Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P503-cd

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.

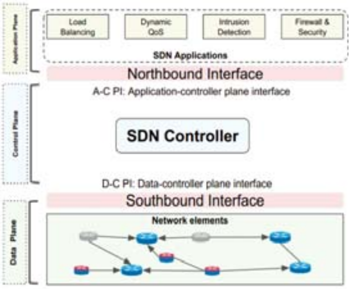


Fig. 1: SDN architecture.

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.

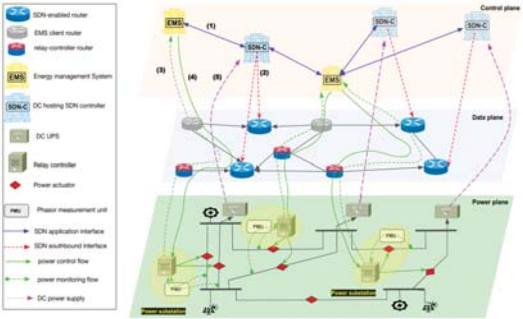


Fig. 2: Architecture of an SDN-enabled smart grid.

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.

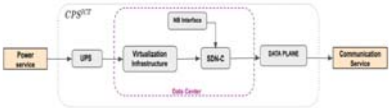


Fig. 3: Functional Block diagram of a cyber-physical system in the ICT domain whose main function is to provide communication service.

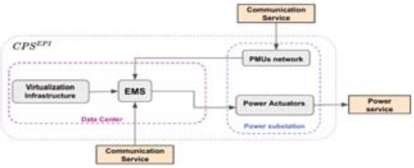


Fig. 4: Functional Block diagram of a cyber-physical system in the EPI domain whose main function is to provide power service. Note that, we assume that the power supply of a DC hosting EMS instances, is reliable and thus, it is not represented in the diagram.

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.

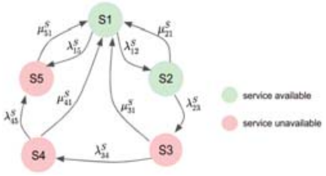


Fig. 5: continuous-time Markov chain describing the state of the **S** subsystem (a virtualized data center composed of: Virtualization Infrastructure Manager (VIM), SDN-C and a programmable data plane).

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.

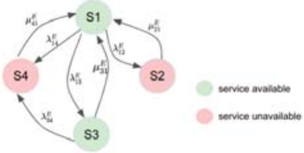
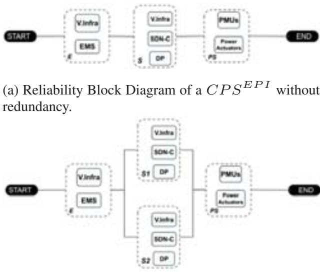


Fig. 6: continuous-time Markov chain describing the state of the **E** subsystem (a virtualized data center composed of : VIM and EMS)

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.

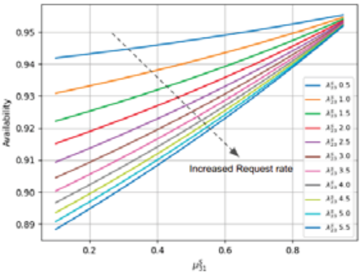


Fig. 8: Availability of subsystem S as a function of the rate μ_{31}^{S} for different networking request rate values.

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.

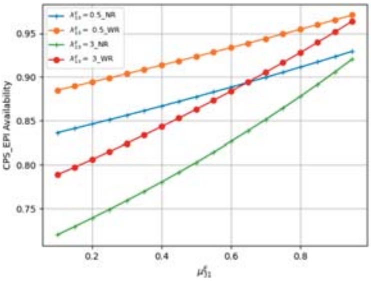


Fig. 9: Steady state availability of CPS^{EPI} in two scenarios: with redundancy (WR and without redundancy NR).

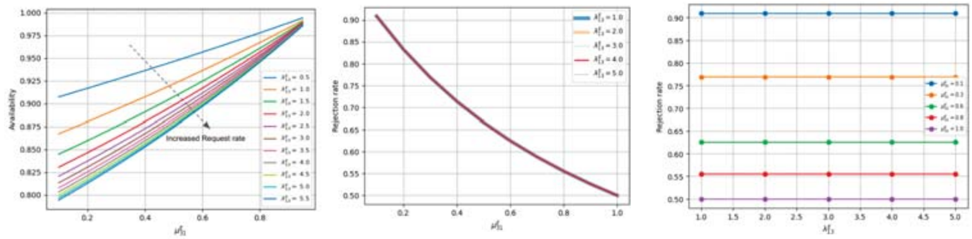
VI. Conclusion

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^E_{31} for different networking request rate values.

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

(c) Rejection rate as a function of λ^E_{13} 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.