific failure propagation patterns. We argue that these patterns will be more frequent due to the high densification of the eDCs networks supporting CIs operations and because of the geographical proximity between interdependent telecommunication and power subsystems. This could be integrated into the eDCs dimensionning decision process whose objective is to determine the minimum amount of computing resources of eDCs and power backup batteries to be installed to reduce short-term (Operational EXpenditure (OPEX)) and long-term (Capital EXpenditure (CAPEX)) costs of running the virtualized eDCs while reducing service downtime. To this end, two parameters are of interest: an eDC's ability to withstand power outages which is characterized by he UPS backup batteries capacity, and the power control frequency applied by the EMS on power substations under control. This latter parameter is an indicator of the sensitivity of the protection scheme to the degree of renewable energy resources penetration of a certain geographical area and how to include such observation into the protection scheme construction.

The values of failure and repair data parameters are adapted from different sources ([33] [34] [35]) and presented in TABLE I. We conduct experiments to study the sensitivity of the model to different variables as well as different service protection schemes depicted in Fig. 8. In this figure, we show the simulated topologies with the correspondent implementation in *Mobius* using the Graph-Join model. We evaluate the Steady State Availability (SSA) of different subsystems in the network with a focus on virtualized services (subsystems ***S*** and ***E***). Note that, the passage from scenario 1 to scenarios 2 and 3 refers to a situation where a redundancy scheme of the communication services (***S1***) is created.

For the next simulations we variate the parameters *UPS/impact* and *P/LB_power* to study the impact of UPS backup capacity and power control rate respectively. We conduct Monte Carlo simulation with 1000000 samples and the results converge within their respective confidence intervals. First, the steady state availability measures of each subsystems under the reference parameters defined in TABLE I are shown in TABLE II. We observe that the steady state availability measure of subsystems ***S1*** and ***E*** increases significantly (by 40.7% and 24.3% respectively) by increasing the redundancy of the communication service (the passage from scenario 1 to scenarios 2). This increase is more significant when switching to scenario 3 where the eDCs hosting the other redundant copy of the service is independent in the power domain of the power substation controlled by ***E***. In scenario 2, the SSAs measures of subsystems ***S1*** and ***S2*** are approximately the same and both increase when ensuring power independency of ***UPS2*** in scenario 3. Overall, the obtained results are aligned with the initial assumptions of the efficiency of integrating power-domain knowledge to the choice of redundant sites. In addition to the virtualized environment constraints (computing capacity, bandwidth, memory), it is worth to make sure that the eDCs doesn't fall in the failure propagation path. In addition, we showed that emerging failure cascading events due to interdependencies between the EMS and SDN services need to be addressed with joint actions both at the virtualized eDCs and power domains. From a network dimensionning perspective, it is worth to study the trade-off between ensuring local power protection (captured by the parameter *UPS/impact*) and ensuring dynamic, redundant protection of virtualized services (passage from scenario 2 to scenario 3). Moreover, this procedure is more adequate to protect eDCs in regions with high penetration of renewable energy (characterized with high control frequency captured by the parameter *P/LB_power*). In what follows, we provide a detailed study on the impact of both parameters.

Subsystem/Parameter	Definition	Distribution	Value (h^{-1})
S-E/VNF_fail	VNF failure rate	Exp	0.01
S-E/VNF_repair	VNF repair rate	Exp	2.94
S-E/VIM_fail	VIM failure rate	Exp	0.0005
S-E/VIM_sw_repair	VIM software repair rate	Exp	0.02
S-E/VIM_hw_repair	VIM hardware repair rate	Exp	0.048
S/AS_cmp	Compromised auto-scaling	Det	2
S/recover	Recovery process after compromise	Exp	0.125
S/served	Request handling rate	Exp	3
S/switch/cases	Switch success probability	-	0.99
S/inspect	SDN software inspection rate	Exp	2
S/inspect/cases	inspection success probability	-	0.6
E/MTTC	Mean time to compromise EMS	Exp	0.5
E/t1-t2	Software inspection process	Exp	3
E/recover	Recovery process after compromise	Exp	0.125
UPS/UPS_fail	UPS failure rate	Exp	0.004
UPS/UPS_repair	UPS repair rate	Exp	0.125
UPS/impact	backup standby time	Det	3
P/P_failure	*P* failure rate	Exp	0.00005
P/P_repair	*P* repair rate	Exp	0.03
P/p_mttc	*P*'s mean time to be compromised	Exp	2
P/detect	*P*'s software inspection rate	Exp	2
P/LB_power	power load balancing control event rate	Exp	2
P/P_recover	*P*'s recovery process rate	Exp	0.03

TABLE I: Failure and Repair data used in the reference scenario (adapted from [33], [34], and [35]). ***Exp*** refers to Exponential distribution whereas ***Det*** refers to Deterministic distribution (an introduced fixed delay).

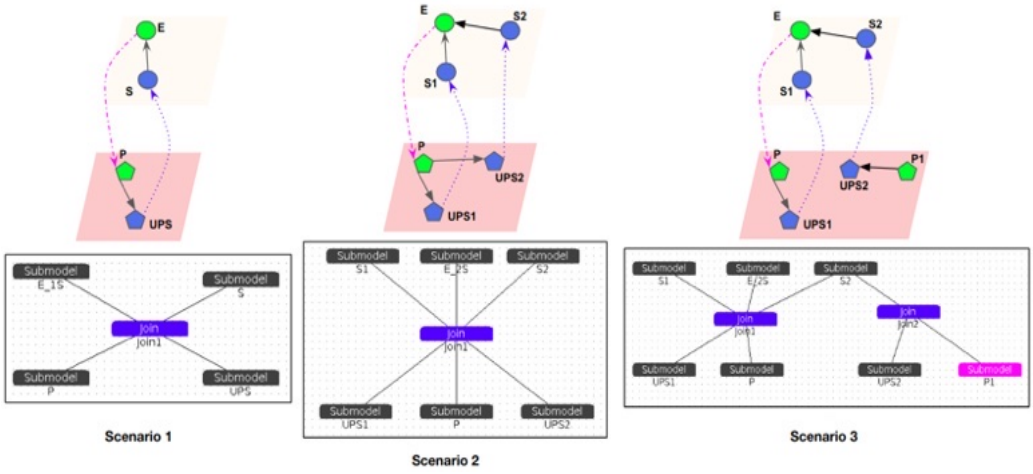


Fig. 8: Graph-Join Model of the different scenarios.

Measure	Scenario 1	Scenario 2	Scenario 3
SSA^{E}	0.745605	0.984982	0.997858
SSA^{S1}	0.575937	0.972332	0.984771
SSA^{S2}	-	0.971048	0.996642

TABLE II: SSA measures for the reference parameters set.

A. The impact of UPS' backup batteries capacity

We study the impact of power outage delay on eDC's services availability by varying the parameter *UPS/impact* which is a delay measured in hours. This parameter characterizes the capacity of the UPS to manage backup batteries and preserve its filtering functions during an abnormal electrical state. The power outage is caused by the application of the wrong EMS control. For subsystems *S1* and *S2*, as shown in figures Fig. 9 and Fig. 10 respectively, an increase in UPS capacity to handle power distribution fluctuations, enhances the service availability (decreasing *(1-SSA)*). For scenario 1, and due to the reliance on only one UPS, the impact of backup capacity shortage is more apparent compared to scenarios 2 and 3 where a redundancy scheme is adopted. When comparing scenarios 2 and 3, we can see clearly that ensuring geographical decoupling of UPS power supply (as in scenario 3), leads to more stable service delivery, compared to scenario 2 where the two *S* subsystems ensuring the protection scheme, are geographically dependent on the same power substation. For subsystem *E*, the results shown in the graph of Fig. 11 show similar behavior as the subsystems *S1* and *S2* due to high dependency. This means that wrong EMS control may have a cascading impact on the service itself due to specific failure propagation patterns. In TABLE III, we show the results for incremental values of the POD (Power Outage Delay) for different subsystems and we notice that the behavior (increase in SSA measure) is common to all subsystems which suggests that failure propagation has been mitigated and that, the external impact on the availability is attenuated. In order to highlight to which extent external failures propagation impacts the SSA measure, we illustrate the frequency of external failures and their contribution to the unavailability in Fig. 9, Fig. 10, and Fig. 11 for subsystems ***S1***, ***S2***, and ***E*** respectively. Note that, *Failure Mode 1* refers to service interruption caused by internal causes (VNF software failure, or shut-down due to eDC hardware failure). Whereas, *Failure Mode 2* refers to failure caused by external factor (***UPS*** failure for ***S*** subsystem and SDN-C failure for the ***E*** subsystem). We start by varying the time that the power UPS backup can sustain a power distribution failure. For the three subsystems and in different scenarios, the results are shown in figures 11, 9, and 10 where the confidence intervals of the results are also represented. We observe that for both subsystems ***E*** and ***S1***, in scenario 1, the steady state unavailability drops when increasing the power backup capacity and that this unavailability is mostly caused by the cascading impact (frequency represented in orange bar). In scenario 2, both subsystems ***S1*** and ***S2*** show the same behaviour when varying the power backup parameter. The unavailability of ***S1*** has dropped by a factor of 10 compared to scenario 1 and the impact of cascading failures decreases with the increase of the backup capacity. The same is observed for subsystem ***E*** whose steady state unavailability measure has decreased by a factor of 10 compared to scenario 1. Also, we observe that the latter subsystem becomes more resilient to cascading failures as the *Failure Mode 1* is more dominant over *Failure Mode 2* in scenario 3.

B. The impact of power control rate

We study the impact of power control rate on eDC's services availability by varying the parameter *P/LB_power*. This parameter characterizes the frequency of event-triggered control which could be an indicator on high penetration of renewable energy sources in a particular geographical area. Higher control frequency might correlates with EMS failure events leading to wrong control that initiates cascading failure events. The obtained results suggest that in regions which require frequent power distribution control, the cascading failures are more frequent. Hence, a resilient protection scheme in the virtualized eDCs domain should be distributed across

Measure	Scenario 1			Scenario 2			Scenario 3		
	POD=0.1	POD=3	POD=6	POD=0.1	POD=3	POD=6	POD=0.1	POD=3	POD=6
SSA E	0.66853	0.74560	0.81231	0.96787	0.98556	0.99023	0.99773	0.99786	0.99788
SSA S1	0.43660	0.57594	0.69951	0.93722	0.97354	0.97941	0.97539	0.98477	0.98830
SSA S2	-	-	-	0.94147	0.97189	0.98097	0.99624	0.99664	0.99716
SSA UPS1	0.52935	0.73555	0.85226	0.94762	0.98282	0.98815	0.98448	0.99188	0.99388
SSA UPS2	-	-	-	0.95789	0.98319	0.98975	0.99893	0.99922	0.99948
SSA P1	0.58061	0.66818	0.75256	0.95602	0.97686	0.97967	0.99034	0.99029	0.99072
SSA P2	-	-	-	-	-	-	0.99973	0.99970	0.99951

TABLE III: Evolution of SSA measures of different subsystems in different scenarios as a function of the UPS backup capacity (expressed as the maximum time before power supply interruption).

Measure	Scenario 1			Scenario 2			Scenario 3		
	PCR=0.1	PCR=1	PCR=5	PCR=0.1	PCR=1	PCR=5	PCR=0.1	PCR=1	PCR=5
SSA E	0.87032	0.72092	0.72345	0.99472	0.98033	0.96948	0.99777	0.99781	0.99784
SSA S1	0.79678	0.54007	0.54061	0.99247	0.96216	0.94027	0.99401	0.97874	0.97557
SSA S2	-	-	-	0.99130	0.96339	0.94208	0.99643	0.99690	0.99665
SSA UPS1	0.89963	0.71181	0.70506	0.99581	0.97442	0.95835	0.99766	0.98772	0.98574
SSA UPS2	-	-	-	0.99654	0.97762	0.96261	0.99911	0.99940	0.99960
SSA P1	0.90725	0.62948	0.61930	0.99548	0.96828	0.94652	0.99826	0.98594	0.98445
SSA P2	-	-	-	-	-	-	0.99972	0.99982	0.99966

TABLE IV: Evolution of SSA measures of different subsystems in different scenarios as a function of the power control rate (which we assume that it reflects the degree of penetration of renewable energies in particular region).

regions with independent power control frequency. In TABLE IV, we show the SSA evolution for different subsystems when varying the power control (or load balancing) rate. We observe that the behaviour of the SSA measure is similar for the different subsystems which suggests that the failure propagation mitigation in one subsystem (or in one domain) has an impact on dependent subsystem's availability. For an in depth analysis of the failure propagation pattern, we illustrate the results depicting the frequency of different failure modes in figures 12, 13, and 14. We observe that for both subsystems ***E*** and ***S1***, in scenario 1, the steady state unavailability increases with high power control rate and that this unavailability is mostly caused by the cascading (external) impact (frequency represented in orange bar). In scenario 2, both subsystems ***S1*** and ***S2*** show the same behaviour when varying the power control rate parameter. The unavailability of ***S1*** has dropped by a factor of 10 compared to scenario 1 and the impact of cascading failures increases with the increase of the power control rate. The same is observed for subsystem ***E*** whose steady state unavailability measure has decreased approximately by a factor of 10 compared to scenario 1. Also, we observe that the frequency of external failure is approximately the same as in scenario 2 for subsystem ***S1*** which is still dependent on the same power substation controlled by ***E***. However, ensuring the decoupling as performed for subsystem ***S2*** in scenario 3 leads to less frequent external failures when comparing in Fig. 14.

C. Sensitivity Analysis

In this section, we perform a sensitivity analysis to study the parameters and their impact on the SSA measures of different virtualized subsystems. One of the drawbacks of model-based availability evaluation is the need to define many parameters whose real value is often unmeasured. The results of the analysis are shown in figures 15, 16, and 17 where the parameters are varied between -75% (inferior (Inf) value) and $+75\%$ (superior (Sup) value) of there reference value. We observe that for subsystem ***E*** in scenario 1, the inspection success probability is the most impacting parameter followed by the MTTC rate. Higher MTTC rate values result in increased vulnerability to the slightest changes in SDN service availability (this service is delivered by subsystem ***S***. Whereas, high inspection success probability means that the system is resilient against anomalies introduced to the misbehaviour of the SDN service. The same is observed for subsystem ***S1*** in scenario 1 sue to the tight coupling between the subsystems. In scenario 2 however, the SSA measures become less sensitive to parameters variations. We observe that power outage delay and the power control rate are most impacting parameters and they are related to external dependent subsystems (***UPS*** and ***P*** respectively). In scenario 3, the variation is 10 times less than the scenario 2 and the model is robust to parameters value fluctuation. For subsystem ***S1***, the ranking of parameters based on their impact on the SSA measure is similar to subsystem ***E***. Also, we observe that the subsystem ***S2*** reacts the same way in scenario 2. However, in scenario 3 ***S2*** is more sensitive to *update_dp_rate* parameter which reflects the increase in data plane update requests. Also, this latter subsystem is also sensitive to switch preference probability which indicates the load balancing preference in terms of data plane update requests between the requesting subsystem ***E*** and SDN-C applications in ***S1*** and ***S2***.

VI. Conclusion

In this paper, we went through the problem of dependability evaluation in interdependent CIs integrating cloud-native management. The cloud-native management is illustrated by the deployment of edge data centers to host critical control applications by means of the vitualization technology. As an example of such CIs, we presented a reference architecture of an SDN-enabled Smart Power Grid in order to highlight emergent interdependencies between ICT and power infrastructure services which may contribute to cross-domain cascading failure. The architecture is used to study the possibility of adopting virtualized services protection schemes while taking into account power-domain knowledge. To this end, we

presented a hierarchical model based on Stochastic activity Network (SAN) formalism to model subsystems dynamics while capturing the impact of cascading failures, evaluate the availability of critical applications, and quantifying the impact of different protection schemes in the virtualization domain on steady-state service-oriented availability measures. The obtained simulation results suggest that ensuring eDCs power supply decoupling leads to more robust protection schemes in the virtualization domain. Also, the installed power backup capacity and the power control rate (as an indicator of the high penetration of renewable energy) are key parameters in our model. These two parameters can be studied in the framework of eDCs dimensionning. We suggest that it is possible for ICT and power operators to coordinate the installation of their eDCs infrastructure in particular geographical regions where the interdependencies patterns we modeled in this work are more relevant. As a perspective for this work, extending the modeling to real-world, network topologies with more subsystems (nodes) can be done to study more complex coupling patterns and failure propagation scenarios. Also, the virtualized services decision process, integrating the power-domain knowledge is to be formulated.

REFERENCES

[1] *IT and OT Convergence - Opportunities and Challenges*, ser. SPE Intelligent Energy International Conference and Exhibition, vol. All Days, 09 2016. [Online]. Available: https://doi.org/10.2118/181087-MS

[2] M. Hoffmann, M. Jarschel, R. Pries, P. Schneider, A. Jukan, W. Bziuk, S. Gebert, T. Zinner, and P. Tran-Gia, "Sdn and nfv as enabler for the distributed network cloud," *Mobile Networks and Applications*, vol. 23, DOI 10.1007/s11036-017-0905-y, 06 2018.

[3] Mijumbi, Rashid and Serrat, Joan and Gorricho, Juan-Luis and Bouten, Niels and De Turck, Filip and Boutaba, Raouf, "Network function virtualization: state-of-the-art and research challenges," *IEEE COMMUNICATIONS SURVEYS AND TUTORIALS*, vol. 18, no. 1, pp. 236–262, 2016. [Online]. Available: http://dx.doi.org/10.1109/COMST.2015.2477041

[4] H. T. Mouftah, M. Erol-Kantarci, and M. H. Rehmani, *Software Defined Networking and Virtualization for Smart Grid*, pp. 171–190, 2019.

[5] M. Panteli and D. S. Kirschen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," in *2011 IEEE/PES Power Systems Conference and Exposition*, DOI 10.1109/PSCE.2011.5772565, pp. 1–7.

[6] P. Wlazlo, K. Price, C. Veloz, A. Sahu, H. Huang, A. Goulart, K. Davis, and S. Zounouz, "A cyber topology model for the texas 2000 synthetic electric power grid," in *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, DOI 10.1109/IPTCOMM.2019.8921260, pp. 1–8, 2019.

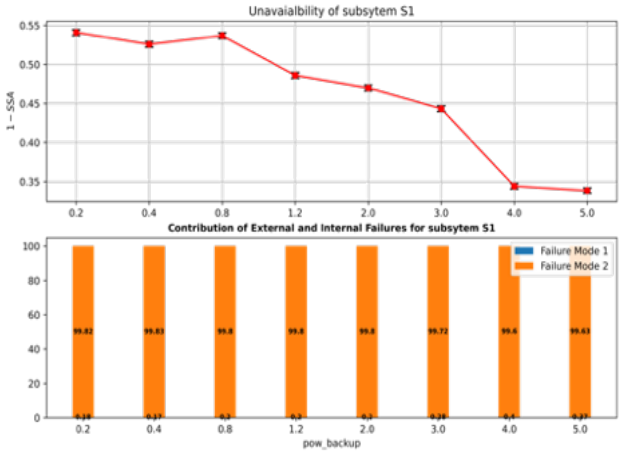
[7] B. Jimada-Ojuolape and J. Teh, "Impact of the integration of information and communication technology on power system reliability: A review," vol. 8, DOI 10.1109/ACCESS.2020.2970598, pp. 24 600–24 615, conference Name: IEEE Access.

[8] Y. Li, X. Li, Y. Zhou, S. Li, and X. Lu, "Impact of cyber failure on cyber-physical distribution system reliability," in *2023 6th International Conference on Energy, Electrical and Power Engineering (CEEPE)*, DOI 10.1109/CEEPE58418.2023.10166112, pp. 714–721.

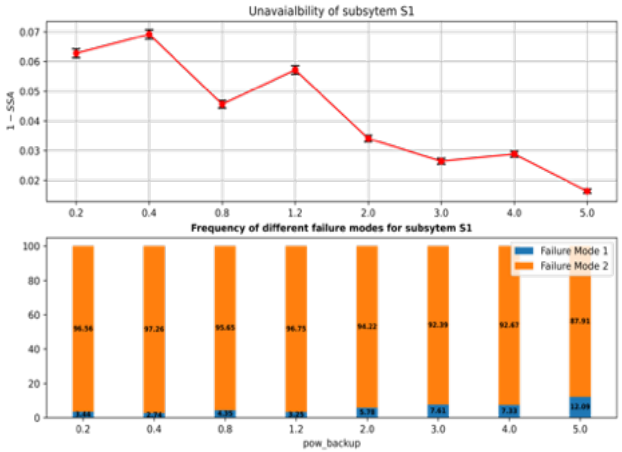
[9] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," vol. 7, DOI 10.1109/MPE.2008.930656, no. 1, pp. 50–60. [Online]. Available: http://ieeexplore.ieee.org/document/4723866/

[10] A. Berizzi, "The italian 2003 blackout," in *IEEE Power Engineering Society General Meeting, 2004.*, DOI 10.1109/PES.2004.1373159, pp. 1673–1679 Vol.2, 2004.

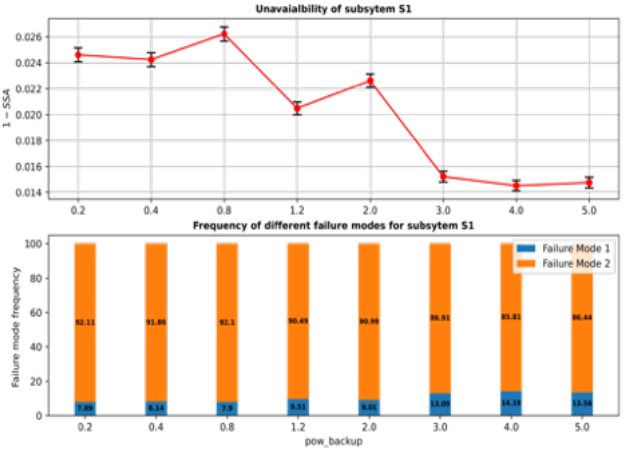
[11] Y. N. Belaid, Y. Fang, Z. Zeng, P. Coudray, A. Legendre, and A. Barros, "Improved modeling of fault propagation, isolation, and fast service restoration in smart grids," *Advances in Modelling to Improve Network Resilience*, p. 56, 2022.



(a) Scenario 1

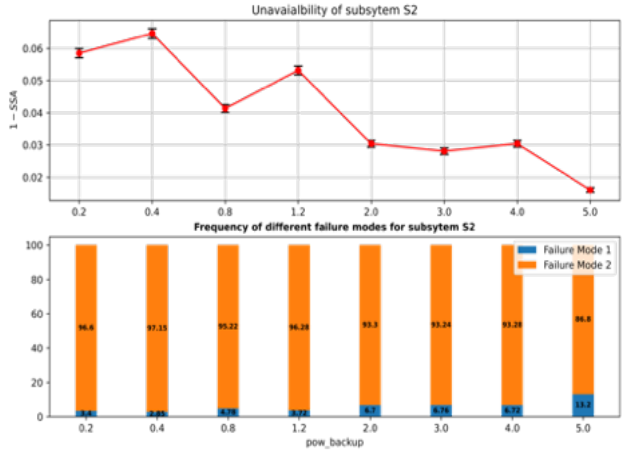


(b) Scenario 2

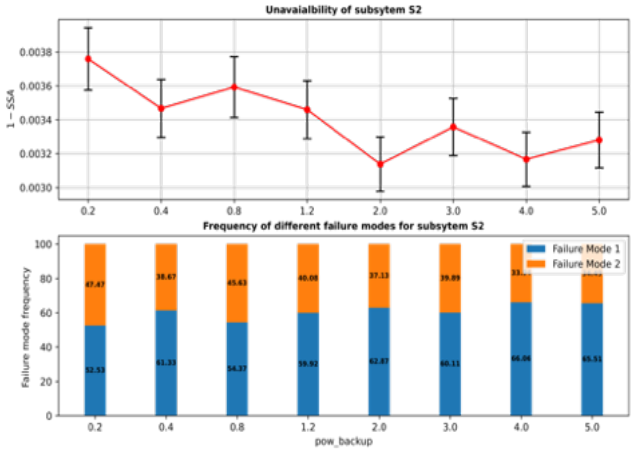


(c) Scenario 3

Fig. 9: $(1-SSA)$ variation of subsystem *S1*, and the frequency of failure modes for different scenarios as a function of **UPS** backup capacity (expressed in hours).



(a) Scenario 2



(b) Scenario 3

Fig. 10: $(1 - SSA)$ variation of subsystem *S2*, and the frequency of failure modes for different scenarios as a function of **UPS** backup capacity (expressed in hours).

[12] M. Rahnamay-Naeini and M. M. Hayat, "Cascading failures in interdependent infrastructures: An interdependent markov-chain approach," *IEEE Transactions on Smart Grid*, vol. 7, DOI 10.1109/TSG.2016.2539823, no. 4, pp. 1997–2006, 2016.

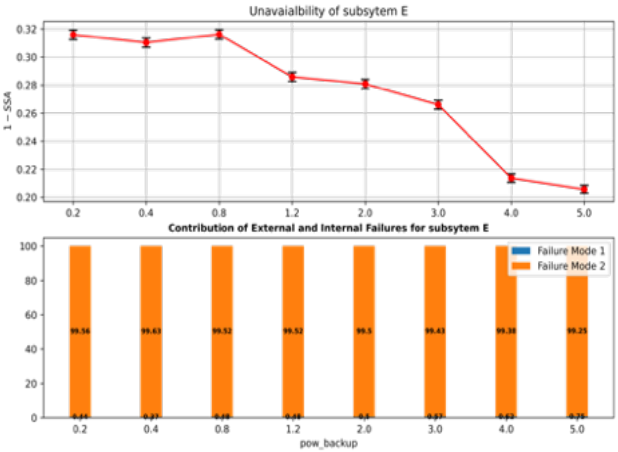
[13] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," vol. 7, DOI 10.1109/TNSE.2018.2872034, no. 2, pp. 817–831, 2020.

[14] A. Aydeger, N. Saputro, K. Akkaya, and S. Uluagac, "Sdn-enabled recovery for smart grid teleprotection applications in post-disaster scenarios," *Journal of Network and Computer Applications*, vol. 138, pp. 39–50, 2019.

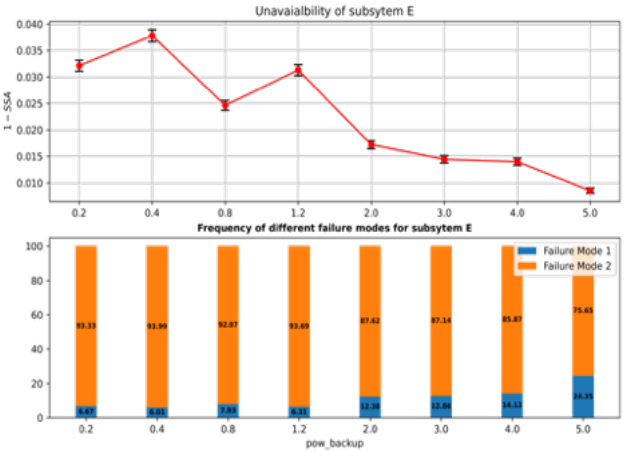
[15] R. Kumar, V. Babu, and D. Nicol, "Network coding for critical infrastructure networks," in *2018 IEEE 26th International Conference on Network Protocols (ICNP)*, DOI 10.1109/ICNP.2018.00061, pp. 436–437, 2018.

[16] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for sdn-enabled smart grids," *Computer Communications*, vol. 133, pp. 1–11, 2019.

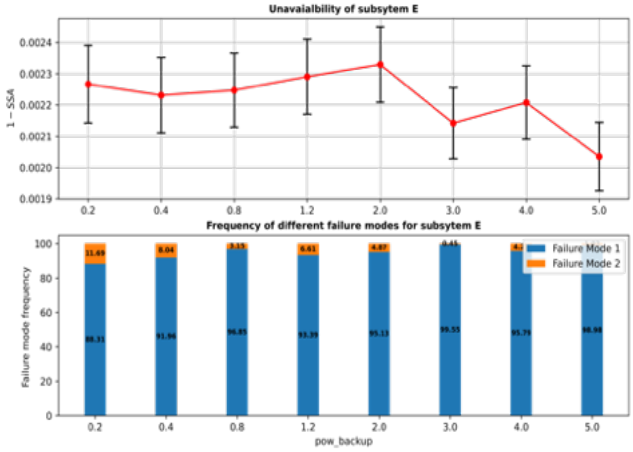
[17] D. Ibdah, M. Kanani, N. Lachtar, N. Allan, and B. Al-Duwairi, "On the security of sdn-enabled smartgrid systems," in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pp. 1–5. IEEE, 2017.



(a) Scenario 1

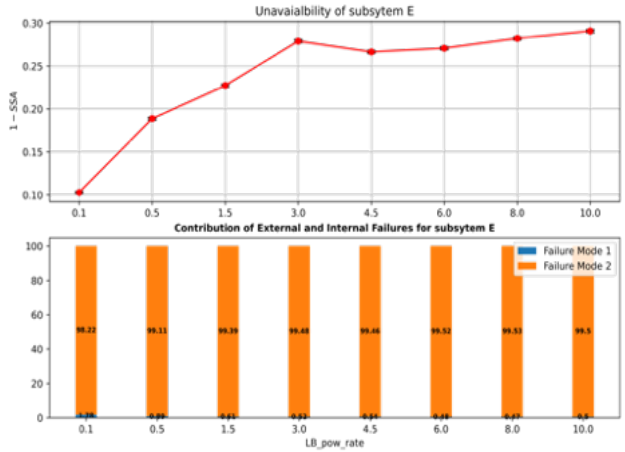


(b) Scenario 2

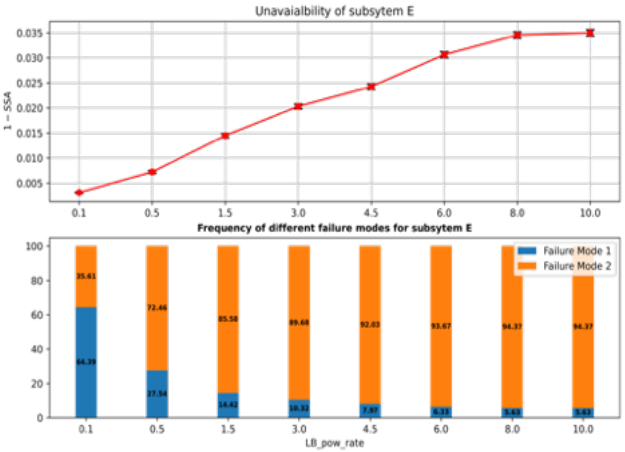


(c) Scenario 3

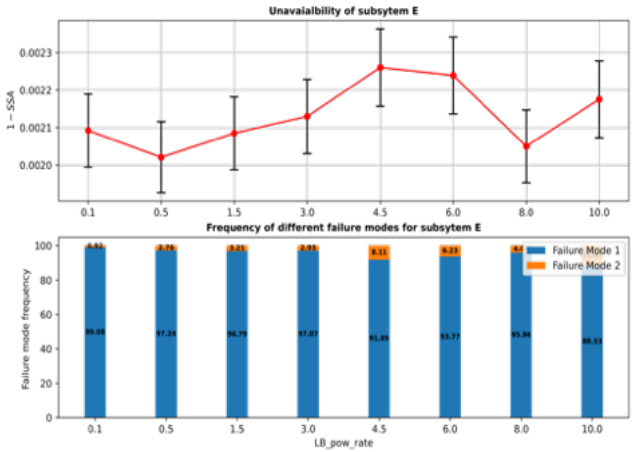
Fig. 11: $(1-SSA)$ variation of subsystem *E*, and the frequency of failure modes for different scenarios as a function of **UPS** backup capacity (expressed in hours).



(a) Scenario 1

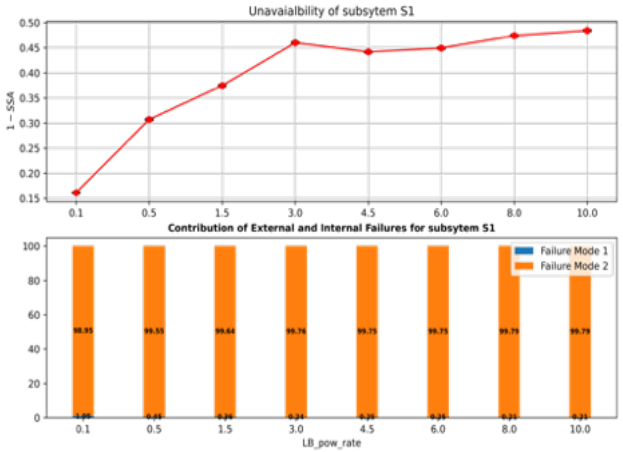


(b) Scenario 2

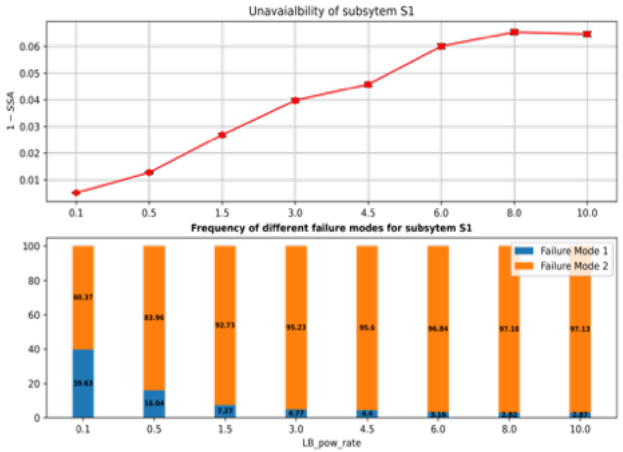


(c) Scenario 3

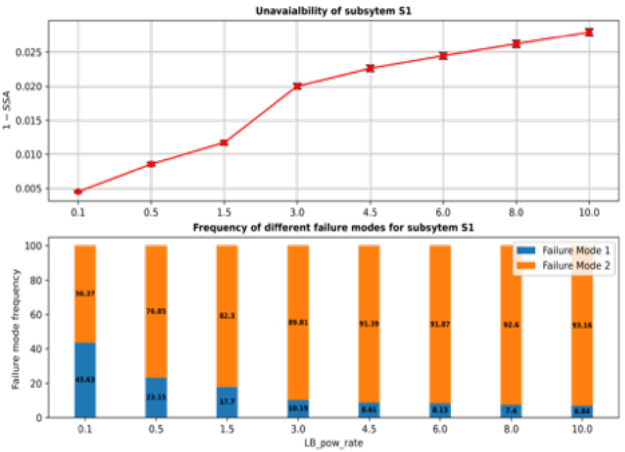
Fig. 12: $(1-SSA)$ variation of subsystem *E*, and the frequency of failure modes for different scenarios as a function of *Power Control Rate (PCR)*.



(a) Scenario 1

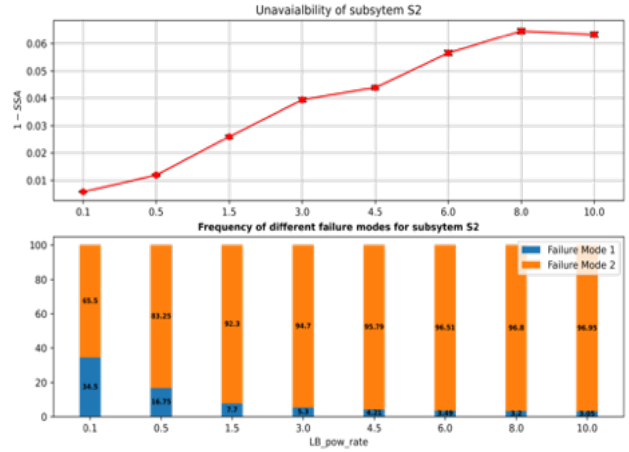


(b) Scenario 2

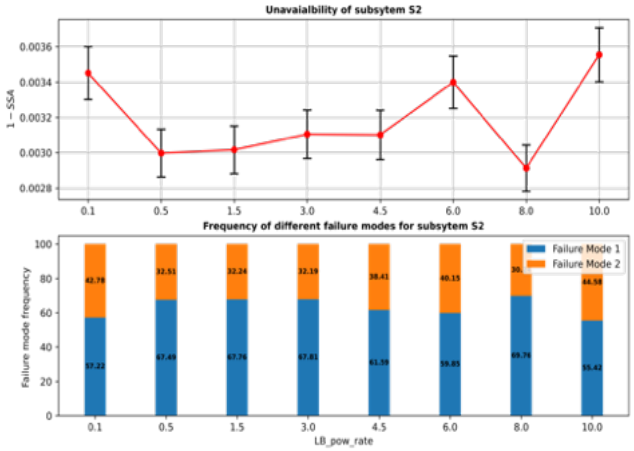


(c) Scenario 3

Fig. 13: $(1-SSA)$ variation of subsystem *S1*, and the frequency of failure modes for different scenarios as a function of *Power Control Rate (PCR)*.



(a) Scenario 2



(b) Scenario 3

Fig. 14: $(1 - SSA)$ variation of subsystem *S2*, and the frequency of failure modes for different scenarios as a function of the *Power Control Rate (PCR)*.

[18] M. Abdelkhalek, B. Hyder, M. Govindarasu, and C. G. Rieger, "Moving target defense routing for sdn-enabled smart grid," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 215–220. IEEE, 2022.

[19] S. Gaonkar, E. Rozier, A. Tong, and W. H. Sanders, "Scaling file systems to support petascale clusters: A dependability analysis to support informed design choices," in *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*, DOI 10.1109/DSN.2008.4630107, pp. 386–391. IEEE. [Online]. Available: http://ieeexplore.ieee.org/document/4630107/

[23] E. Torres, G. Callou, and E. Andrade, "A hierarchical approach for availability and performance analysis of private cloud storage services," *Computing*, vol. 100, no. 6, pp. 621–644, 2018.

[20] C. Zhang, A. G. Kumbhare, I. Manousakis, D. Zhang, P. A. Misra, R. Assis, K. Woolcock, N. Mahalingam, B. Warrier, D. Gauthier, L. Kunnath, S. Solomon, O. Morales, M. Fontoura, and R. Bianchini, "Flex: High-availability datacenters with zero reserved power."

[21] B. Tola, Y. Jiang, and B. E. Helvik, "Model-driven availability assessment of the NFV-MANO with software rejuvenation," vol. 18, DOI 10.1109/TNSM.2021.3090208, no. 3, pp. 2460–2477. [Online]. Available: https://ieeexplore.ieee.org/document/9459426/

[22] T. A. Nguyen, D. Min, E. Choi, and T. D. Tran, "Reliability and availability evaluation for cloud data center networks using hierarchical models," *IEEE Access*, vol. 7, pp. 9273–9313, 2019.

[24] B. Tola, G. Nencioni, B. E. Helvik, and Y. Jiang, "Modeling and evaluating NFV-enabled network services under different availability modes," in *2019 15th International Conference on the Design of Reliable Communication Networks (DRCN)*, DOI 10.1109/DRCN.2019.8713765, pp. 1–5. IEEE. [Online]. Available: https://ieeexplore.ieee.org/document/8713765/

[25] J. Zhu, N. Huang, J. Wang, and X. Qin, "Availability model for data center networks with dynamic migration and multiple traffic flows," DOI 10.1109/TNSM.2023.3242321, pp. 1–1, conference Name: IEEE Transactions on Network and Service Management.

[26] M. K. Rahmat and S. Jovanovic, "Reliability and availability estimation of DC uninterruptible power supply systems using monte-carlo simulation," in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, DOI 10.1109/INDIN.2015.7281713, pp. 76–81. IEEE. [Online]. Available: http://ieeexplore.ieee.org/document/7281713/

[27] H. Ito, K. Kaneda, K. Hamamatsu, T. Tanaka, and K. Nara, "Dependability evaluation of substation automation system with redundancy," pp. 713–721, 07 2008.

[28] R. Zeng, Y. Jiang, C. Lin, and X. Shen, "Dependability analysis of control center networks in smart grid using stochastic petri nets," vol. 23, DOI 10.1109/TPDS.2012.68, no. 9, pp. 1721–1730, conference Name: IEEE Transactions on Parallel and Distributed Systems.

[29] C. Nan, I. Eusgeld, and W. KrÃ¶ger, "Analyzing vulnerabilities between SCADA system and SUC due to interdependencies," vol. 113, DOI 10.1016/j.ress.2012.12.014, pp. 76–93. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0951832013000033

[30] O. Moises Levy, "Smart grid ready ups for an even more sustainable data center," website : https://omdia.tech.informa.com/OM019365/Smart-grid-ready-UPS-for-an-even-more-sustainable-data-center, 2021.

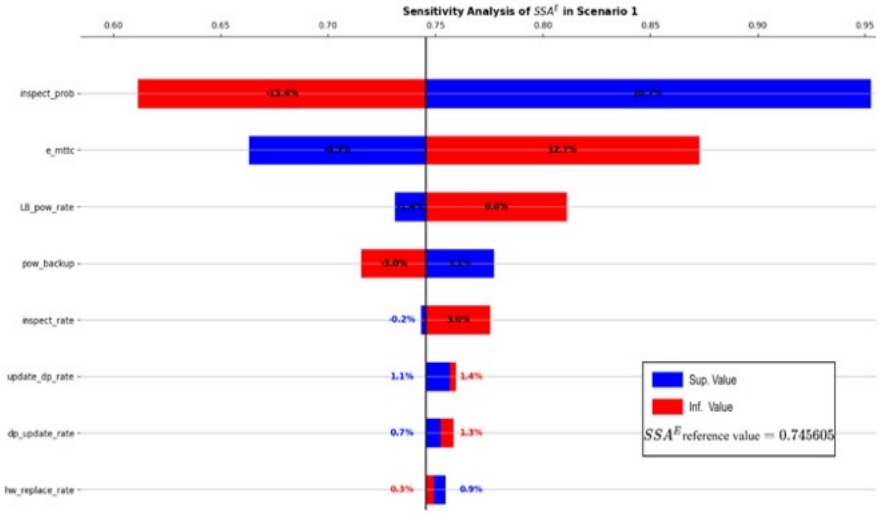
[31] T. Courtney, S. Gaonkar, K. Keefe, E. W. D. Rozier, and W. H. Sanders, "Möbius 2.3: An extensible tool for dependability, security, and performance evaluation of large and complex system models," in *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, DOI 10.1109/DSN.2009.5270318, pp. 353–358. IEEE. [Online]. Available: http://ieeexplore.ieee.org/document/5270318/

[32] K. S. Trivedi and A. Bobbio, *Dependability*, p. 3â14. Cambridge University Press, 2017.

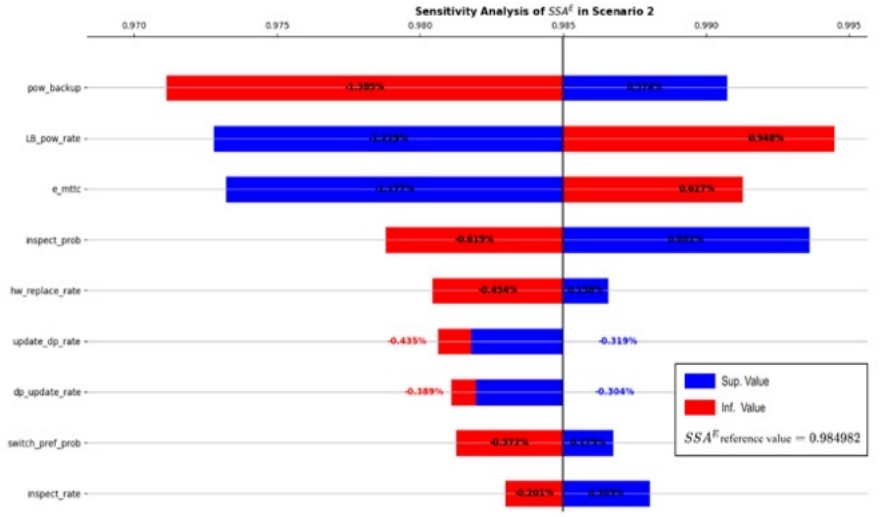
[33] C. Nan and I. Eusgeld, "Exploring impacts of single failure propagation between scada and suc," in *2011 IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1564–1568. IEEE, 2011.

[34] J. Zheng, H. Okamura, T. Dohi *et al.*, "Availability importance measures for virtualized system with live migration," *Applied Mathematics*, vol. 6, no. 02, p. 359, 2015.

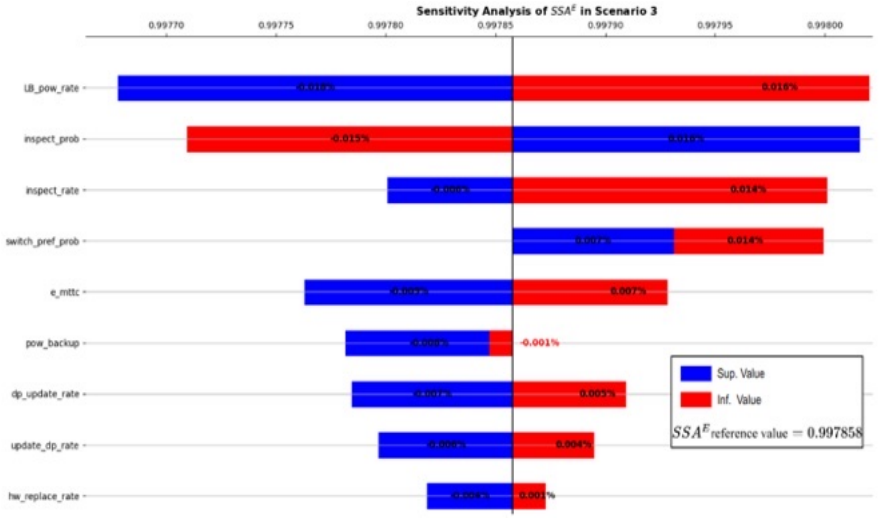
[35] ABB, "White paper: Reliability of uninterruptible power supplies," website : https://power-backup.ro/wp-content/uploads/2018/04/White_Paper_Relibility_150506.pdf, 2006.



(a) Scenario 1

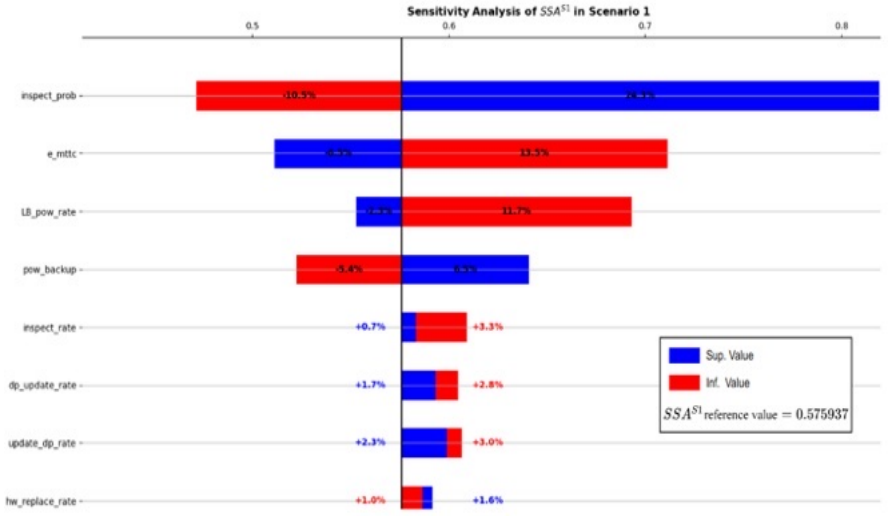


(b) Scenario 2

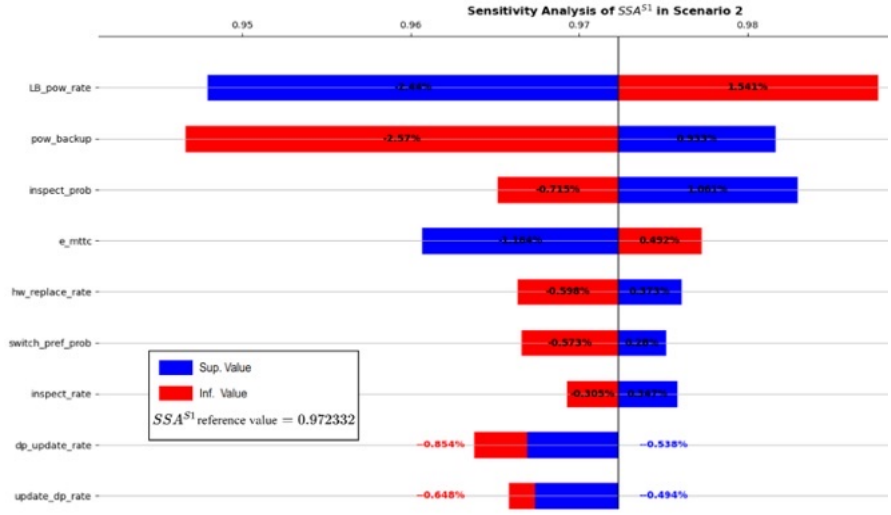


(c) Scenario 3

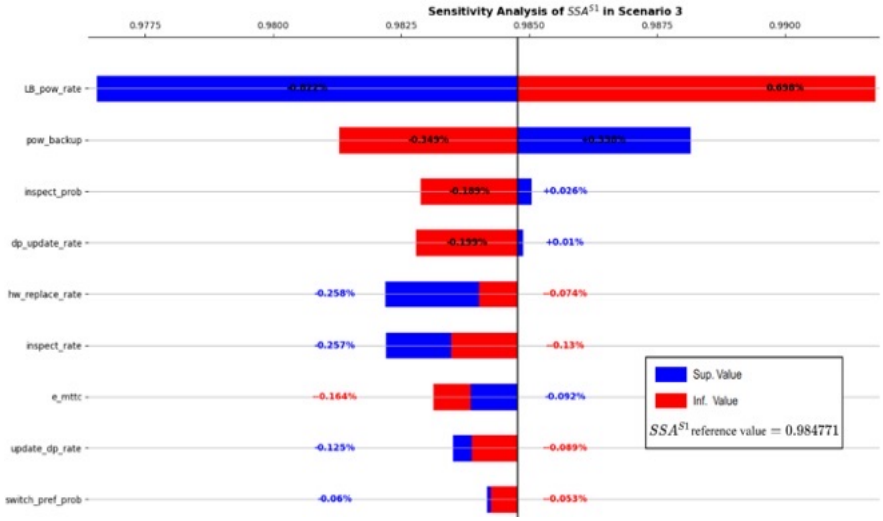
Fig. 15: SSA variation of subsystems E in scenarios 1,2, and 3



(a) Scenario 1

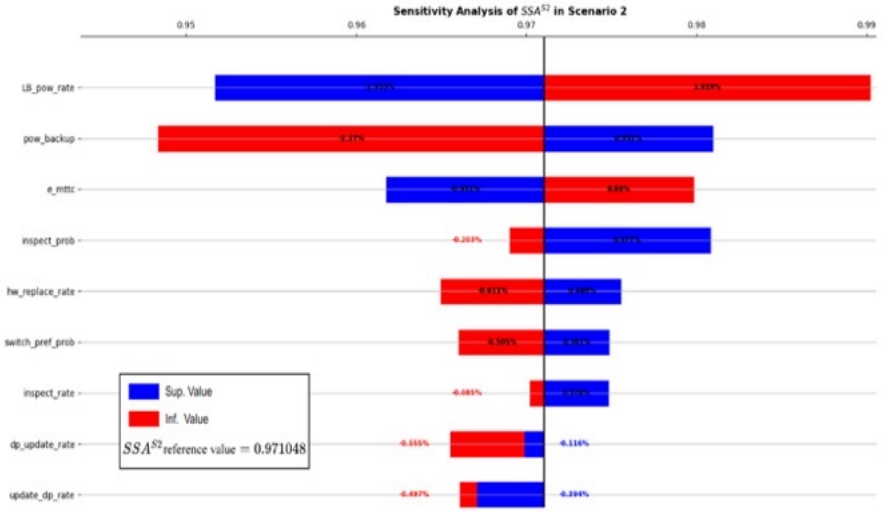


(b) Scenario 2

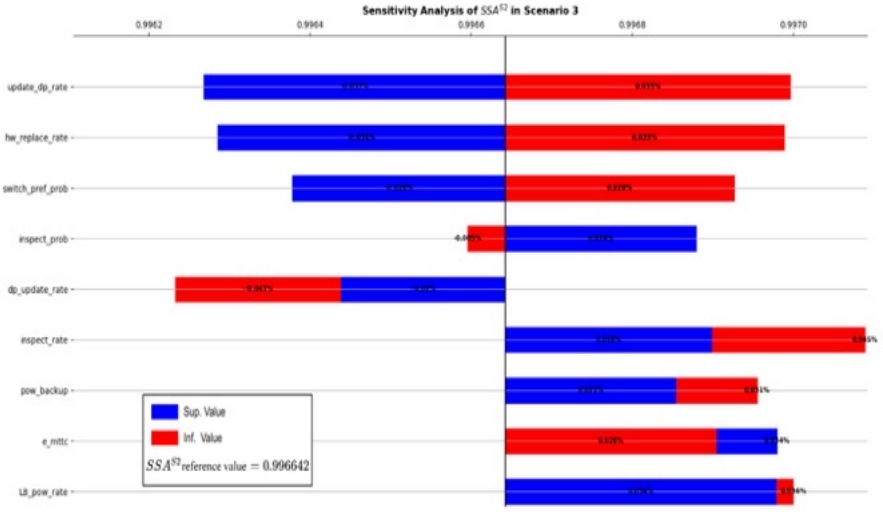


(c) Scenario 3

Fig. 16: SSA variation of subsystem *S1* in scenarios 1,2, and 3



(a) Scenario 2



(b) Scenario 3

Fig. 17: SSA variation of subsystem *S2* in scenarios 2 and 3

D - Paper D

Interdependency-Aware Resource Allocation for High Availability of 5G-enabled Critical Infrastructures Services

Khaled SAYAD[1,2] , Yi-Ping FANG[1] , Anne BARROS[1], Zhiguo ZENG[1], Benoît LEMOINE[2]

[1]*Chaire Risk and Resilience of Complex Systems, Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, 3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France*
E-mail: firstname.lastname@centralesupelec.fr
[2]*Dept. of Infrastructure Innovation and Engineering, Orange Innovation Networks, 2 Avenue Pierre Marzin, 22300 Lannion, France*
E-mail: firstname.lastname@orange.com

The introduction of the fifth generation of mobile technologies (5G) in critical infrastructures (CIs) operations will allow the delivery of more sophisticated critical services. Smart grid, intelligent transportation systems (ITS), and industrial internet of things (IIOT) are examples of 5G-enabled critical infrastructures which are highly dependent on the information and communication technology (ICT) infrastructure. In this work, we propose a collaborative framework that enables critical infrastructures operators (CIOs) to effectively share their data center (DC) infrastructure to achieve cross-domain resilience. Critical services hosted in a DC subject to a disruptive event, for example a maintenance operation, are migrated to a close DC operated by another CI operator. By doing so, we guarantee high service availability and mitigate failure propagation if the hosting DC is dependent on the services impacted by the DC maintenance. Moreover, DC sharing will help CIs operators to optimize their CapEx by avoiding the installation of new edge DCs. We formulate a mixed integer non linear program (MINLP) to model the migration process. Also, an epidemic model is formulated to capture failure propagation, based on which, an interdependency-aware overbooking strategy is designed to increase resource usage and decrease request blocking rate. The model will be tested on real network topologies under different settings.

Keywords: Critical Infrastructure, Resilience, Interdependency, Resource Allocation, Data-center management, Infrastructure sharing.

1. Introduction

Critical infrastructure protection is crucial to ensure an interrupted delivery of vital services like energy, transport, and telecommunication. In order to achieve a CI network-level resilience , different CI operators (CIOs) must coordinate their efforts to withstand interruption events. Due to strong interdependencies, a failure in one CI asset could propagate to other CI assets and cause a large-scale interruption of critical services, resulting in a huge socio-economic impact. In addition, with the rise of 5G as a key technology in future CIOs strategies, the CI network will be more vulnerable to cyber-risks as a result of the massive softwarization of critical services which is a requirement to achieve 5G performances in terms of latency and connectivity Maziku et al. (2019). Furthermore, this new trend in critical services delivery requires a long-term investment in terms of capital expenditures (CapEx) to build the softwarized data center (DC) network supporting the demand for critical services Lam et al. (2020). Our approach is motivated by the homogeneity at the physical infrastructure level, brought by the softwarization of critical services. In contrast to legacy service management and delivery, where services run on dedicated software and hardware resources, 5G-enabled critical services run on Commercial-Off-The-Shelf (COTS) hardware following the same network function virtualization (NFV) standards.

We present a framework for efficient coordination between CIOs at the DC network level. This framework supports CIOs to plan the capacity and geo-distribution of their DCs by taking into account not only internal services requirements but also the vulnerability of other interdependent CIs. During a disruptive event (long power outage,

Proceedings of the 32nd European Safety and Reliability Conference.
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini and Simon Wilson
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_output

maintenance operations, cyber-attacks..), hosted services are migrated to other DCs operated by other CIOs to ensure service continuity and high availability. Our framework performs a service migration process with the objective of minimizing the total migration cost with respect to latency, availability, and interdependency constraints. This paper is organized as follows: in section 2 we present a brief literature review related to coordination and information sharing in critical infrastructures network. In section 3 we formulate the optimization model that maps service migration requests to a set of available DCs. Then, we present the interdependency-aware overbooking strategy allowing maximum resource usage and effective failure mitigation. In section 4, we test the migration model on real-world network topologies from the survivable network library Orlowski et al. (2009). We test different scenarios to assess the efficiency of the overbooking strategy and the effect of the availability of critical information in mitigating failure propagation.

2. Related Work

Coordinating the efforts of interdependent critical infrastructures operators has become a major interest for a nation's security over the past two decades Michel-Kerjan (2003). Information sharing between different operators and stakeholders is considered a key aspect of effective coordination. In Gordon et al. (2003) an economic analysis is carried out to study investment in information security in a network of interdependent entities. The authors demonstrate the effectiveness of information sharing in reducing the overall security breach costs and propose incentive mechanisms to maximize social welfare. The authors in Parrish and Leary (2009) deliver recommendations to secure information sharing between private and public for effective collaboration to withstand disruptive events. In Rinaldi (2004), some challenges towards ensuring a continuous flow of infrastructure data were discussed, among them privacy and economic competitiveness among private stakeholders. More recent efforts like the InfraStress project Denis and al. (2020) Settanni and al. (2017), propose a set of software-based mechanisms for resilience assessment insensitive and large-scale cyber-physical systems. The framework is divided into three layers: data acquisition, situational awareness, and service delivery, and allows service subscribers (stakeholders) to share their experiences in mitigating disruptive events. By doing so, a collective intelligence mechanism emerges, achieving effective coordination. However, the information sharing is restricted to a post-disaster period which doesn't allow the assessing the absorptive resilience capacity of the network.

Privacy has long been a bottleneck to sharing critical information about the state of the infrastructure, this is often due to security concerns. Recent efforts like the European project for Federated Secure Data Infrastructure: GAIA-X (2022) represent a modern solution for secure information sharing. The use case presented in Laskowski (2022) considers the platform as a moderator for secure data provisioning where third-party entities purchase CIs data to develop new business models.

The introduction of cloud technology as part of CIs' operations is fueled by the need to enhance the quality of service (QoS). As explained in Al-Gharibi et al. (2018), the migration towards cloud-based monitoring of critical services offers more flexibility and cost-saving compared to legacy supervisory control and data acquisition (SCADA) systems. However, this adoption exposes the critical services to cyber-risks and sensitive data exposure. This latter issue can be avoided with the building of a private cloud (data centers network). In Niedermeier and de Meer (2016), a comparison between a standardized and a network function virtualization (NFV) architectures for smart metering, shows an enhancement in service reliability. This is achieved thanks to the dynamic redundancy offered by the NFV technologies.

In this work, we take advantage of the flexibility and homogeneity offered by cloud technology to propose a shared resilience scheme between heterogeneous CIs. The contributions of this paper are :

- A framework for cross-domain resilience in CIs network at the data centers

network-level allowing real-time response to disruptive events implicating critical services hosted in softwarized data centers. The framework considers the DCs of different CIOs as one private cloud and dynamically orchestrates resources in response to disruptive events. This approach paves the way for the study of the absorptive capacity of interdependent CIs and their impact on stakeholders' strategies to deal with common risks.

- An interdependency-aware service migration program allowing the mapping of requests to a set of available DCs. In order to achieve high service availability, the model takes into account the failure of the hosts and builds a service protection scheme based on assignment redundancy. In addition, an overbooking strategy is implemented to leverage the coordination between DCs hosting interdependent critical services.

3. A framework for shared resilience

3.1. *Service Migration Process Formulation*

A centralized orchestrator referred to as the critical service management and orchestration (CSMO) handles service migration requests by mapping them to a set of available DCs. A service is characterized by the number of virtual resources required to run the software components composing it. Also, each request is associated with service latency and availability requirements. High availability is achieved through assignment redundancy. A service is simultaneously migrated to a primary host DC that may fail with a certain probability, and other DCs, forming an active-standby redundancy scheme. The number of backups is an output of the service migration scheduler.

The problem of migrating critical services to available DCs considering cost and capacity constraints can be formulated as a capacitated reliable facility location problem Chantre and da Fonseca (2018). Assuming that the disruptive event is a maintenance operation causing DC unavailability, we define the problem parameters:

parameter	definition
I	Set of DCs subject to maintenance intervention.
K^i	Set of services impacted by the maintenance of DC $i \in I$
J	Set of available hosts DC
c_{ki}	Resource amount request of service $k \in K^i$
θ_{ki}	Maximum latency violation allowed for service k
A_{ki}	Availability requirement of service $k \in K^i$
f_j	The setup cost of a DC j (energy consumption, rack and servers installation related costs)
λ_j	Resource usage cost (generated from renting one unit computing resource in DC j)
κ_j	The total capacity available of the host DC j.
q_j	Failure probability of DC j
t_{ij}	Data transmission latency between two connected DC i and j

Table 1.: Model Parameters

The decision is captured by the binary variables Y_{kijr}, with :

$$Y_{kijr} = \begin{cases} 1, \text{ if DC } j \text{ is chosen as } r^{th} \text{ backup} \\ \text{for demand } (k,i) \\ 0, \text{ otherwise} \end{cases}$$

The service protection scheme is designed so that a service (k,i) is assigned to more than one DC, depending on its availability requirement. The service is running actively only in one DC j as r^{th} backup and in standby mode in the other backups $m \in J/\{j\}$ ($Y_{kimx} = 1, x > r$). For example, $r = 1$ is the primary assignment, $r = 2$ is the first backup and so on. Considering that a host j may

fail with a probability q_j, we define the probability that a service $k \in K^i, i \in I$ is active in its r^{th} backup j :

$$\mathbb{P}_{kijr} = (1-q_j) \sum_{m \in J/\{j\}} \frac{q_m}{1-q_m} \mathbb{P}_{kim(r-1)} Y_{kim(r-1)} \tag{1}$$

This probability is calculated for a DC j as r^{th} backup, assuming that the $(r-1)^{th}$ backup DC m ($m \neq j$) fails with a probability q_m. The summation in Equation 1 is reduced to one element (where $Y_{kim(r-1)} = 1$). If a DC j is chosen to host two services from two different CI, the setup cost is paid by the two tenants. In addition, the cost of using the resources at full capacity in active mode (the product $c_{ki}\lambda_j$) is generated only if the service is being served by DC j at level r with probability $\mathbb{P}_{kijr}$. Note that, $\mathbb{P}_{kijr}$ is a decision variable as it is function of $Y_{kij(r-1)}$. We formulate the optimization problem :

$$\min_{Y_{kijr}} \sum_{i \in I} \sum_{k \in K^i} \sum_{j \in J} \sum_{r=1}^{|J|} (f_j + c_{ki}\lambda_j \mathbb{P}_{kijr}) Y_{kijr} \tag{2}$$

s.t:

$$\sum_{r=1}^{|J|} \sum_{i \in I} \sum_{k \in K^i} c_{ki} Y_{kijr} \leq \kappa_j, \quad \forall j \in J \tag{3}$$

$$(\theta_{ki} - t_{ij}) Y_{kijr} \geq 0, \forall k \in K^i, i \in I, j \in J, \forall r \tag{4}$$

$$\sum_{j \in J} Y_{kijr} \leq 1, \forall k \in K^i, i \in I, \forall r \tag{5}$$

$$\sum_{r=1}^{|J|} Y_{kijr} \leq 1, \forall k \in K^i, i \in I, j \in J \tag{6}$$

$$Y_{kijr} \leq Y_{kij(r-1)}, \forall k \in K^i, i \in I, j \in J, \forall r \tag{7}$$

$$\mathbb{P}_{kijr} = (1-q_j) \sum_{m \in J/\{j\}} \frac{q_m}{1-q_m} \mathbb{P}_{kim(r-1)} Y_{kim(r-1)} \tag{8}$$

$$\sum_{j \in J} \sum_{r=1}^{|J|} \mathbb{P}_{kijr} Y_{kijr} \geq A_{ki}, \forall k \in K^i, i \in I \tag{9}$$

$$Y_{kijr} \in \{0,1\}, \forall k \in K^i, i \in I, j \in J, \forall r \tag{10}$$

Constraint 3 ensures that the sum of resource demands doesn't exceed the total capacity of the host j. Constraint 4 ensures that the latency between the chosen host j and affected DC i doesn't exceed the latency violation threshold. Constraint 5 forces the process to choose at least one host DC for each request. Constraint 6 ensures the assignment to one DC j at each backup level r. Constraint 7 guarantees the service activation order in the DCs forming the protection scheme (passing from standby to active mode). Constraint 9 guarantees the minimum number of backups to reach the desired availability for service k. Constraints 8 and 10 highlight the definition and domain of the decision variables. Note that, the process is forced to choose a minimum number of backups to satisfy the availability requirements with the minimum cost.

The objective function and constraint 9 are nonlinear as they include a product of two binary decision variables $\mathbb{P}_{kijr}$ and Y_{kijr}. We linearize them by introducing an auxiliary variable Γ_{kijr} McCormick (1976):

$$\Gamma_{kijr} = \mathbb{P}_{kijr} Y_{kijr} \tag{11}$$

$$\Gamma_{kijr} \leq Y_{kijr} \mathbb{P}^u \iff \Gamma_{kijr} \leq Y_{kijr} \tag{12}$$

$$\Gamma_{kijr} \leq \mathbb{P}_{kijr} \tag{13}$$

$$\Gamma_{kijr} \geq \mathbb{P}_{kijr} - (1 - Y_{kijr}) \mathbb{P}^u \iff \Gamma_{kijr} \geq \mathbb{P}_{kijr} + Y_{kijr} - 1 \tag{14}$$

$$\Gamma_{kijr} \geq 0 \tag{15}$$

$\forall (k \in K^i, i \in I), j \in J, r \in \{1,2,...|J|\}$. With $\mathbb{P}^u = 1$ is the upper bound of the continuous variable $\mathbb{P}_{kijr}$.

3.2. *Interdependency-aware overbooking startegy*

3.2.1. *Epidemic model for failure propagation*

In this section, we model the cascading failure impact caused by the rejection of a service migration request on critical services dependent on that request. Interdependency is quantified in our model as the probability of inoperability of a DC j due to the inoperability of a interdependent

DC i. Considering the DC network as a graph $G(V,E)$ of $|V|$ vertices and $|E|$ edges, two DCs i and j are interdependent if the link $(i,j) \in E$. We use the same approach presented in Lelarge and Bolot (2008) to model the cascading impact of failures in a network of interdependent nodes. We define the state of a DC i by S_i. If i is subject to a maintenance intervention: $S_i = 1$, otherwise: i is healthy ($S_i = 0$). For two DCs i and j in the network: if link $(i,j) \in E$ and $S_i = 1$, then j is contaminated (failure propagates from i to j represented by $\mathrm{C}_{ij} = 1$) with a probability $P(\mathrm{C}_{ij} = 1) = \tau = 1 - P(\mathrm{C}_{ij} = 0)$, where C_{ij} is a Bernoulli variable of parameter τ. We assume that $\mathrm{C}_{ij} = \mathrm{C}_{ji}$ and no possible recovery, so if a DC is contaminated, then it will be out of service until the maintenance intervention. Note that, we use the notation "*DCs i and j are interdependent*" as equivalent to "*services K in DCs i and j are interdependent* ".

3.2.2. *overbooking policy*

The protection scheme modeled in 3.1 presents some drawbacks regarding optimal resource usage in host DCs. Resources reserved in backup DCs are locked for new requests but might not be used if the primary assignment ($r = 1$) doesn't fail during the maintenance operation of the impacted DCs. This would make the capacity constraint infeasible for upcoming requests, and hence, increase the request rejection rate and accelerate failure propagation. To avoid this situation, we implement an overbooking strategy taking into account the probability of contagion of j due to the failure of i. The admission of a service (k,i) to a DC j doesn't depend only on the host's resources capacity, but also on the dependency of services in j on service (k,i). We present the overbooking policy pseudo-code 1. The variable κ_j^{ob} is the new capacity of DC j after applying the overbooking. The variable *guests* contains all the anterior requests already fulfilled by j and not yet freed (ongoing maintenance in their original DCs). The resources reserved as standby by some requests are overbooked by j to host a interdependent service (k,i) where $P(\mathrm{C}_{ij} = 1)$ exceeds some threshold. This policy is applied to all $j \in J$, by doing so, the constraint 3 can be rewritten:

$$\sum_{r=1}^{|J|} \sum_{i \in I} \sum_{k \in K^i} c_{ki} Y_{kijr} \leq \kappa_j^{ob}, \quad \forall j \in J$$

Algorithm 1: Overbooking Policy

Input: $i, j, \kappa_j, guests$
Output: κ_j^{ob}: the new capacity of DC j seen by request i
$\kappa_j^{ob} \leftarrow \kappa_j$
if $P(\mathrm{C}_{ij} = 1) > threshold$ **then**
  for $g \in guests$ **do**
    if j *is not primary assignment* **then**
      $\kappa_j^{ob} \leftarrow \kappa_j^{ob} +$ (reservation of g)
    end
  end
end
return κ_j^{ob}

4. Simulation

The simulations were conducted on an Ubuntu 20.04 computer with 8 Intel i5/1.60 GHz CPU cores. The migration process programs were developed using *Python* programming language and *CPLEX* CPLEX (2015) solver to implement the MILP model. We test the migration process over 100 periods on different network topologies specified in Table 2 with *Av_ND* is the average node degree of each network. For each period, several migration requests are generated randomly and treated as in a first-in-first-out queuing model for a number of cycles equal to the number of demands. Cost parameters, f_j and λ_j are the same for each DC. Capacities κ_j are fixed over the simulation periods. A demand is characterized by a tuple $\{c_{ki}, \theta_{ki}, A_{ki}\}$. The latency parameters θ_{ki} were chosen so that only a few nodes can serve the latency requirement. We set the repair period to be equal to more than one, i.e: resources are reserved and cannot be assigned for the next request in the queue at least for 1 cycle.

Table 2.: Networks Characteristics Orlowski et al. (2009)

Network	$\|V\|$	$\|E\|$	Av_ND
France	25	45	3.60
Cost 266	37	57	3.08
Atalanta	15	22	2.93
Di-yuan	11	42	7.64
Dfn-g	11	47	8.55

To study the impact of critical services interdependencies on failure propagation, we set the parameters A_{ki} and q_j so that each request is migrated to more than one DC. Furthermore, we set the repair period to be more than one to capture the impact of overbooking. We implement the overbooking strategy introduced in 3.2 and calculate the ratio of impacted nodes IN_{OB} with :

$$IN_{OB} = \frac{\text{number of contagions}}{\text{total number of nodes}}$$

and service rejection rate RR_{OB} with:

$$RR_{OB} = \frac{\text{number of requests rejected}}{\text{total number of requests}}$$

We compare to a scenario where the overbooking strategy is not applied and obtain the results illustrated in Fig. 1a. The obtained results show a small decline in service rejection rate when adopting the overbooking strategy for the two networks *France* and *Di-yuan*.

To study the impact of critical information availability prior to the migration process, we compare the previous results with a "Protection" setting where the nodes with the highest betweenness centrality measure are considered to be critical and are protected (don't fail during the simulation). Betweenness centrality quantifies the presence of the node in the shortest paths between all pairs of other nodes in the network:

$$B_c(v) = \sum_{s,t \in V} \frac{\sigma(s,t|v)}{\sigma(s,t)}$$

Where $B_c(v)$ is the betweenness centrality measure of node v in network with vertices set V. $\sigma(s,t)$ is the set of all shortest path between nodes s and t and $\sigma(s,t|v)$ is the subset that contains only the paths passing by v. The betweeness centrality measures of the networks used in the simulation, are presented in Table 3.

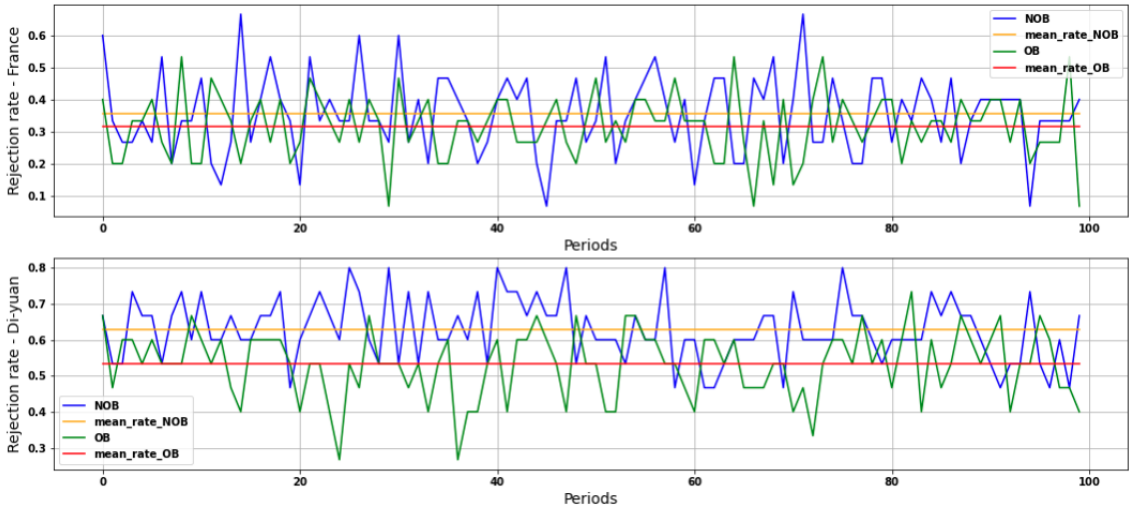
Table 3.: $B_c(v)$ measures of the networks

Network	$Mean(B_c)$	$Std(B_c)$	$Max(B_c)$
France	0.39	0.07	0.58
Cost 266	0.27	0.03	0.34
Atalanta	0.40	0.05	0.50
Di-yuan	0.81	0.04	0.90
Dfn-g	0.89	0.11	1.00

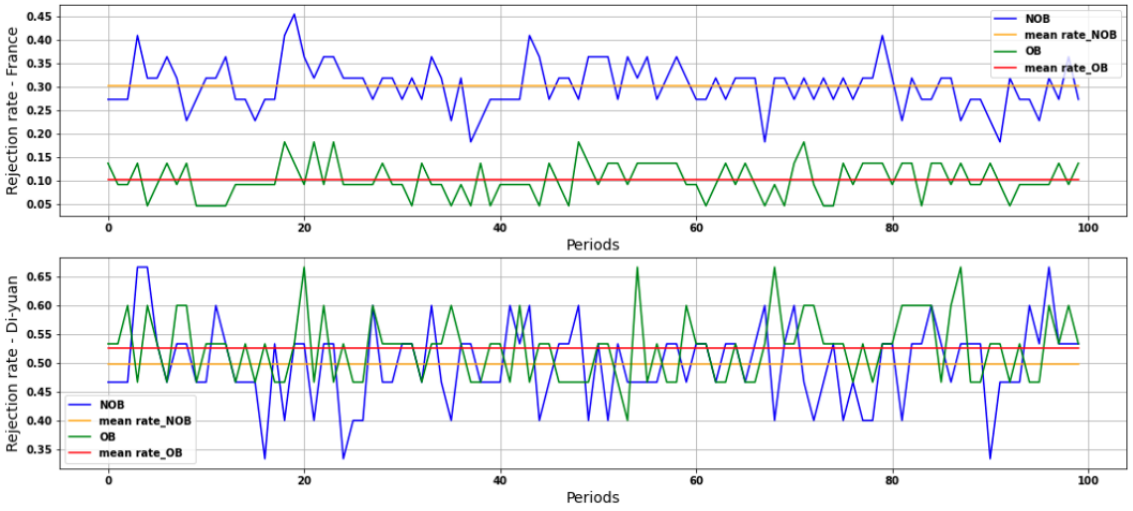
We follow the same steps as in the previous "No Protection" setting simulation to obtain the results illustrated in Fig.1b. The rejection rate has dropped compared to the "No protection" setting. The drop is more important in the *France* network compared to the *Di-yuan* network when adopting an overbooking strategy. The complete results are presented in Tables 4 and 5. Comparing the "Protection" and "No Protection" settings, we notice a reduction in the rejection rate and failure propagation when adopting an interdependency-aware overbooking strategy. However, the amount of drop in rejection rate differs depending on topology characteristics. In networks with a low number of nodes and high average node degree (*Di-yuan* and *Dfn-g*), the decrease in rejection and contagion rates is less visible compared to larger networks. In addition, the adoption of a protection scheme in these networks is irrelevant as all the nodes have the same criticality value (Table 3). While the overbooking strategy impacts the capacity of the host and makes the constraint 3 feasible for some requests, the protection of the nodes with the highest B_c value ensures the fulfillment of the latency requirements of different requests. Nodes with a high B_c value are more probable to host a request generated at any node in the network due to their topological centrality which favors them to fulfill latency requirements.

5. Conclusion & Perspective

In this work, we proposed a framework to support CIs operators' coordination at their DC network level. Sharing DCs resources between interdependent CIs represent a promising solution to mitigate



(a) The rejection rate dynamics in a "No Protection Setting"



(b) The rejection rate dynamics in a "Protection Setting"

Fig. 1.: Rejection rate dynamics

Table 4.: Simulation results - No Protection Setting

Network	$Mean(RR_{NOB})$	$Std(RR_{NOB})$	IN_{NOB}	$Mean(RR_{OB})$	$Std(RR_{OB})$	IN_{OB}
France	0.319	0.046	0.197	0.200	0.040	0.134
Cost266	0.100	0.020	0.064	0.085	0.020	0.060
Atalanta	0.391	0.063	0.269	0.352	0.033	0.240
Di-yuan	0.612	0.071	0.503	0.571	0.074	0.477
Dfn-g	0.396	0.073	0.366	0.312	0.062	0.296

the cascading impact of failures and support CIs operators to better dimension their DCs network and therefore, reduce their CapEx. We studied the use case of planned DC maintenance as a disruptive event where a mixed-integer linear program was formulated to model the service migration

Table 5.: Simulation results - Protection setting

Network	$Mean(RR_{NOB})$	$Std(RR_{NOB})$	IN_{NOB}	$Mean(RR_{OB})$	$Std(RR_{OB})$	IN_{OB}
France	0.303	0.050	0.170	0.110	0.037	0.072
Cost266	0.0759	0.023	0.050	0.070	0.021	0.047
Atalanta	0.381	0.077	0.247	0.332	0.074	0.222
Di-yuan	0.499	0.070	0.372	0.525	0.057	0.375
Dfn-g	0.473	0.057	0.368	0.426	0.069	0.320

process. An epidemic model was presented to capture the cascading effect of service migration request blocking. In addition, an overbooking strategy is implemented with the objective to lower the request rejection rate. The results have shown an improvement in service acceptance rate and better mitigation of the effect of cascading failure. Protecting critical nodes in the network has shown a remarkable enhancement compared to a non-protection scenario. However, the efficiency of the overbooking and protection strategies depends on the topology of the network. More precisely, the number of nodes and link distribution. For future work, the effect of overbooking on service availability needs to be studied alongside the problem of DC capacity planning.

Acknowledgement

This work is funded by Orange/EDF/SNCF in the framework of the Chair on Risk and Resilience of Complex Systems (CentraleSupélec, EDF, Orange, SNCF).

References

Al-Gharibi, M., M. Warren, and W. Yeoh (2018, 10). Risks of critical infrastructure adoption of cloud computing within government.

Chantre, H. D. and N. L. S. da Fonseca (2018). Multi-objective optimization for edge device placement and reliable broadcasting in 5g NFV-based small cell networks. *IEEE Journal on Selected Areas in Communications 36*(10).

CPLEX, I. I. (2015). Ibm ilog cplex optimization studio getting started with cplex, v12 release 6. *International Business Machines Corporation*, 130.

Denis and A. J. L. R. L. S. al., Caleta (2020). Infrastress: Enhancing resilience of industrial plants against cyber-physical threats. *The Italian Conference on CyberSecurity*.

GAIA-X (2022). Gaia-x project: https://www.gaia-x.eu/node/34.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy 22*(6), 461–485.

Lam, P. T., D. Lai, C.-K. Leung, and W. Yang (2020). Data centers as the backbone of smart cities: principal considerations for the study of facility costs and benefits. *Facilities*.

Laskowski, M. (2022). Infrastructure data for new business models: https://www.bmwk.de/redaktion/en/artikel/digital-world/gaia-x-use-cases/infrastructure-data-for-new-business-models.html.

Lelarge, M. and J. Bolot (2008). Network externalities and the deployment of security features and protocols in the internet. *Sigmetrics Performance Evaluation Review - SIGMETRICS 36*(1), 37–48.

Maziku, H., S. Shetty, and D. M. Nicol (2019). Security risk assessment for SDN-enabled smart grids. *Computer Communications 133*.

McCormick, G. P. (1976). Computability of global solutions to factorable nonconvex programs: Part i — convex underestimating problems. *10*(1), 147–175.

Michel-Kerjan, E. (2003). New Challenges in Critical Infrastructures : A US Perspective. working paper or preprint.

Niedermeier, M. and H. de Meer (2016). Constructing dependable smart grid networks using network functions virtualization. *Journal of Network and Systems Management 24*(3), 449–469.

Orlowski, S., R. Wessäly, M. Pioro, and A. Tomaszewski (2009, 01). Sndlib 1.0—survivable network design library. *Networks 55*, 276 – 286.

Parrish, L. and M. Leary (2009). Secure global collaboration among critical infrastructures. *Inf. Sec. J.: A Global Perspective 18*(2), 57–63.

Rinaldi, S. (2004). Modeling and simulating critical infrastructures and their interdependencies. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, pp. 8 pp.–.

Settanni, G. and al. (2017). A collaborative cyber incident management system for european interconnected critical infrastructures. *Journal of Information Security and Applications 34*, 166–182.

Bibliographie

[1] Alessandro Lazari. *European critical infrastructure protection*. Springer, 2014.

[2] Madelene Lindström and Stefan Olsson. *The European Programme for Critical Infrastructure Protection*, pages 37–59. 07 2009.

[3] Ryan K Baggett and Brian K Simpkins. *Homeland security and critical infrastructure protection*. ABC-CLIO, 2018.

[4] Wayne Harrop and Ashley Matteson. Cyber resilience : A review of critical national infrastructure and cyber-security protection measures applied in the UK and USA. In Frederic Lemieux, editor, *Current and Emerging Trends in Cyber Operations : Policy, Strategy and Practice*, pages 149–166. Palgrave Macmillan UK.

[5] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6) :11–25, 2001.

[6] Austen D. Givens and Nathan E. Busch. Realizing the promise of public-private partnerships in u.s. critical infrastructure protection. 6(1).

[7] Godslove Ampratwum, Osei-Kyei Robert, and Professor Tam. Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events : A systematic review. *International Journal of Critical Infrastructure Protection*, 39 :100556, 08 2022.

[8] Kenji Watanabe. *PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan : 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018, Revised Selected Papers*, pages 169–178. 01 2019.

[9] Paul Reilly, Elisa Serafinelli, Rebecca Stevenson, Laura Petersen, and Laure Fallou. *Enhancing Critical Infrastructure Resilience Through Information-Sharing : Recommendations for European Critical Infrastructure Operators*, pages 120–125. 03 2018.

[10] Raffaele Cantelmi, Giulio Di Gravio, and Riccardo Patriarca. Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, 41 :1–36, 09 2021.

[11] Talal Halabi, Aawista Chaudhry, Sarra Alqahtani, and Mohammad Zulkernine. A scary peek into the future : Advanced persistent threats in emerging computing environments. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8, 2022.

[12] Pietro Tedeschi and Savio Sciancalepore. Edge and fog computing in critical infrastructures : Analysis, security threats, and research challenges. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 1–10, 2019.

[13] A. Berizzi. The italian 2003 blackout. In *IEEE Power Engineering Society General Meeting, 2004.*, pages 1673–1679 Vol.2, 2004.

[14] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20(4) :1922–1928, 2005.

[15] Xu Zhiqun, Chen Duan, Hu Zhiyuan, and Sun Qunying. Emerging of telco cloud. *China Communications*, 10(6) :79–85, 2013.

[16] Yacine Khettab, Miloud Bagaa, Diego Leonel Cadette Dutra, Tarik Taleb, and Nassima Toumi. Virtual security as a service for 5g verticals. *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2018.

[17] Christian Tipantuña and Xavier Hesselbach. Nfv/sdn enabled architecture for efficient adaptive management of renewable and non-renewable energy. *IEEE Open Journal of the Communications Society*, 1 :357–380, 2020.

[18] Helen C. Leligou, Theodore Zahariadis, Lambros Sarakis, Eleftherios Tsampasis, Artemis Voulkidis, and Terpsichori E. Velivassaki. Smart grid : a demanding use case for 5g technologies. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 215–220, 2018.

[19] Th. Zahariadis and al. Smart energy as a service network architecture. June 2018. This work is part of the NRG-5 project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 762013.

[20] Erwin Alexander Leal and Juan Felipe Botero. Software defined power substations : An architecture for network communications and its control plane. In *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6, 2016.

[21] Turner and Townsend. Data centre cost index 2022. https://reports.turnerandtownsend.com/dcci-2022/data-centre-cost-trends, 2022. Accessed : 02-08-2023.

[22] Arnaud Braud, Gaël Fromentoux, Benoit Radier, and Olivier Le Grand. The road to european digital sovereignty with gaia-x and idsa. *IEEE Network*, 35(2) :4–5, 2021.

[23] Alfieri and al. Development of the eu green public procurement (gpp) criteria for data centres, server rooms and cloud services, eur 30251 en. *Publications Office of the European Union*, 35(2) :4–5, 2020.

[24] Ola Michalec, Sveta Milyaeva, and Awais Rashid. When the future meets the past : Can safety and cyber security coexist in modern critical infrastructures ? *Big Data & Society*, 9(1) :20539517221108369, 2022.

[25] GSMA. Infrastructure sharing : An overview. https://www.gsma.com/futurenetworks/wiki/infrastructure-sharing-an-overview/, 2019. Accessed : 27-07-2023.

[26] Davide Strusani and Georges Vivien Houngbonon. Accelerating digital connectivity through infrastructure sharing. 2020.

[27] Luis Velasco, Marco Signorelli, Oscar González De Dios, Chrysa Papagianni, Roberto Bifulco, Juan Jose Vegas Olmos, Simon Pryor, Gino Carrozzo, Julius Schulz-Zander, Mehdi Bennis, Ricardo Martinez, Filippo Cugini, Claudio Salvadori, Vincent Lefebvre, Luca Valcarenghi, and Marc Ruiz. End-to-end intent-based networking. *IEEE Communications Magazine*, 59(10) :106–112, 2021.

[28] Kashif Mehmood, H. V. Kalpanie Mendis, Katina Kralevska, and Poul E. Heegaard. Intent-based network management and orchestration for smart distribution grids. pages 1–6, 2021.

[29] Marie-Paule Odini and A. Manzalini. SDN in NFV architectural framework. *IEEE Software Defined Networks Newsletter*, 2016.

[30] Geng Zhang, Jiawen Shi, Shiyan Huang, Jiye Wang, and Hao Jiang. A cascading failure model considering operation characteristics of the communication layer. 9 :9493–9504, 2021.

[31] Agostino Sturaro, Simone Silvestri, Mauro Conti, and Sajal K. Das. A realistic model for failure propagation in interdependent cyber-physical systems. 7(2) :817–831, 2020.

[32] Vincent Messié, Gaël Fromentoux, Nathalie Labidurie Omnes, Benoit Radier, S. Vaton, and Isabel Amigo. Baladin : truthfulness in collaborative access networks with distributed ledgers. *Annals of Telecommunications*, 77, 06 2021.

[33] Babak Mafakheri, Tejas Subramanya, Leonardo Goratti, and Roberto Riggio. Blockchain-based infrastructure sharing in 5g small cell networks. In *2018 14th International Conference on Network and Service Management (CNSM)*, pages 313–317, 2018.

[34] Peter Mell, Tim Grance, et al. The nist definition of cloud computing. 2011.

[35] Tarik Taleb. Toward carrier cloud : Potential, challenges, and solutions. *IEEE Wireless Communications*, 21(3) :80–91, 2014.

[36] Network Function Virtualization ETSI. Architectural framework. *ETSI GS NFV*, 2 :v1, 2014.

[37] Cristina Badulescu and Joan Triay. Etsi nfv, the pillar for cloud ready ict deployments. *Journal of ICT Standardization*, pages 141–156, 2019.

[38] Marie-Paule Odini and A Manzalini. Sdn in nfv architectural framework. *IEEE Software Defined Networks Newsletter*, 2016.

[39] Sumit Badotra and Japinder Singh. Open daylight as a controller for software defined networking. *International Journal of Advanced Research in Computer Science*, 8(5), 2017.

[40] Pankaj Berde, Matteo Gerola, Jonathan Hart, Yuta Higuchi, Masayoshi Kobayashi, Toshio Koide, Bob Lantz, Brian O'Connor, Pavlin Radoslavov, William Snow, et al. Onos : towards an open, distributed sdn os. In *Proceedings of the third workshop on Hot topics in software defined networking*, pages 1–6, 2014.

[41] Chander Prabha, Anjuli Goel, and Jaspreet Singh. A survey on sdn controller evolution : A brief review. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, pages 569–575, 2022.

[42] Network Functions Virtualisation. Etsi gs nfv-inf 005 v1. 1.1 : Network functions virtualization (nfv); infrastructure. *Network Domain," Tech. Rep., Dec*, 2014.

[43] ISGNFV ETSI. Network functions virtualisation (nfv); acceleration technologies; report on acceleration technologies and use cases. *V1*, 1 :2015–12, 2015.

[44] James A Momoh. *Smart grid : fundamentals of design and analysis*, volume 63. John Wiley & Sons, 2012.

[45] Enrique Santacana, Gary Rackliffe, Le Tang, and Xiaoming Feng. Getting smart. *IEEE Power and Energy Magazine*, 8(2) :41–48, 2010.

[46] IEEE. Ieee standard for scada and automation systems. *IEEE Std C37.1-2007 (Revision of IEEE Std C37.1-1994)*, pages 1–143, 2008.

[47] Rakesh Kumar, Vignesh Babu, and David Nicol. Network coding for critical infrastructure networks. In *2018 IEEE 26th International Conference on Network Protocols (ICNP)*, pages 436–437, 2018.

[48] Kilho Lee, Minsu Kim, Hayeon Kim, Hoon Sung Chwa, Jinkyu Lee, and Insik Shin. Fault-resilient real-time communication using software-defined networking. In *2019 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pages 204–215, 2019.

[49] Philip Church, Harald Mueller, Caspar Ryan, Spyridon V Gogouvitis, Andrzej Goscinski, Houssam Haitof, and Zahir Tari. Scada systems in the cloud. *Handbook of Big Data Technologies*, pages 691–718, 2017.

[50] Philip Church, Harald Mueller, Caspar Ryan, Spyridon V. Gogouvitis, Andrzej Goscinski, Houssam Haitof, and Zahir Tari. Moving scada systems to iaas clouds. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, pages 908–914, 2015.

[51] Quoc Tuan Tran, Yvon Besanger, et al. Scada as a service approach for interoperability of micro-grid platforms. *Sustainable Energy, Grids and Networks*, 8 :26–36, 2016.

[52] Van Hoa Nguyen, Quoc Tuan Tran, Hervé Buttin, and Mouloud Guemri. Implementation of a coordinated voltage control algorithm for a micro-grid via scada-as-a-service approach. *Electrical Engineering*, 104(2) :389–399, 2022.

[53] Mao Yi, Harald Mueller, Liu Yu, and Jiang Chuan. Benchmarking cloud-based scada system. In *2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 122–129, 2017.

[54] Murat Kuzlu, Manisa Pipattanasomporn, and Saifur Rahman. Communication network requirements for major smart grid applications in han, nan and wan. *Computer Networks*, 67 :74–88, 2014.

[55] Ralph E Mackiewicz. Overview of iec 61850 and benefits. In *2006 IEEE Power Engineering Society General Meeting*, pages 8–pp. IEEE, 2006.

[56] Patrick Wlazlo, Kevin Price, Christian Veloz, Abhijeet Sahu, Hao Huang, Ana Goulart, Katherine Davis, and Saman Zounouz. A cyber topology model for the texas 2000 synthetic electric power grid. In *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pages 1–8. IEEE, 2019.

[57] Youba Nait Belaid, Patrick Coudray, José Sanchez-Torres, Yi-Ping Fang, Zhiguo Zeng, and Anne Barros. Resilience quantification of smart distribution networks—a bird's eye view perspective. *Energies*, 14(10) :2888, 2021.

[58] Mathaios Panteli, Dimitris N Trakas, Pierluigi Mancarella, and Nikos D Hatziargyriou. Power systems resilience assessment : Hardening and smart operational enhancement strategies. *Proceedings of the IEEE*, 105(7) :1202–1213, 2017.

[59] Tomas E. Dy Liacco. The adaptive reliability control system. *IEEE Transactions on Power Apparatus and Systems*, 5 :517–531, 1967.

[60] Youba Nait Belaid, Yi-Ping Fang, Zhiguo Zeng, Anthony Legendre, Patrick Coudray, and Anne Barros. Resilience optimization of wide-area control in smart distribution grids. *IFAC-PapersOnLine*, 55(16) :136–141, 2022.

[61] OMDIA Moises Levy. Smart grid ready ups for an even more sustainable data center. website : https://omdia.tech.informa.com/OM019365/

Smart-grid-ready-UPS-for-an-even-more-sustainable-data-center, 2021.

[62] IEC 60812 Technical Committee et al. Analysis techniques for system reliability-procedure for failure mode and effects analysis (fmea). *IEC 60812*, 2006.

[63] Marta Chinnici, Davide De Chiara, and Andrea Quintiliani. Data center, a cyber-physical system : Improving energy efficiency through the power management. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, pages 269–272, 2017.

[64] Petra Vizarreta, Poul Heegaard, Bjarne Helvik, Wolfgang Kellerer, and Carmen Mas Machuca. Characterization of failure dynamics in sdn controllers. In *2017 9th international workshop on resilient networks design and modeling (rndm)*, pages 1–7. IEEE, 2017.

[65] Kishor S Trivedi, Michael Grottke, and Ermeson Andrade. Software fault mitigation and availability assurance techniques. *International Journal of System Assurance Engineering and Management*, 1 :340–350, 2010.

[66] *IT and OT Convergence - Opportunities and Challenges*, volume All Days of *SPE Intelligent Energy International Conference and Exhibition*, 09 2016.

[67] Marco Hoffmann, Michael Jarschel, Rastin Pries, Peter Schneider, Admela Jukan, Wolfgang Bziuk, Steffen Gebert, Thomas Zinner, and Phuoc Tran-Gia. Sdn and nfv as enabler for the distributed network cloud. *Mobile Networks and Applications*, 23, 06 2018.

[68] Mijumbi, Rashid and Serrat, Joan and Gorricho, Juan-Luis and Bouten, Niels and De Turck, Filip and Boutaba, Raouf. Network function virtualization : state-of-the-art and research challenges. *IEEE COMMUNICATIONS SURVEYS AND TUTORIALS*, 18(1) :236–262, 2016.

[69] Hussein T. Mouftah, Melike Erol-Kantarci, and Mubashir Husain Rehmani. *Software Defined Networking and Virtualization for Smart Grid*, pages 171–190. 2019.

[70] Mathaios Panteli and Daniel S. Kirschen. Assessing the effect of failures in the information and communication infrastructure on power system reliability. In *2011 IEEE/PES Power Systems Conference and Exposition*, pages 1–7.

[71] Bilkisu Jimada-Ojuolape and Jiashen Teh. Impact of the integration of information and communication technology on power system reliability : A review. 8 :24600–24615. Conference Name : IEEE Access.

[72] Yue Li, Xin Li, Yangjun Zhou, Shan Li, and Xin Lu. Impact of cyber failure on cyber-physical distribution system reliability. In *2023 6th International Conference on Energy, Electrical and Power Engineering (CEEPE)*, pages 714–721.

[73] D. Kirschen and F. Bouffard. Keeping the lights on and the information flowing. 7(1) :50–60.

[74] A. Berizzi. The italian 2003 blackout. In *IEEE Power Engineering Society General Meeting, 2004.*, pages 1673–1679 Vol.2, 2004.

[75] Youba Nait Belaid, YiPing Fang, Zhiguo Zeng, Patrick Coudray, Anthony Legendre, and Anne Barros. Improved modeling of fault propagation, isolation, and fast service restoration in smart grids. *Advances in Modelling to Improve Network Resilience*, page 56, 2022.

[76] Mahshid Rahnamay-Naeini and Majeed M. Hayat. Cascading failures in interdependent infrastructures : An interdependent markov-chain approach. *IEEE Transactions on Smart Grid*, 7(4) :1997–2006, 2016.

[77] Abdullah Aydeger, Nico Saputro, Kemal Akkaya, and Selcuk Uluagac. Sdn-enabled recovery for smart grid teleprotection applications in post-disaster scenarios. *Journal of Network and Computer Applications*, 138 :39–50, 2019.

[78] Rakesh Kumar, Vignesh Babu, and David Nicol. Network coding for critical infrastructure networks. In *2018 IEEE 26th International Conference on Network Protocols (ICNP)*, pages 436–437, 2018.

[79] Hellen Maziku, Sachin Shetty, and David M Nicol. Security risk assessment for sdn-enabled smart grids. *Computer Communications*, 133 :1–11, 2019.

[80] Duha Ibdah, Maryam Kanani, Nada Lachtar, Neveen Allan, and Basheer Al-Duwairi. On the security of sdn-enabled smartgrid systems. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pages 1–5. IEEE, 2017.

[81] Moataz Abdelkhalek, Burhan Hyder, Manimaran Govindarasu, and Craig G Rieger. Moving target defense routing for sdn-enabled smart grid. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 215–220. IEEE, 2022.

[82] Shravan Gaonkar, Eric Rozier, Anthony Tong, and William H. Sanders. Scaling file systems to support petascale clusters : A dependability analysis to support informed design choices. In *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*, pages 386–391. IEEE.

[83] Chaojie Zhang, Alok Gautam Kumbhare, Ioannis Manousakis, Deli Zhang, Pulkit A Misra, Rod Assis, Kyle Woolcock, Nithish Mahalingam,

Brijesh Warrier, David Gauthier, Lalu Kunnath, Steve Solomon, Osvaldo Morales, Marcus Fontoura, and Ricardo Bianchini. Flex : High-availability datacenters with zero reserved power.

[84] Besmir Tola, Yuming Jiang, and Bjarne E. Helvik. Model-driven availability assessment of the NFV-MANO with software rejuvenation. 18(3) :2460–2477.

[85] Tuan Anh Nguyen, Dugki Min, Eunmi Choi, and Thang Duc Tran. Reliability and availability evaluation for cloud data center networks using hierarchical models. *IEEE Access*, 7 :9273–9313, 2019.

[86] Elton Torres, Gustavo Callou, and Ermeson Andrade. A hierarchical approach for availability and performance analysis of private cloud storage services. *Computing*, 100(6) :621–644, 2018.

[87] Besmir Tola, Gianfranco Nencioni, Bjarne E. Helvik, and Yuming Jiang. Modeling and evaluating NFV-enabled network services under different availability modes. In *2019 15th International Conference on the Design of Reliable Communication Networks (DRCN)*, pages 1–5. IEEE.

[88] Juxing Zhu, Ning Huang, Junliang Wang, and Xiaopeng Qin. Availability model for data center networks with dynamic migration and multiple traffic flows. pages 1–1. Conference Name : IEEE Transactions on Network and Service Management.

[89] Mohd. Khairil Rahmat and Slobodan Jovanovic. Reliability and availability estimation of DC uninterruptible power supply systems using monte-carlo simulation. In *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, pages 76–81. IEEE.

[90] Hachidai Ito, Keiichi Kaneda, Koichi Hamamatsu, Tatsuji Tanaka, and Koichi Nara. Dependability evaluation of substation automation system with redundancy. pages 713–721, 07 2008.

[91] Rongfei Zeng, Yixin Jiang, Chuang Lin, and Xuemin Shen. Dependability analysis of control center networks in smart grid using stochastic petri nets. 23(9) :1721–1730. Conference Name : IEEE Transactions on Parallel and Distributed Systems.

[92] Cen Nan, Irene Eusgeld, and Wolfgang Kröger. Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. 113 :76–93.

[93] Tod Courtney, Shravan Gaonkar, Ken Keefe, Eric W. D. Rozier, and William H. Sanders. Möbius 2.3 : An extensible tool for dependability, security, and performance evaluation of large and complex system models. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, pages 353–358. IEEE.

[94] Wei Koong Chai, Vaios Kyritsis, Konstantinos V. Katsaros, and George Pavlou. Resilience of interdependent communication and power distribution networks against cascading failures. In *2016 IFIP Networking Conference (IFIP Networking) and Workshops*, pages 37–45, 2016.

[95] Rongfei Zeng, Yixin Jiang, Chuang Lin, and Xuemin Shen. Dependability analysis of control center networks in smart grid using stochastic petri nets. *IEEE Transactions on Parallel and Distributed Systems*, 23(9) :1721–1730, 2012.

[96] Tesfaye Amare, Bjarne E Helvik, and Poul E Heegaard. A modeling approach for dependability analysis of smart distribution grids. In *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pages 1–8. IEEE, 2018.

[97] Kishor S. Trivedi and Andrea Bobbio. *Dependability*, page 3–14. Cambridge University Press, 2017.

[98] Cen Nan and Irene Eusgeld. Exploring impacts of single failure propagation between scada and suc. In *2011 IEEE International Conference on Industrial Engineering and Engineering Management*, pages 1564–1568. IEEE, 2011.

[99] Junjun Zheng, Hiroyuki Okamura, Tadashi Dohi, et al. Availability importance measures for virtualized system with live migration. *Applied Mathematics*, 6(02) :359, 2015.

[100] ABB. White paper : Reliability of uninterruptible power supplies. website : https://power-backup.ro/wp-content/uploads/2018/04/White_Paper_Relibility_150506.pdf, 2006.

[101] Louiza Yala, Pantelis A. Frangoudis, and Adlen Ksentini. Latency and availability driven vnf placement in a mec-nfv environment. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7, 2018.

[102] Dejene Boru Oljira, Karl-Johan Grinnemo, Javid Taheri, and Anna Brunstrom. A model for qos-aware vnf placement and provisioning. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–7, 2017.

[103] Satyam Agarwal, Francesco Malandrino, Carla-Fabiana Chiasserini, and S. De. Joint vnf placement and cpu allocation in 5g. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pages 1943–1951, 2018.

[104] Nassima Toumi, Olivier Bernier, Djamal-Eddine Meddour, and Adlen Ksentini. On using physical programming for multi-domain sfc placement with limited visibility. *IEEE Transactions on Cloud Computing*, 10(4) :2787–2803, 2022.

[105] Yunmei Luo, Yuping Luo, Xueping Ye, Jun Lu, and Shuqing Li. Reliability-based and qos-aware service redundancy backup method in iot-based

smart grid. In *Artificial Intelligence and Security : 5th International Conference, ICAIS 2019, New York, NY, USA, July 26–28, 2019, Proceedings, Part IV 5*, pages 588–598. Springer, 2019.

[106] Peng-Yong Kong and Yuming Jiang. Vnf orchestration and power-disjoint traffic flow routing for optimal communication robustness in smart grid with cyber-physical interdependence. *IEEE Transactions on Network and Service Management*, 19(4) :4479–4490, 2022.

[107] Sophie Cerf. *Control Theory for Computing Systems : Application to big-data cloud services & location privacy protection*. PhD thesis, UNIVERSITÉ GRENOBLE ALPES, 2019.

[108] Mauro Gaggero and Luca Caviglione. Model predictive control for the placement of virtual machines in cloud computing applications. In *2016 American Control Conference (ACC)*, pages 1987–1992. IEEE, 2016.

[109] Mauro Gaggero and Luca Caviglione. Model predictive control for energy-efficient, quality-aware, and secure virtual machine placement. *IEEE Transactions on Automation Science and Engineering*, 16(1) :420–432, 2018.

[110] Sebastian Orlowski, Roland Wessäly, Michal Pióro, and Artur Tomaszewski. Sndlib 1.0—survivable network design library. *Networks : An International Journal*, 55(3) :276–286, 2010.

[111] Boris Petrenj, Emanuele Lettieri, and Paolo Trucco. Towards enhanced collaboration and information sharing for critical infrastructure resilience : Current barriers and emerging capabilities. *Int. J. of Critical Infrastructures*, 8 :107 – 120, 09 2012.

[112] Stephane Couture and Sophie Toupin. What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10) :2305–2322, 2019.

[113] Danniar Reza Firdausy, Patrício De Alencar Silva, Marten Van Sinderen, and Maria-Eugenia Iacob. Towards a reference enterprise architecture to enforce digital sovereignty in international data spaces. In *2022 IEEE 24th Conference on Business Informatics (CBI)*, volume 01, pages 117–125, 2022.

[114] Zoltan Nyikes and Zoltan Rajnai. Big data, as part of the critical infrastructure. In *2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY)*, pages 217–222, 2015.

[115] Yan Xin, Kai Yang, Chih-Lin I, Sanyogita Shamsunder, Xingqin Lin, and Lifeng Lai. Guest editorial : Ai-powered telco network automation : 5g evolution and 6g. *IEEE Wireless Communications*, 30(1) :68–69, 2023.

[116] Mauricio Monsalve and Juan De la Llera. Data-driven estimation of interdependencies and restoration of infrastructure systems. *Reliability Engineering and System Safety*, 181, 10 2018.

[117] Edward Curry, Wassim Derguech, Souleiman Hasan, Christos Kouroupetroglou, and Umair ul Hassan. A real-time linked dataspace for the internet of things : Enabling "pay-as-you-go" data management in smart environments. *Future Generation Computer Systems*, 90, 07 2018.

[118] Edward Curry and Amit Sheth. Next-generation smart environments : From system of systems to data ecosystems. *IEEE Intelligent Systems*, 33(3) :69–76, 2018.

[119] Alon Halevy, Michael Franklin, and David Maier. Principles of dataspace systems. In *Proceedings of the Twenty-Fifth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, page 1–9, New York, NY, USA, 2006. Association for Computing Machinery.

[120] Michael Franklin, Alon Halevy, and David Maier. From databases to dataspaces : A new abstraction for information management. 34(4) :27–33, dec 2005.

[121] *Designing Data Spaces*.

[122] Fraunhofer. White paper industrial data space. 2016.

[123] International Data Spaces Association. Idsa reference architecture model, 2023.

[124] Vinay Murudi, Krishna M. Kumar, and Dhilip S. Kumar. Multi data center cloud cluster federation - major challenges and emerging solutions. In *2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, pages 107–112, 2016.

[125] Kiril Antevski and Carlos J. Bernardos. Federation in dynamic environments : Can blockchain be the solution ? *IEEE Communications Magazine*, 60(2) :32–38, 2022.

[126] Fraunhofer. Idsa position paper gaia-x and ids version 1.0. 2021.

[127] Renato Ianella. Open digital rights language (odrl). *Open Content Licensing : Cultivating the Creative Commons*, 2007.

[128] Tobias Dam, Lukas Daniel Klausner, Sebastian Neumaier, and Torsten Priebe. A survey of dataspace connector implementations. *arXiv preprint arXiv :2309.11282*, 2023.

[129] Veronika Siska, Vasileios Karagiannis, and Mario Drobics. Building a dataspace : Technical overview. 2023.

[130] Sebastian Bader, Jaroslav Pullmann, Christian Mader, Sebastian Tramp, Christoph Quix, Andreas W Müller, Haydar Akyürek, Matthias Böckmann, Benedikt T Imbusch, Johannes Lipp, et al. The international data spaces information model–an ontology for sovereign exchange of digital content. In *International Semantic Web Conference*, pages 176–192. Springer, 2020.

[131] TM Forum. Telco data space - tm forum. https://myaccount.tmforum.org/networks/21-0-223/index.html, 2020. Accessed : 29-07-2023.

[132] Xavier Marjou, Tangui Le Gleau, Vincent Messie, Benoit Radier, Tayeb Lemlouma, and Gael Fromentoux. Evaluating inter-operator cooperation scenarios to save radio access network energy. In *2022 1st International Conference on 6G Networking (6GNet)*, pages 1–5, 2022.

[133] Berkhout V. and Skubowius E. Predictive maintenance für windenergieanlagen energy data space whitepaper. dortmund. website : https://internationaldataspaces.org/download/19022/, 2020.

[134] ETSI GS NFV-IFA 013 V3.4.1. Network functions virtualisation (nfv) release 3; management and orchestration; os-ma-nfvo reference point-interface and information model specification, 2020.

[135] Kostas Katsalis, Navid Nikaein, and Andy Edmonds. Multi-domain orchestration for nfv : Challenges and research directions. In *2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*, pages 189–195, 2016.

[136] Antonio Francescon, Giovanni Baggio, Riccardo Fedrizzi, Enrico Orsini, and Roberto Riggio. X-mano : An open-source platform for cross–domain management and orchestration. In *2017 IEEE Conference on Network Softwarization (NetSoft)*, pages 1–6, 2017.

[137] Pol Alemany, Ricard Vilalta, Raul Muñoz, Ramon Casellas, and Ricardo Maríinez. Peer-to-peer blockchain-based nfv service platform for end-to-end network slice orchestration across multiple nfvi domains. In *2020 IEEE 3rd 5G World Forum (5GWF)*, pages 151–156, 2020.

[138] Toru Mano, Takeru Inoue, Dai Ikarashi, Koki Hamada, Kimihiro Mizutani, and Osamu Akashi. Efficient virtual network optimization across multiple domains without revealing private information. *IEEE Transactions on Network and Service Management*, 13(3) :477–488, 2016.

[139] Raul Muñoz, Ricard Vilalta, Ramon Casellas, Ricardo Martínez, Felipe Vicens, Josep Martrat, Víctor López, and Diego López. Hierarchical and recursive nfv service platform for end-to-end network service orchestration across multiple nfvi domains. In *2018 20th International Conference on Transparent Optical Networks (ICTON)*, pages 1–5, 2018.

[140] A Kojukhov, AM de Nicolas, B Chatras, D Druta, D Gassanov, M Brunner, M Brenner, S Li, T Nguyenphu, U Rauschenbach, et al. Network functions virtualisation (nfv) release 2; protocols and data models; vnf package specification. gs nfv-sol 004 v2. 3.1. *Group specification, ETSI*, 2017.

[141] ETSI NFVISG. Network functions virtualisation (nfv) release 3; protocols and data models; restful protocols specification for the or-vnfm reference point, 2020. *Cited in*, page 17.

[142] Xiaoxi Zhang, Chuan Wu, Zongpeng Li, and Francis C.M. Lau. Proactive vnf provisioning with multi-timescale cloud resources : Fusing online learning and online optimization. In *IEEE INFOCOM 2017*, pages 1–9, 2017.

[143] Huawei Huang and Song Guo. Proactive failure recovery for nfv in distributed edge computing. *IEEE Communications Magazine*, 57(5) :131–137, 2019.

[144] A Adhiappan, A Chernetsov, M Fenomenov, U Karabudak, A Korabanova, S Kislyakov, L Le Beller, M Nati, B Radier, A Sushkov, et al. Federated csps marketplace : A dlt-based data trust enabling business assurance for csps platforms federation. In *TM Forum, White Paper*, volume 1, 2020.

[145] Bruno Chatras. Etsi nfv rest apis and data models. 04 2018.

[146] GSNFV ETSI. Etsi gs nfv-ifa 013 v3. 4.1 : Management and orchestration ; os-ma-nfvo reference point-interface and information model specification, 2020.