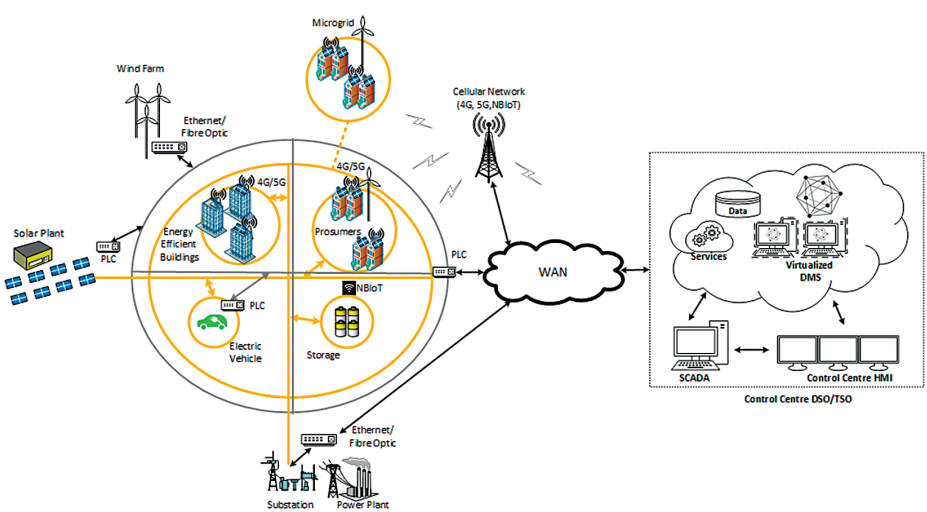
E.ON Energy Research Center | RWTH AACHEN UNIVERSITY

Towards resilient design of distribution grid automation system: An evaluation of its reliability against random failures and susceptibility to targeted attacks

Abhinav Sadu
Institute for Automation of Complex Power Systems



Towards resilient design of distribution grid automation system: An evaluation of its reliability against random failures and susceptibility to targeted attacks

Von der Fakultät für Elektrotechnik und Informationstechnik
der Rheinisch-Westfälischen Technischen Hochschule Aachen
zur Erlangung des akademischen Grades eines Doktors
der Ingenieurwissenschaften genehmigte Dissertation

vorgelegt von

Abhinav Sadu, M. Sc.

aus
Chennai, India

Berichter:
Univ.-Prof. Antonello Monti, Ph. D.
Prof.Anurag Srivastava, Ph. D, West
Virginia University, USA

Tag der mündlichen Prüfung: 20. Dezember 2021

Bibliographische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb-nb.de abrufbar.

D 82 (Diss. RWTH Aachen University, 2021)

Herausgeber:
Univ.-Prof. Dr. ir. Dr. h. c. Rik W. De Doncker
Direktor E.ON Energy Research Center

Institute for Automation of Complex Power Systems (ACS)
E.ON Energy Research Center
Mathieustraße 10
52074 Aachen

E.ON Energy Research Center I 108. Ausgabe der Serie
ACS I Automation of Complex Power Systems

Printed in Germany

ISBN: 978-3-948234-22-5
1. Auflage 2022

Verlag:
E.ON Energy Research Center, RWTH Aachen University
Mathieustraße 10
52074 Aachen
Internet: www.eonerc.rwth-aachen.de
E-Mail: post_erc@eonerc.rwth-aachen.de

Herstellung:
Druckservice Zillekens
Rainweg 19
52224 Stolberg

Kurzfassung

Ein resilientes System zur Automatisierung von Verteilnetzen (Distribution Grid Automation-DGA) gewährleistet einen sicheren und zuverlässigen Betrieb aktiver Verteilnetze und deren Versorgungssicherheit. Für eine robuste Auslegung des DGA-Systems muss seine Zuverlässigkeit gegenüber zufälligen Komponentenausfällen und die Anfälligkeit für gezielte Angriffe bewertet werden, damit geeignete Komponentenredundanzen sowie Cyber- und physische Sicherheitsmaßnahmen implementiert werden können. Daher wird für die Zuverlässigkeitsbewertung von DGA-Systemen eine auf der Continuous Time Markov Chain (CTMC) basierende Bewertungsmethode vorgeschlagen, die die Multi Domain Reliability Matrix (MDRM) einbezieht und die cyber-physische Interdependenz erfasst. Um die Anfälligkeit von DGA-Systemen gegen cyber-physische Angriffe zu bewerten und die Auswirkungen von Sicherheitsmaßnahmen zu untersuchen, wird eine CTMC-basierte Methodik vorgestellt, die eine Multi-Criteria-Decision-Making-Methodik beinhaltet. Schließlich wird ein auf Blockchain und Smart Contracts basierendes, resilientes Design von DGA-Systemen vorgeschlagen, das eine hohe Verfügbarkeit der DGA-Funktionen auch bei zufälligen Ausfällen und gezielten Angriffen auf die DGA-Systeme gewährleistet.

Abstract

A resilient Distribution Grid Automation (DGA) system ensures safe and reliable operation of active distribution grids and its supply security . For resilient design of the DGA system its reliability against random component failures and the susceptibility to targeted attacks must be evaluated, so that appropriate component redundancies and cyber & physical security measures could be implemented. Hence, a Continuous Time Markov Chain (CTMC) based methodology, incorporating the Multi Domain Reliability Matrix (MDRM) is proposed for the reliability evaluation DGA systems that captures the cyber-physical interdependence. Furthermore, to evaluate the susceptibility of the DGA systems against cyber-physical attacks and study the impact of the security countermeasures, a CTMC based methodology incorporating a Multi-Criteria-Decision-Making methodology is presented. Finally, a Blockchain, and Smart contract based resilient design of DGA systems is proposed that ensures high availability of DGA functions even against random failures and targetted attacks on the DGA systems

Acknowledgements

I would like to thank **Univ.-Prof. Antonello Monti, Ph. D** and **Univ.-Prof. Ferdinanda Ponci, Ph. D**, for giving me the opportunity to pursue my doctoral research work at the Institute for Automation of Complex Power Systems (ACS). I would also thank them for their immense support, guidance and efforts in providing the conducive working environment for productive research work. I would also like to thank **Prof. Anurag Srivastava, Ph. D** for being my second supervisor and providing valuable comments on my work. Additionally, I would like to thank RWTH Aachen University and the administration of the E.ON Energy Research Centre for providing the best research facilities that helped me to finish my doctoral thesis successfully. From an administrative stand point I would also like to Thank Ms.Bettina Schäfer and the entire controlling and secretary team of ACS who helped me in all organizational aspects at ACS.

During my doctoral work, I have been part of various research and industrial projects and had successfully coordinated them with the help of competent project colleagues. Therefore, I would like to thank all the colleagues with whom I had worked in these projects, as each of them was competent in their field and had always brought something new, that inspired me and helped me to improve not only my technical know-how but also my managerial skills.The time I spent at ACS was always joyful and educational. This was possible only because of very talented, friendly and open doctoral candidates, postdoctoral fellows and valuable students. I would like to thank all my colleagues at ACS and students who directly or indirectly were helpful in refining my ideas for my doctoral work.

I would also like to thank Dr.Rajesh Kumar for helping me in developing an aptitude for research during my undergraduate studies at Malaviya National Institute of Technology, Jaipur India. Furthermore, I would like to thank all teachers at CRS Ambalamugal who kindled my interest for science and mathematics at high school. Finally I would like to thank my parents, my wife, my brother and all my friends and relatives who have always believed and supported me in every respect.

Contents

List of Publications

Journal Articles

[Sad+21] A. Sadu, A. Jindal, G. Lipari, F. Ponci, and A. Monti. "Resilient Design of Distribution Grid Automation System against cyber-physical attacks using Blockchain and Smart Contract". In: *Blockchain: Research and Applications* (2021), p. 100010. ISSN: 2096-7209. DOI: https://doi.org/10.1016/j.bcra.2021.100010. URL: https://www.sciencedirect.com/science/article/pii/S2096720921000051.

[McK+20] P. McKeever, A. Sadu, S. Rohilla, Z. Mehdi, and A. Monti. "Ensuring Uninterrupted MTC Service Availability during Emergencies Using LTE/5G Public Mobile Land Networks". In: *Telecom* 1.3 (2020), pp. 181–195. URL: https://www.mdpi.com/2673-4001/1/3/13.

[Sad+20b] A. Sadu, G. K. Roy, F. Ponci, and A. Monti. "Methodology for Reliability Analysis of Cyber-Physical MTdc Grids". In: *IEEE Journal of Emerging and Selected Topics in Power Electronics* (2020), pp. 1–1.

[Kum+19] G. Kumar Roy, J. Hu, A. Sadu, F. Ponci, A. Monti, and R. W. De Doncker. "Data modelling of converters for the automation and monitoring of MTDC grids". English. In: *IET Smart Grid* 2 (3 Sept. 2019), 456–463(7).

[Pon+18] F. Ponci, A. Sadu, R. Uhl, M. Mirz, A. Angioni, and A. Monti. "Instrumentation and measurement testing in the real-time lab for automation of complex power systems". In: *IEEE Instrumentation Measurement Magazine* 21.1 (2018), pp. 17–24.

[Cos+17] F. B. Costa, A. Monti, F. V. Lopes, K. M. Silva, P. Jamborsalamati, and A. Sadu. "Two-Terminal Traveling-Wave-Based Transmission-Line Protection". In: *IEEE Transactions on Power Delivery* 32.3 (2017), pp. 1382–1393.

[Man+16a] M. Manbachi, A. Sadu, H. Farhangi, A. Monti, A. Palizban, F. Ponci, and S. Arzanpour. “Impact of EV penetration on Volt–VAR Optimization of distribution networks using real-time co-simulation monitoring platform”. In: *Applied Energy* 169 (2016), pp. 28–39. ISSN: 0306-2619. DOI: https://doi.org/10.1016/j.apenergy.2016.01.084. URL: https://www.sciencedirect.com/science/article/pii/S030626191630071X.

[Man+16b] M. Manbachi, A. Sadu, H. Farhangi, A. Monti, A. Palizban, F. Ponci, and S. Arzanpour. “Real-Time Co-Simulation Platform for Smart Grid Volt-VAR Optimization Using IEC 61850”. In: *IEEE Transactions on Industrial Informatics* 12.4 (2016), pp. 1392–1402.

Pantents

[Sad+20c] A. Sadu, J. Akshay, G. Lipari, and F. Ponci. “Verfahren und Vorrichtungen für eine Lastzuweisung und Überwachung für eine zuzuweisende versorgungssicherheitskritische Ressource in einem Netzwerk”. U.S. pat. DE 10 2019 203 874.3. Mar. 1, 2020.

Book Chapters

[Dog+20a] A. Dognini, A. Sadu, N. Wirtz, A. Monti, G. Brito, G. di Orio, P. Maló, and C.-S. Nechifor. “14. Securing CEI by-design”. In: *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Now Publishers, 2020. DOI: 10.1561/9781680836875.ch14. URL: https://doi.org/10.1561/9781680836875.ch14.

[MRS16] A. Monti, A. Roscoe, and A. Sadu. “Chapter 6 - International Standards for PMU and Tests for Compliance”. In: *Phasor Measurement Units and Wide Area Monitoring Systems*. Ed. by A. Monti, C. Muscas, and F. Ponci. Academic Press, 2016, pp. 87–121. ISBN: 978-0-12-804569-5. DOI: https://doi.org/10.1016/B978-0-12-804569-5.00006-9. URL: https://www.sciencedirect.com/science/article/pii/B9780128045695000069.

[MST16] A. Monti, A. Sadu, and J. Tang. "Chapter 8 - Wide Area Measurement Systems: Applications". In: *Phasor Measurement Units and Wide Area Monitoring Systems*. Ed. by A. Monti, C. Muscas, and F. Ponci. Academic Press, 2016, pp. 177–234. ISBN: 978-0-12-804569-5. DOI: https://doi.org/10.1016/B978-0-12-804569-5.00008-2. URL: https://www.sciencedirect.com/science/article/pii/B9780128045695000082.

Conference Articles

[Dog+20b] A. Dognini, A. Sadu, A. Angioni, F. Ponci, and A. Monti. "Service Restoration Algorithm for Distribution Grids under High Impact Low Probability Events". In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. 2020, pp. 237–241. DOI: 10.1109/ISGT-Europe47291.2020.9248823.

[Sad+20a] A. Sadu, M. Stevic, N. Wirtz, and A. Monti. "A Stochastic Assessment of Attacks based on Continuous-Time Markov Chains". In: *2020 6th IEEE International Energy Conference (ENERGYCon)*. 2020, pp. 11–16. DOI: 10.1109/ENERGYCon48941.2020.9236600.

[Roy+19] G. K. Roy, M. Pau, A. Sadu, F. Ponci, and A. Monti. "Inclusion of converter controller measurements into state estimation algorithm for hybrid ac-dc grid". In: *2019 IEEE Milan PowerTech*. 2019, pp. 1–6. DOI: 10.1109/PTC.2019.8810853.

[Jam+17] P. Jamborsalamati, A. Sadu, F. Ponci, A. Monti, and M. Hossain. "Improvement of supply restoration in multi-spare-feeder active distribution grids using IEC 61850". In: *2017 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia)*. 2017, pp. 1–5. DOI: 10.1109/ISGT-Asia.2017.8378326.

[Jam+16] P. Jamborsalamati, A. Sadu, F. Ponci, and A. Monti. "A flexible HiL testing platform for performance evaluation of IEC 61850-based protection schemes". In: *2016 IEEE Power and Energy Society General Meeting (PESGM)*. 2016, pp. 1–5.

[Pat+16] D. Patel, M. I. N. Mohamed, S. Z. R. Mehdi, F. Williams, A. Sadu, F. Ponci, and A. Monti. "Investigating the performance of QoS enabled LTE networks for IEC 61850 based smart grid applications". In: *2016 IEEE International Energy Conference (ENERGYCON)*. 2016, pp. 1–6. DOI: 10.1109/ENERGYCON.2016.7513965.

[Pau+16a] M. Pau, A. Sadu, S. Pillai, F. Ponci, and A. Monti. "A state estimation algorithm for hybrid AC/DC networks with multiterminal DC grid". In: *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. 2016, pp. 1–6. DOI: 10.1109/ISGTEurope.2016.7856278.

[Sad+16] A. Sadu, M. Pau, S. Pillai, F. Ponci, and A. Monti. "Impact of uncertainty propagation on the design of state estimation for hybrid ac-dc grids". In: *2016 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. 2016, pp. 1–6.

[Jam+15] P. Jamborsalamati, A. Sadu, F. Ponci, and A. Monti. "Design, implementation and real-time testing of an IEC 61850 based FLISR algorithm for smart distribution grids". In: *2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. 2015, pp. 114–119. DOI: 10.1109/AMPS.2015.7312748.

[Man+15a] M. Manbachi, A. Sadu, H. Farhangi, A. Monti, A. Palizban, F. Ponci, and S. Arzanpour. "Real-time co-simulated platform for novel Volt-VAR Optimization of smart distribution network using AMI data". In: *2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. 2015, pp. 1–7.

[Sad+14] A. Sadu, A. Angioni, J. Liu, F. Ponci, and A. Monti. "A platform for testing monitoring systems for the power distribution grid". In: *2014 IEEE International Workshop on Applied Measurements for Power Systems Proceedings (AMPS)*. 2014, pp. 1–6. DOI: 10.1109/AMPS.2014.6947714.

"The more original a discovery, the more obvious it seems afterwards."
- Arthur Koestler

1

Introduction

1.1 Motivation

The current power system is going through fundamental changes in design. There is a paradigm shift in how the energy is produced, delivered and consumed as shown in Fig. 1.1. This can be attributed to the higher penetration of distributed energy resources (specifically from renewable energy resources),reduction in coal based power generation, increase in e-vehicles, cheaper energy storage solutions, smart demand response measures, efficient load management systems (smart home, smart building and smart city initiatives), evolution of consumers to a prosumers and government legislature supporting peer-to-peer energy trading and neighbourhood energy exchange [MIS19],[Coma],[HW17],[Sil+21],[RPD14].

Most of the transformation is happening at the distribution grid level. The Distribution System Operators (DSO) are facing problems in managing the transformation of a passive distribution grid to an active grid with bi-directional power flows as shown in Fig. 1.1, with higher penetration of renewable, E-Vehicles, controllable loads and storage systems. Therefore, similar to the transmission grid, the distribution grid automation is being upgraded to support power dispatch, congestion management, Volt-Var optimization, complex Fault Localisation Isolation and Service Restoration (FLISR), Black-Start, and wide area monitoring utilizing Advance Metering Infrastructure (AMI) and low cost Phasor Measurement Unit (PMU)s. Varied methodologies to implement these functions have been proposed in the literature and have been implemented in trial sites. The authors in [Man+16b],[Man+15b] present an IEC 61850 based implementation of the Volt-Var application for distribution grids, they also include the resources offered by E-Vehicles for Volt-Var applications in [Man+16a]. The authors in [Ang+15] present an implementation of the Volt-Var application using Long Term Evolution (LTE)(4G) infrastructure. A real-time platform for the design and implementation of an IEC

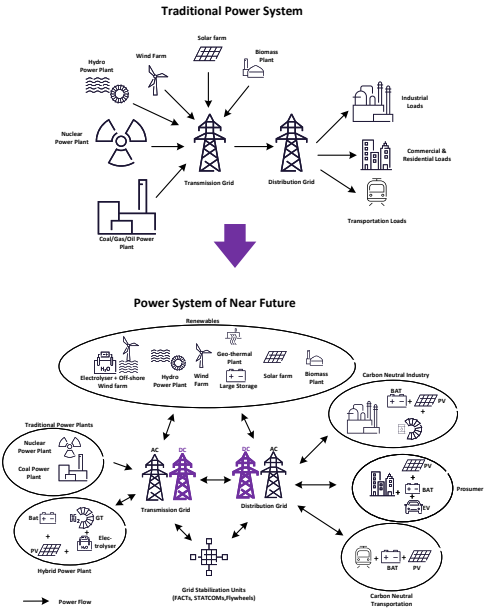


Figure 1.1: Power grid transformation

61850 based FLISR application for distribution grids has been presented in [Jam+16]. A real-time platform utilising smart meter measurements (AMI) and low cost PMUs has been presented in [Ang+16][Ang+17], which was also implemented at the trial site of Italian DSO Unareti in the framework of IDE4L project, an FP7 project funded by European Commission [Rep+17]. A 5G and cellular network enabled Black-Start functionality have been proposed in [McK+20],[McK+17], for distribution grid and deployed at different DSO trial sites in Europe within the framework of the project SUCCESS, a Horizon 2020 project funded by the European Commission [Suc],[SUC]. A cloud based state estimation for monitoring distribution grid using smart meters has been presented in [Pau+18],[Pau+16b]. The presented work has been implemented in different trial sites within the scope of the project Flexmeter, a Horizon 2020 initiative funded by the European Commission. The authors present the recent advances in the demand side management and the different automation architectures implementing them in [DMS18]. Furthermore,

the concept of dual demand side management has been introduced in [Mon+15] and the details of the operation is also provided. The authors in [She+19], [Han+17] propose different methodologies to perform congestion management in distribution grids by interacting with different actors namely the market entities, aggregators demand and supply forecasting entities, thus necessitating a complex automation architecture that enables communication with heterogeneous entities responsible for realising the congestion management. Furthermore, a higher degree of interaction between the Transmission System Operators (TSO)s and DSOs is expected in the future to manage the volatility in the energy generation from the renewable energy resources to keep the power grid stable [Sil+21]. Therefore, the Distribution Grid Automation (DGA) system is required, that helps in realising all the aforementioned automation functions for distribution grids. The DGA would be responsible for monitoring, control and protection of the distribution grid and its assets, while interacting with the TSOs to maintain the complete power grid stable.

However, in order to achieve the aforementioned goals thanks to the advancement in Information and Communication Technology (ICT) infrastructures, highly flexible and scalable architectures of DGA have been proposed in the literature. Architectures varying in nature from hierarchical structures, as in [Rep+17], to completely distributed multi-agent architectures as presented in [Kam] have been proposed. The digitization of the substation with Ethernet based IEC 61850 based automation architectures, packet based communication protocols, deployment of smart meters and low cost Phasor Measurement Unit (PMU)s (Advance Metering Infrastructure (AMI)) [FLE],[NRG], deployment of heterogeneous communication infrastructure (Wireless (Cellular, Wi-Fi), Wired (Ethernet, Serial, PLC)) for measurement data acquisition and control [GR15] [SUC],[ESA],[NRG] and adoption of edge cloud and other cloud based automation [FIS], [PLA] have enabled the design and implementation of futuristic automation architectures for distribution grids [MP16].

By considering all possible use-cases for the automation of power grids, a smart Grid road map as shown in Fig. 1.2, has been identified. From this figure it is clear that there are different automation actors involved in the different zones and domains. Furthermore, it can also be seen that, for the complete automation of the distribution grids, a wide range of communication and data acquisition systems have to be deployed. A single automation function can be successfully carried out by different automation actors participating at different operation zones. Therefore, for successful realisation of a complete automation function the proper functioning of the ICT infrastructures along with the different measurement and control system should be ensured. The authors in [Hae+19]

provide a survey of the different blackouts that happened globally. They also provide a detailed estimation of socio-economic costs incurred due to the various blackouts. A set of the major reasons for a large number of blackouts are being attributed to the failure of the control and automation system and the complex interdependence of the ICT infrastructure and the power equipment (Sensors and Actuators) [Hae+19]. This problem becomes even more acute, when ICT enabled automation systems are deployed for proactively identifying and taking precautionary measures through Wide Area Monitoring, Protection And Control (WAMPAC) [Gup+16][TCF09], to avoid blackouts. However, it should be noted that the different automation functions realised by the WAMPAC are heavily dependent on the ICT infrastructure and their interdependence. The architecture of the DGA infrastructure determines how the different functions of the WAMPAC are realised. For evaluating the effectiveness of a specific automation architecture, the complex interdependence between the different ICT infrastructure (that forms the cyber part of DGA) and the physical components (sensors, actuators, controllers, breakers, etc) have to be analysed. The DGA system, hence, becomes a critical cyber-physical system with complex inter-dependencies, that ensures safe and reliable supply of electrical energy. Its availability impacts the availability of power to the consumers and ensure stability of the grid. The impact of failures of the cyber and physical components of the DGA systems have different impacts on the availability of different automation functions realised by the DGA system.

Therefore, designers of the DGA architecture have to carefully plan the system hardening measures that makes the DGA systems inherently reliable and resilient-by-design. There are different measures that could be deployed to improve the reliability and resiliency of the system against failures. The reliability of the system can be improved by deploying adequate redundancies and component maintenance strategies. Improving the reliability helps in coping with random failures of the components of the DGA system. Normally, the reliability/availability of the system is calculated considering the random failure of its constituting components. Though a lot of research has been done in this regard, availability of the DGA systems considering the failure of cyber and physical components, and their dependence in realising a specific automation function is sparsely studied. A generic methodology to evaluate the reliability of the cyber-physical DGA system, in particular the reliability of the DGA system to implement an automation function, is required. This enables the system designers to evaluate and compare the effectiveness of the different hardening measures (component redundancies) put in place. One of the main contribution of this thesis is to provide a methodology to evaluate

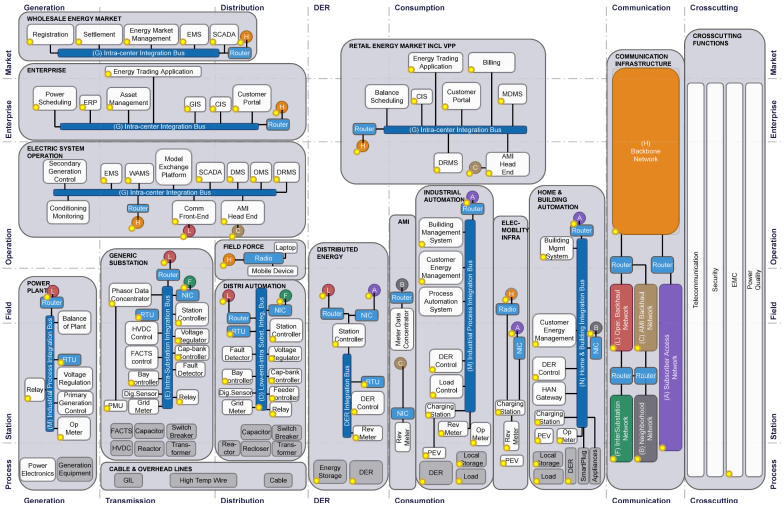


Figure 1.2: Smart grid roadmap [Comb]

the availability/reliability of the DGA systems due to random failures of the cyber and physical components considering the complex dependencies between the cyber and physical components in realising the automation function, to evaluate the effectiveness of redundancies in cyber and physical components.

But apart from the random failures of the component, intentional failures (attacks) on the cyber and physical components of the DGA systems have also resulted in the unavailability of automation functions resulting in large blackouts. One of the relevant examples is the attack on theDGA system of the Ukranian DSO, where different vulnerabilities of the cyber and physical components of the DGA systems were exploited, resulting in a blackout impacting 225,000 people. The system designers must also harden the system against intentional attacks. For effective hardening of the system against intended failures, the susceptibility of the DGA system should be evaluated. The susceptibility can then be used as an index to evaluate the effectiveness of the countermeasures. The implemented hardening measures help in reducing the risk of the intended attack. However, while evaluating the susceptibility of the DGA systems to cyber-physical attacks, major aspects of the uncertainties of exploiting the vulnerabilities, skill of the attacker and the stochasticity in the attack propagation should be considered.

Understanding the system performance against random and intended failures is important to define mechanisms that make the DGA systems resilient-by-design. Evaluating the reliability and susceptibility of the DGA system helps in quantifying the risk of a random and intended failures on to the DGA system and subsequently the effectiveness of the system hardening measures. These two metrics (Reliability/Availability & Susceptibility) helps to quantify the preparedness of the system against a known set of failures. Unfortunately, as all the possible sources of failure can not be known a-priori, no level of hardening measures can ensure 100% availability and full protection against all possible intended attacks. Therefore, additional hardening measures have to be taken to make system resilient-by-design. Goal is to make sure that, even when a random failure or an intended attack makes the DGA unavailable, inherent processes are enabled that ensure fast recovery making the all the DGA system functionalities available as soon as possible. A lot of studies have been made to improve the resiliency of the distribution grid by optimally planning for adequate placement and operation of DERs, E-Vs and storage capacities in the distribution grid. Furthermore, optimal power grid network planning and service restoration schemes have been proposed for improving the resilience of the distribution grid. However, measures to improve the resiliency of the cyber-physical DGA systems is sparsely studied.

Therefore, in this thesis, in the wake to create a DGA system that is reliable and resilient-by-design, the following have been proposed:

- Develop a theoretical methodology to evaluate the availability/reliability of the cyber-physical DGA systems due to random failures of the cyber and physical components.
  - Consider the complex dependencies between the cyber and physical components in realising the automation function.
- Develop a theoretical methodology to evaluate the susceptibility of the DGA to targeted cyber & physical attacks.
  - Consider uncertainty in attack frequency, launch of atomic attacks, effectiveness of countermeasure, skill of the attacker (based on exposure and exploitability of vulnerabilities).
  - Evaluate the attack propagation for optimal countermeasure design.
- Develop a theoretical concept and a proof-of-concept implementation of DGA that is resilient by design.

1.2 Main contribution

The evaluation of the reliability/availability is done by developing a failure model of a DGA function by considering the failure characteristics of the cyber & physical components and their interdependence in realising the DGA function. A methodology is proposed, where the DGA function is divided into mutually exclusive and collectively exhaustive cyber-physical Functional Blocks (FBs). The reliability of the DGA is then derived as the function of the reliability of the combination of the FBs. The failure of cyber and physical components of each FB is modelled using Continuous Time Markov Chain (CTMC). A novel Multi Domain Reliability Matrix (MDRM) is then proposed to capture the interdependence of the cyber and physical components in realising the DGA function successfully. The reliability of cyber-physical Multi-Terminal DC grids and heterogenous wide area monitoring of distribution grids is presented. The proposed method of representing the DGA function as a set of FBs and using the CTMC with MDRM to evaluate its reliability/availability is a new addition to the current state of the art, that enables to study the complex cyber-physical DGA system.

To evaluate the susceptibility of the DGA system to targeted cyber and physical attacks and predict its propagation, a stochastic methodology is proposed. A threat scenario is assumed to be available, (depicting foreseeable attack vectors) determined by the security experts considering the vulnerabilities of the cyber and physical components, their exposure and exploitability. The proposed methodology adds to the current state of art by enabling the modelling of dependence of each attack step (concurrency, sequency etc) in realising a coordinated attack and the uncertainty of the attack step namely the uncertainty in attack/atomic attack launch time, exploitability of vulnerability, effectiveness of the countermeasures and the uncertainty in the launch time of the countermeasure. It also enables the probabilistic risk evaluation of an attack agent/vector. The proposed methodology assumes that a threat scenario has been identified by the security experts and represented as attack trees. To model the attack dependencies (like concurrency and sequence) the attack tree is re-modelled as a Petri net. Then a reachability graph of the Petri net is generated to identify the possible attack vectors and the attack goals and subgoals. The reachability graph is then considered as the Markov chain where the states correspond to the attack state (goals & subgoals) and a transition corresponds to the atomic attack step (exploitability of device vulnerability). The Markov chain enables the modelling of the attack propagation as a transition in a state based stochastic process where the uncertainty of each step in the attack propagation (state transi-

tion), represents the uncertainty in the attack launch time, uncertainty in exploitability of device vulnerability, effectiveness of the countermeasure, uncertainty in launch time of a countermeasure. The standard metrics of attack propagation namely the probability of reaching goals and subgoals of the attack, time to compromise and the mean time spent in sub-goals before reaching the final goal can be calculated using the Markov chain formalism. In a nutshell, a probabilistic threat propagation analysis method is proposed that incorporates the following aspects, which have not been comprehensively addressed in the literature before:

- Dependence of the different attacks (e.g sequential, concurrent etc)
- Uncertainty and frequency of occurrence of an attack event
- Uncertainty in launching time of an atomic attack (atomic attack step)
  - Level of vulnerabilities
  - Degree of exploitation of these vulnerabilities
  - Skill of the attacker
- Effectiveness of a countermeasure
- Time/ Rate of countermeasure actuation

Finally, to enable the DGA system to be Resilient-By-Design and survive an unavoidable cyber/physical component failure a novel solution exploiting the virtualization of the grid operation functions, Blockchain and Smart contracts is proposed. Furthermore, a simple proof of concept implementation of the proposed solution is also presented. The proposed solution optimally allocates the different grid operation functions, considering the hardware resources and requirements of the grid operation function, in a network of geographically separated control /automation units, when specific automation unit is compromised (either due to a random or intended failure). The Blockchain (or a Distributed Ledger Technology (DLT)) is used to store the status/configuration of the all the automation devices and requirements of the automation functions, so that safe and securer-initialisation of the grid operation functions hosted by the compromised automation device can be done on other healthy automation devices. a Multi Attribute Decision Making (MADM) based smart contract is proposed to perform this allocation of the DGA functions on the detection of the unavailable automation unit. A proof-of-concept implementation is done using Node-Red, Hyperledger and CALVIN framework. As such a solution is not been developed before for DGA system,

the work has resulted in a patent filed in Germany and in Luxemburg. The major contribution of the thesis is as follows:

- Explains how the Blockchain technology can be utilized in enabling the resilient functioning of the IT infrastructure supporting DGA system based on IDE4L architecture, where Substation Automation Unit (SAU)s are responsible for monitoring, control and protection of distribution grid.
- An explanation of how Blockchain based smart contracts can perform secure and distributed migration of applications is presented.
- A Proof of Concept (PoC) implementation of the proposed solution is presented. The Hyperledger Composer [Hyp] and Hyperledger Fabric are utilized for implementing the Blockchain and Smart contract component of the PoC. Then the implemented Blockchain application is integrated with the Calvin platform [Eri] via the flow programming tool called Node-Red [Nod] and REST API. Then, the scenario in which application (or actor) migration would get triggered automatically by the devices (or Runtimes) are proposed.
- A Multiple Attribute Decision Making (MADM) based algorithm is proposed for choosing the destination machine (or Runtime) to migrate the selected applications (or actors) is proposed.
- The working functionality (i.e. migration process) of the implemented prototype is tested and the performance evaluation i.e. variation in transaction latency under certain conditions, is performed.

1.3 Organization

The thesis is organised as given below.

1. Chapter 2 presents the methodology for the reliability evaluation of cyber-physical DGA system.
2. Chapter 3 presents the methodology for the susceptibility evaluation of cyber-physical DGA system.
3. Chapter 4 presents the a concept of a Resilient-by-Design DGA system and a Proof-of-Concept implementation.
4. Chapter 5 presents the Conclusion of the thesis.
5. Chapter 6 presents the possible future works.

2

Reliability of DGA systems

2.1 Introduction

The Reliability is defined as the probability that an entity (system, subsystem or a component) performs its set of required functions for an intended amount of time under given operational and environmental conditions[SW13]. It represents the probability that the system would function without failures over a time interval. The first rigorous definition of reliability was proposed by Laprie[LC87].The definition was further refined in [Avi+04]and was brought under an umbrella concept of dependability. Once the reliability of an entity is derived then the other attributes of dependability namely the availability and maintainability can be derived with additional information on the recovery procedures [TB17]. The purpose of analysing the reliability of any entity is to evaluate the probability of its failure at a specific time, so as to calculate the steady state and transient reliability indices like the Mean Time To Failure (MTTF) and transient failure probability respectively. The evaluation of reliability helps the entity designer in the following aspects.

- To choose the optimal recovery processes to ensure compliance of the entity to specific service level agreements. Generally the service level agreements are defined by percentage availability where the availability is defined as in equation(2.1) where MTTR corresponds to the Mean Time To Repair[TB17].

$$A = \frac{MTTF}{MTTF + MTTR} \tag{2.1}$$

- Evaluate the risks of the failure and their impacts.

A short introduction to the concept of the reliability and the basic mathematical formulations are provided below for better understanding.

Assuming that the entity is up at time $t = 0$, a continuous random variable $X \geq 0$ is defined to denote the failure time of the entity. The Cumulative Distribution Function (CDF) $F(t)$ of the time to failure of the entity before the time t is given as in equation(2.2). For non repairable entities(entities that do not have a recovery/repair mechanisms that would be activated once the entity fails), the $F(t)$ is a non decreasing function and as time tends to infinity the probability that the entity would fail reaches 1. Whereas for repairable entities the $F(t)$ converges to a specific value k where $0 \leq k < 1$ [TB17].

$$\begin{aligned} F(t) =& P\{X \leq t\}, where\ F(0) \geq 0, \\ & \lim_{t\to\infty} F(t) = 1 (non\ repairable\ entities) \\ & \lim_{t\to\infty} F(t) = k\ (repairable\ entities)\ where\ 0 \leq k < 1 \end{aligned} \tag{2.2}$$

The $F(t)$ is the probability that the entity fails before time t, thus representing the unreliability of the entity. Hence the reliability ($R(t)$) of the entity can then be derived from $F(t)$ as shown in equation(2.3).

$$R(t) = 1 - F(t) \tag{2.3}$$

The MTTF of an entity is calculated using the Probability Density Function (PDF) ($f(t)$) of the failure of the entity as shown in equation(2.5). It is interpreted as the first moment of the random variable X that denotes the failure of the entity. The $f(t)$ is derived either from $F(t)$ or the $R(t)$ as shown in equation(2.4).

$$f(t) = \frac{dF(t)}{dt} = \frac{-dR(t)}{dt} \tag{2.4}$$

The relation between the Reliability $R(t)$ and the $MTTF$ is as given in the equation(2.5) considering that the time for the entity to fail is a non negative random variable.

$$MTTF = \int_0^{+\infty} t \cdot f(t)dt = \int_0^{+\infty} R(t)dt \tag{2.5}$$

The calculation of $R(t)$ and the MTTF enables the system designer to predict the system failure and thus plan the redundancy, recovery and repair measures. It should be noted that the MTTF can only be defined for those entities that do not have any recovery/repair measures incorporated in other words for non-repairable entities [TB17]. A highly unreliable system would take small time to fail, thus demanding faster and expensive repair/recovery measures to meet specific service level agreements. For

repairable systems the Mean Time Between Failures (MTBF), that denotes the mean time between two consecutive failures of a repairable system.

From the equations(2.2)-(2.5) it is clear that in order to calculate the reliability of an entity the knowledge of the CDF of the failure of the entity is required. However, for all practical situations instead of the CDF the failure rate ($h(t)$) of the entity is known. The failure rate ($h(t)$ as shown in equation(2.6)) of a random variable X (where X denotes the time of failure of the entity) is defined as the conditional probability that the entity fails within a time interval $(t, t + dt]$ given that the entity has not failed till time t.

$$h(t) = \frac{f(t)}{R(t)} = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \tag{2.6}$$

Therefore, the reliability $R(t)$ can be represented as a function of $h(t)$ as given in equation(2.7).

$$R(t) = exp[-\int_0^t h(u)du] = e^{-\int_0^t h(u)du} \tag{2.7}$$

All the functions $F(t)$, $R(t)$, $f(t)$ and $h(t)$ are interrelated as shown in equations(2.2)-(2.7). With any of them known the remaining functions can be calculated. The aforementioned basic functions are applicable for the reliability analysis of a single component and also for a system with multiple components.

In the case of automation systems, different kinds of cyber-physical components are involved in ensuring a continuous service of an automation function. These may include sensors, actuators, connectors, peripherals, communication devices, communication mediums, data storage devices and data processing devices. In order to realise a specific automation service a set of the aforementioned components have to interact and be functional. Failure of any of the component would jeopardise the functioning of the automation service. Thus to quantify the reliability of the automation system to realise a specific automation service the following steps should be followed.

- Selection of an appropriate modelling formalism
- Derivation of a cross domain reliability index for cyber-physical system

There are different methods to evaluate the reliability of an entity. This can be done either by using simulation methods or derived analytically on the basis of predefined models of the failure process.

The most popular simulation approaches for the reliability evaluation are the non sequential and sequential Monte Carlo method [LB13][Li14]. Both methods generate randomly a large set of possible failure configurations of the constituting components of the entity. Each configuration would either correspond to a healthy state or a failure state of the entity. The frequency and probability of occurrence of the specific state of the entity is calculated. Once these are calculated the reliability of the entity is calculated as described in [LB13]. The only additional feature of the sequential Monte Carlo method over the non sequential method is that, it is able to evaluate even the temporal characteristics of the reliability of the entity[Li14]. A detailed analysis of the two aforementioned simulation methods is provided in [Li14]. It should be noted that the performance of the simulation method, both computational cost and accuracy of estimation, heavily depends on the sampling schemes used and the convergence criteria set. Furthermore, the aforementioned simulation methods can not be used for stochastically correlated failures of the constituting components of the entity. However, the simulation methods are favourable for the reliability analysis of large and complex entities, given that its constituting components have time insensitive independent failure characteristics.

The other approach for the reliability evaluation is based on pre-defined models of entity failure. There are different modelling formalism proposed for the reliability analysis[TB17][Li14]. They can be broadly divided into state space models and combinatorial models[TB17]. While choosing the modelling formalism, care should be taken to consider the limitation of each of them in modelling specific failure/recovery processes of an entity. For instance, the combinatorial methods like the Fault Tree (FT) and Reliability Block Diagram (RBD) can only be used for system reliability analysis where the constituting components of the entity have statistically independent failure characteristics, for e.g in those cases where there is no common entity present in the redundancies deployed. However, if they are statistically dependant and also have a failure state dependant failure/repair characteristics, then the state space methods like the Continuous Time Markov Chain (CTMC), variants of Stochstic Petri Nets (SPN) and methods based on Probabilistic Relational Models (PRM) [KNO13] can be used. A state space model consists of states and state transitions. Each state in the state space model represents the failure status of the entity. Whereas, the state transition represents the evolution of the failure status due to the failure of a specific component. Furthermore, the state space models can be used for modelling the time dependant failure mechanisms. However, it should be noted that as the size of the entity increases the computational cost of calculating the reliability indices increases exponentially. This is because, for an entity with n components will have 2^n

possible failure states. However, with state reduction methods as proposed in [Buc95][Son99][DHS03], this state explosion problem can be solved. In addition to the computational cost, for large state space models, the manual generation of the correct state transitions, can be challenging and error prone. Hence tools for automatic generation of the state space models (like the SPNs) should be employed. The generated models should be validated so as to ensure that it reflects the failure behaviour of the entity [TB17]. In spite of their inherent drawbacks, the CTMC(state space modelling formalism) is considered to be a powerful against all other aforementioned reliability evaluation methods because of the following reasons[Dom12][TB17].

- Model specific sequence of component failures
- Model different repair strategies
- Model state dependant failure rate
- Incorporate effectiveness of repair strategies
- Model common mode failures

The decision to choose a specific modelling formalism should be based on the structure and nature of the entity being modelled, specific reliability measure that is interesting to quantify and the ease of representation of the entity's failure/recovery processes into a specific modelling formalism[TB17].

In this study the CTMC has been used as the modelling formalism to evaluate the transient reliability of the cyber-physical systems as it allows the modelling of wide range of failure and recovery processes which can also be state dependant. Furthermore, CTMC models can be solved analytically without any measures of approximations required (unlike the simulation methods namely Sequential and Non-Sequential Monte Carlo method), allowing us to accurately estimate the reliability of the entity. Additionally a methodology to calculate the cross domain reliability of cyber-physical systems based on the analytical evaluation of the CTMC is presented .

2.2 Reliability analysis of DGA : Review

The distribution grid automation systems include the automation of secondary and primary substations, and their coordination with the help of the DMS deployed in the control centres. Major increase in the interest for the reliability analysis of DGA systems is because of the adoption of packet

based communication technologies (like Ethernet, 4G,5G, wireless etc) and communication protocols like IEC 61850 standard for the substation automation. The IEC 61850 standard proposes an Ethernet based communication infrastructure design for intra substation automation, provides framework for the development of digital models of the physical components of a substation and the semantics of data exchange and provides the mapping to standard communication services that enables IP based intra-substation and inter-substation communication. The IEC 61850 standard enables the digitization of substation. Thus, currently, there is a need to understand the reliability of the automation functions due the digitization of the substations.

The impact of the different communication architectures, reliability of the physical communication link and the reliability of data transmission within the prescribed latency, affects the performance of the automation system in realizing a specific automation function. Hence, most of the reliability analysis, reported in literature is done for specific automation functions. For instance the authors in [LSS14] propose cyber-physical interface matrix based on RBD for an IEC 61850 based protection application. The reliability of the substation automation systems to realize the switch gear control, interlocking, synchronization and indications using RBD is presented in [Haj11]. The authors in [HG12] evaluated the reliability of the communication architectures for data exchange for substation automation using RBD and quantified the sensitivity of the component failures on the overall reliability and availability of the communication infrastructure for substation automation. A hybrid approach utilizing the event tree and RBD is used to evaluate the impact of the reliability of the different communication infrastructures deployed within a substation to operate eight standard Industrial Substation switch gear configurations [HHG12]. A novel methodology based on zone graphs and minimal cutsets has been proposed in [DWD12] to evaluate the reliability of the power components for the substation. A stochastic flow network based analysis method is been proposed in [RJL18] to evaluate the reliability of a communication constrained protection system. The aforementioned research majorly focuses on either the cyber or the physical part of the part of a DGA. The reliability evaluation of cyber-physical DGA system is sparsely studied. However, in this regard, the authors in [Dom12], present a system theoretic approach that is based on state space modelling formalism. The authors in [KNO13] present a PRM based method that extends the standard Bayesian networks based analysis with incorporation of the functional and logical dependencies between the cyber and physical components of a substation. A sequential Monte Carlo method based reliability analysis of the cyber-physical distribution grid is presented in [Liu+18b]. From

the studies mentioned earlier it is evident that to evaluate the reliability of cyber-physical DGA system, a stochastic failure modelling formalism should be adopted that enables the modelling of complex redundancies and state dependant failure/recovery mechanisms. Furthermore, as different cyber and physical components are involved in the realisation of an automation function of the DGA, the logical dependence between the cyber and physical components have to be captured. The dependence capturing is important to identify the success and failure of an automation function that is subject to failure of the cyber and physical component failure. The capturing of the logical dependance helps in integrating, complex redundancy and recovery mechanisms, that heavily influence the reliability of the DGA system.

The methodology proposed in this thesis utilizes the CTMC to model the failure and recovery characteristics of the cyber and physical systems of the DGA system. Furthermore, a MDRM matrix is proposed that captures the logical and functional dependence of the cyber and the physical components in realising an automation function. A detailed explanation on the mathematical background of the CTMC and the proposed methodology is provided in the subsequent sections.

2.3 Mathematical background : CTMC and Markov Reward Models

2.3.1 System abstraction

CTMC is a state space modelling technique used to model the system failure and recovery processes to quantify the system reliability. One of the major steps in defining the CTMC based system failure model is the system abstraction. It determines the accuracy of its failure model. The system abstraction, in the context of reliability analysis, corresponds to the definition of the system failure characteristics. But before we do the abstraction of the system, to define its failure characteristics, we need to define what a system is.

Typically, a system is generally composed of one or more components. Each component has its own failure characteristics. A component can have 2 or more functional states.The major functional states are namely, the operational state and the failed state. The transition from an operational state to the failed state denotes the failure of the component, whereas, the transition from the failed state to the operational state denotes the recovery/maintenance/replacement of the failed component. In addition to the aforementioned functional states a component can have other functional states that can correspond to partial operation state due to the failure of

its sub-components. Such components in this study are considered as a system and status of its sub-components as the state of the system, where the sub-components have only two functional states namely operational and failed state. Such an abstraction methodology facilitates the break down of a complex system into a set of interacting simpler systems, where, each system is composed of components with just 2 functional states. This allows the detailed failure modelling of the individual simpler systems. Additionally by modelling the interaction between these simpler systems the overall failure characteristics of the bigger complex system can be evaluated. Typically these simpler systems interact with each other for realising a specific functionality of the bigger complex system. In order to do so, they either interact sequentially or provide alternate paths for the sequential interaction that correspond to the redundant measures adopted in the operation of the complex system. With the abstraction of individual system failure characteristics and their interaction with each other the over all failure characteristics can be modelled.

In this study the cyber-physical DGA is considered as a complex system. The CTMC is used to model the detailed failure process of cyber and physical systems. Furthermore a Multi Domain Reliability Matrix (MDRM) is proposed that captures the interactions between these different systems. Thus with the CTMC and MDRM the reliability of the cyber-physical system in realising an automation function is deduced. Furthermore, once the reliability is calculated, meaningful performance indices would be calculated using the Markov Reward Modelling (MRM)formalism.

2.3.2 System failure modelling with CTMC

The evolution of the system operational states under component failures is represented as a markovian stochastic process $\{X(t), t \geq 0\}$ with continuous-time and discrete state $\aleph = 0, 1, .., n$ [TB17], where the states represent the current set of functional components of the system. The stochastic time when a component fails, which triggers the state transition is represented as t. Assuming that the state of the system at time k is $X(k) = i$, the conditional probability that the system will be in state j at time $t + k$ can be mathematically expressed as Eq. (2.8):

$$\begin{aligned} Pr(X(k+t) = j | X(k) = i) = & Pr(X(k+t) = j | X(k) = i, \\ & X(u) = x(u), 0 \leq u < k) \end{aligned} \tag{2.8}$$

Where $X(u) = x(u), 0 \leq u < k$ denotes the history of the system state evolution until the time k but not including k.The Eq. (2.8) means that the probability of being in state j at time $k + t$ is only dependant on

the current state (i at time k) and is completely independent of anything that has happened in the past (from time $0 \leq u < k$).The state evolution at any specific point of time triggered by the component failure at that specific time, thus this process can be modelled as a markovian. Given a CTMC with all the possible states and the conditional state transition probability , the probability of specific state occupancy is calculated as shown in Eq. (2.9)

$$\begin{aligned} \pi_j(t) &= \sum_{i=0}^{n} p_{ij}(0,t) * \pi_i(0); \quad \textit{such that} \\ \sum_{i=0}^{n} p_{ij}(0,t) &= 1 \quad \textit{and} \quad \sum_{j=0}^{n} \pi_j(t) = 1 \end{aligned} \tag{2.9}$$

Where $\pi_j(t)$ is the Probability Mass Function (PMF) of the system to be in state j at time t, p_{ij} is the conditional probability of jumping to state j from state i , $\pi_i(0)$ is the PMF of the system to be in state i initially and n is the total number of system states possible.

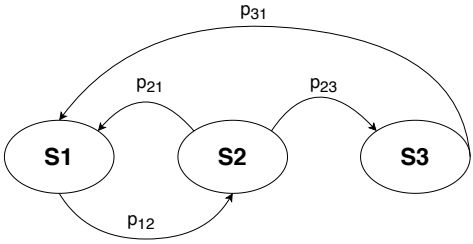


Figure 2.1: Generic CTMC

A generic CTMC model of a system, as shown in Fig. 2.1, is a directed graph, where the nodes represent the different system operational states ($S1, S2\&S3$) and the transitions(p_{ik}) denote the conditional probability of transiting from i^{th} state to k^{th} state.

Generic reliability indices derivable from CTMC failure models

The primary reliability index that can be calculated once the failure characteristics has been represented as a CTMC is the dynamic state occupancy probability ($\pi_j(t)$). It is the probability of the system being in j^{th} state as a function of time. Other reliability indices that could be derived from the dynamic state occupancy calculation are the mean failure

time of the system and mean time the system stays in a specific state before the system fails. The solution for the dynamic state occupancy probabilities is then obtained by solving the Eq. (2.10) which are based on the Chapman Kolmogorov's Eq. (2.11)-Eq. (2.12). A detailed derivation of the Eq. (2.10) based on equations Eq. (2.11)-Eq. (2.12) can be found in [TB17].

$$\frac{d\left(\pi(t)\right)}{dt} = \boldsymbol{\pi}(t)Q \tag{2.10}$$

$$\pi_j(t) = \sum_i \pi_i(u)(0,t) * p_{ij}(u,t) \tag{2.11}$$

$$p_{ij}(u,v) = \sum_k p_{ik}(u,t) * p_{kj}(t,v) \quad for\ u \leq t \leq v \tag{2.12}$$

Where $\boldsymbol{\pi}(t) = [\pi_1(t), \ldots \pi_j(t) \ldots, \pi_n(t)]$ is a row vector with dimension $(1 \times n)$ of dynamic state occupancy probabilities. Q (as shown in Eq. (2.13))is the infinitesimal generator matrix and u,t,v are three instants of time.

$$Q = [q_{ij}]\,,\ such\ that\ q_{ii} = -\sum_{\forall j} q_{ij} \tag{2.13}$$

Where q_{ij} is the rate at which the system transits from state i to state j. The off-diagonal elements of Q (q_{ij} where $i \neq j$) correspond to the failure rate of the k^{th} component (specified as λ_k) that triggered the state transition of the system(from i to j). It should be noted that the $p_{ij}(u,t)$, the conditional probability that a system jumps from state i to j at time t instant given that the system is at state i at time u, corresponds to the failure of k^{th} component by time t given that that time u it was functional. Therefore, the failure rate (λ_k) the conditional probability of the state transition (p_{ij}) and is given as in Eq. (2.14). However, in our study since the focus of the investigation is on the operational life time and not on the ageing conditions of the component, the failure rate is considered constant. Therefore, for the current study the relationship between the elements of the infinitesimal generator (Q) is given as in Eq. (2.15).

$$\begin{aligned} &\lambda_k(t) = -\frac{1}{1-p_{ij}(t)} \cdot \frac{d}{dt}(1-p_{ij}(t)) \\ &where \\ &p_{ij} = 1 - e^{\lambda_k(t)t}\,; \end{aligned} \tag{2.14}$$

$$q_{ij} = \lambda_k \tag{2.15}$$

Given the initial probability of finding the system in any of the failure states as $\boldsymbol{\pi}(0)$, the prediction of the probability of finding the system in any of the failure states as a function of time $\boldsymbol{\pi}(t)$ can then be calculated as shown in Eq. (2.16).

$$\boldsymbol{\pi}(t) = \boldsymbol{\pi}(0)e^{Qt} \tag{2.16}$$

Additional reliability indices derivable from CTMC failure models of non-repairable systems

A system without a complete recovery process is considered as a non repairable system [TB17]. For such systems the MTTF can be calculated. In order to calculate the MTTF of the system, a failure state is modelled as an absorbing state in a CTMC. An exemplary CTMC model of a system with a failure state from which no recovery is possible is shown in Fig. 2.2. The state S_{fail} is the absorbing state where there is only an incoming transition but no out going transition. The system failure model with an absorbing state represents a non repairable system, wherein, when the system reaches the absorbing state (failed state) has zero probability to leave this state. In this exemplary system composed of three components, when all the three components function the system is in fully functional S_{up} state. If component 1 fails (with a failure rate λ_3) followed by failure of component component 2 (with a failure rate λ_2) then the system reaches the failure state , S_{fail}. Alternatively if component 3 fails (with a failure rate λ_3) when the system was fully functional, then the system fails. If only Component 1 fails (with a failure rate λ_1) when the system was previously fully functional, the system goes to partial functional state $S_{partial-up}$. The MTTF of the system, whose failure model has an absorbing state,

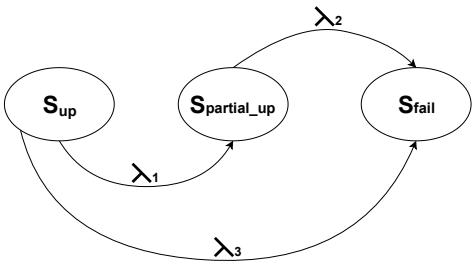


Figure 2.2: Generic CTMC model with an absorbing state

is then calculated as the expected time ($E[T_a]$) to be absorbed into the

absorbing state, as shown in Eq. (2.17). The ε is a row vector of ones, with an order of the transient states (all states in the CTMC except the absorbing states).

$$E[T_a] = -\boldsymbol{\pi}_u(0)Q_u^{-1}\varepsilon^T \tag{2.17}$$

Subsequently, the time spent in each transient state before it fails ($\tau = [\tau_1, \tau_2, ..., \tau_u]$) can also be calculated as shown in Eq. (2.18). The transient states represent the different operational states of the system that might correspond to full operation mode or sub-optimal operational mode depending on the severity of the component failure condition.The time spent in sub-optimal operation states might be required to evaluate the total cost of sub-optimal operation.

$$\boldsymbol{\tau} = -\boldsymbol{\pi}_u(0)Q_u^{-1} \tag{2.18}$$

$$Q = \begin{bmatrix} Q_u & \boldsymbol{a_1}^T \\ 0 & 0 \end{bmatrix} \tag{2.19}$$

Q_u (as shown in Eq. (2.19) is a partition of Q over the transient states Ω_u , $\boldsymbol{a_1}$ is a column vector grouping the transition rates from any transient state to the absorbing state.

Additional reliability indices derivable from CTMC failure models of repairable systems

A repairable system is characterized by at least a single recovery process from the failed state. An exemplary CTMC based failure model of a repairable system is shown in Fig. 2.3. It has three operational states, namely, a full operational state denoted as S_{up}, a partial operational state ($S_{partial-up}$) and failed state (S_{fail}). The system fails with a rate of λ_1 from full operational state to a partial operational state and similarly fails at a rate of λ_2 from a partial operational state to the failed state. However, there are two recovery processes modeled with a recovery rate of μ_1 and μ_2 from partial operational state and the failed state to the full operational state respectively. Physically, the failure rate corresponds to the rate at which the components of the system fail, which triggers the system to move from full operational state to partial operational state and to failed state. Whereas, the recovery rate corresponds to the rate at which a specific failed component of the system has been repaired or replaced by the maintenance crew.

It can be noted from the CTMC model presented in Fig. 2.3, that one can reach all the other states in the system from any state. Such CTMCs are

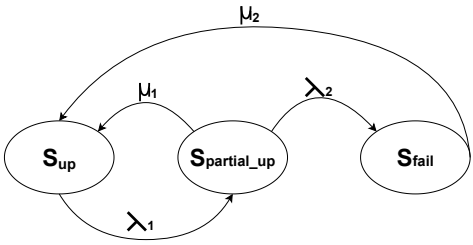


Figure 2.3: CTMC model of a repairable system

known as irreducible markov chains. One of the interesting properties of such irreducible markov chains is that, irrespective of the initial condition of the system, the probability of the system being in any of the states would converge to a steady state value [TB17]. That means that the state occupancy probability would be constant and not be a function of time anymore. One can interpret such a failure dynamics as process of reaching an equilibrium point, that denotes the probability of finding the system in different operational states, which is time independent. The main forces governing the process of reaching this equilibrium point are the rates at which the failure happens and the rates at which the maintenance/recovery is carried out. Therefore for a completely repairable system, modeled as a CTMC with no absorbing state, the state occupancy probability can be calculated by solving the Eq. (2.20) and Eq. (2.21) simultaneously.

$$\boldsymbol{\pi}_{\boldsymbol{steady-state}} \cdot Q = 0 \tag{2.20}$$

$$\sum_i \boldsymbol{\pi}_{\boldsymbol{steady-state}}(\boldsymbol{i}) = 1 \tag{2.21}$$

$$\boldsymbol{\pi_{steady-state}} = (A^T * A)^{-1} * A^T * B$$
$$where$$
$$A = \begin{bmatrix} Q^T \\ 1 \end{bmatrix} = \begin{bmatrix} q_{11} & q_{21} & \dots & q_{n1} \\ \vdots & \vdots & \vdots & \vdots \\ q_{1n} & q_{2n} & \dots & q_{nn} \\ 1 & 1 & 1 \dots & 1 \end{bmatrix} \tag{2.22}$$
$$B = \begin{bmatrix} 0_1 \\ \vdots \\ 0_n \\ 1 \end{bmatrix}$$

The state occupancy probability calculated is normally called as the steady state probability. Solving for the steady state probability is a typical example of solving an over determined problem. Therefore the standard method of solving over-determined linear equations as shown in Eq. (2.22) can be used to find the steady state probability. Where, n is the number of states in the CTMC model.

2.3.3 Markov Reward Models

A Markov Reward Model (MRM) extends the modeling capabilities of a CTMC by adding to the states or the transitions or both an attribute called reward [TB17]. The reward often represents a performance level or a cost associated with the state, or some property of the state or of the transition. Further, the use of a non-negative reward attached to CTMC models provides a unified framework to define and compute measures that characterize the system behavior of interest to the modeler. For example, if the performance of a real-time state estimation distribution grids is being evaluated for failures in data acquisition, then through MRM the average achievable accuracy of the state estimation for the various failures of the components involved in the acquisition of the measurements, can be calculated. In this case the reward is the achievable accuracy for the available measurements, the states being the set of measurements that are available considering the failure of components involved in measurement acquisition. Similarly, for the evaluation of a control/protection application, the energy not supplied could be considered as a cost associated to each operational state of the control/protection function CTMC failure model.

Given the state occupancy probability (or calculated using the principles of CTMC) the performance of a non repairable system can then

be calculated as per Eq. (2.23), where n is the number of states in the CTMC model, r_i is the reward/cost associated to each state and $\pi_i(t)$ is the probability of occupying the i^{th} state.

$$Performance - Index_{avg}^{non-repairable}(t) = \sum_{i=1}^{n} r_i * \pi_i(t) \tag{2.23}$$

Similarly for a complete repairable system the average performance of the system can be evaluated as given in Eq. (2.24).

$$Performance - Index_{avg}^{repairable} = \sum_{i=1}^{n} r_i * \pi_i \tag{2.24}$$

In some cases the total accrued reward/cost over a time period might be of interest. For such cases the performance index can then be evaluated as per Eq. (2.25)

$$Performance - Index_{time-avg} = \sum_{i=1}^{n} r_i \int_0^t \pi_i(u)du \tag{2.25}$$

2.3.4 Component failure model : Hardware and Software failures

One of the most important information required for generating the CTMC based failure models of any system is to model the failure characteristics of its constituting components. In this study the reliability analysis of DGA infrastructure is made, where the components of the DGA are cyber-physical in nature. This means that a majority of the components have a hardware part and a software part.

Generally, the reliability of the hardware part is characterized by its failure rate, which is a function of time, and it follows a bathtub curve [Joh89], as depicted in 2.4. A Typical component life cycle can be divided into three sections the burn-in period, the useful life, and the wear-out period. The burn-in period corresponds to the high failure rate of the components due to undetected defects in the manufacturing process. The failure rate tends to stabilize after the initial burn-in period to a constant value. The useful period corresponds to the warranty period of the component; finally, as the component ages, the failure rate increases. This study considers that all the components of the system are in a useful period of their life cycle and thus have a constant failure rate. In this study all the hardware related failures would be modelled with a constant failure rate. There are different standards that provide the failure rates for different hardware

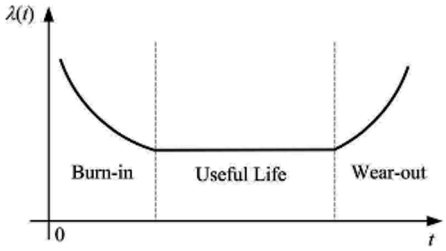


Figure 2.4: Failure rate of the component as a function of time

components. In this study the failure rates provided in [Def91],[AG05]. It should be noted that, the failure rates of the same equipment provided in different standards may differ. This variation is due to the assumption in the environmental conditions in which the failure tests were made, the assumptions made in the calculation of failure statistics, the testing time intervals, the failure sample size, sample homogeneity and the different failure modes that affect the failure of the equipment analysed using the Failure Mode Effect & Diagnostic Analysis (FMEDA). Therefore, care should be taken in selecting the failure rates from different standards, by properly checking the different FMEDA results of the equipment.

As for the modelling of software failures, in this study the method presented in [AFB07] is assumed to be used which is based on the method proposed by Shooman in [Sho73][Sho72] to predict the failure rate and repair time of a specific software. The software reliability can be defined as the probability of a given software operating for a specified time period without a software error, when used within the design limits on an appropriate machine [AFB07]. A detailed modelling of the software failure is out of scope of this thesis. With these methods the software failure can also be represented as random event with exponential distribution. In this study all the firmware failures and failures in the specific algorithms implemented in a hardware would be considered as part of software failure.

2.4 Reliability analysis of DGA infrastructure

The DGA infrastructure is responsible for realising many automation functions. The automation functions are help in monitoring, control and protection of distribution grids. The generic components involved in the DGA is shown in Fig. 2.5. They are namely the sensors (Measurement devices), communication infrastructure, Controllers and Actuators. A

combination of the aforementioned devices are responsible for realising any automation function. Additionally, any automation function can be considered as a combination of the three basic functional blocks depicted in the Fig. 2.5. These functional blocks are the following.

- Measurement data Acquisition
- Measurement data processing and decision making
- Actuation of the control action

For example, the real-time monitoring of distribution grids involves Measurement data acquisition and processing of measurement data using a State Estimation(SE) algorithm that enable condition monitoring of the power grids even if the measurements are corrupted by noise. The measurements could be from Phasor Measurement Units(PMUs), Remote Terminal Units(RTUs) and/or Smart Meters(SMs). Depending upon the automation architecture the measurement data could be either collected centrally or collected at distributed (regional) data concentrators where the SE is hosted the SE processes this data and provides an estimate of the state of the power grid. In case of Volt-VAr control of distribution grid following the IDE4L automation architecture, the state of the grid provided by the SE is used to determine the deviation of the grid voltage from the prescribed operational ranges. If there are any violation then a control command to either change the tap position of an On Load Tap Changer(OLTC) or the opening/closing the capacitor banks is issued. Hence the Volt-VAr function can be implemented with all the three basic functional blocks.

The sensors, measurement devices like the PMUs, remote actuator control devices like the RTUs form the part of the physical infrastructure. The communication devices like the switches, routers, modems, base stations (in case of cellular communication infrastructure) and the ICT infrastructure hosting the different databases and servers hosting the algorithms of the EMS/DMS form the cyber infrastructure. The CTMC is a state space based method, hence it is subject to the state explosion problem. This is because, for system with n components there would be 2^n states in the failure model.

Therefore, in this study the automation function is subdivided into smaller basic functional blocks that interact sequentially. By doing so the failure model of the complete automation function can be reduced to a set of smaller failure models interacting with each other. This also reduces the chances of introducing errors in the failure models as smaller systems are involved. In order to further reduce the size of the models individual failure

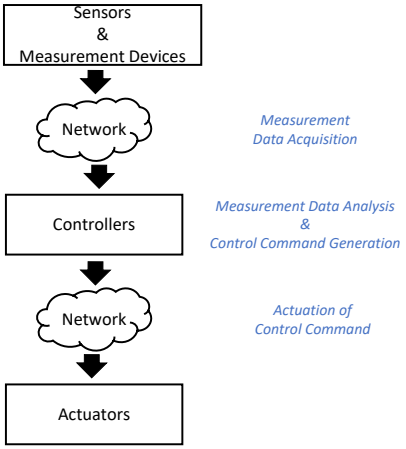


Figure 2.5: Basic functional blocks of any automation function

models are created for physical infrastructure and cyber infrastructure considering their hardware and software failure characteristics. Detailed CTMC failure models of cyber and physical systems involved in each functional blocks are created. The interaction of the cyber and physical systems within a basic functional block is captured in a MDRM. Using the reliability indices derivable from the CTMC models and the MDRM the reliability of the complete basic functional block is derived. Similarly the reliability of the other functional blocks that play a part in realising the whole automation function is calculated. The overall reliability of the automation function is then just the product of the reliability of the involved functional blocks as they are sequentially interacting with each other. A detailed explanation of the proposed methodology for evaluating the reliability of a specific automation function is provided in upcoming sections.

2.4.1 Proposed Methodology

The major steps involved in the reliability analysis of the DGA systems in realising a specific automation function is as given below:

1. Identify the functional blocks involved in realising a specific DGA function.

2. Identify the different deployment schemes of the different physical and cyber infrastructures involved in each functional block.

3. Model failure characteristics of each function block using CTMC and MDRM.
   a) Create the failure models of physical infrastructure involved in the realising the functional block.
   b) Create the failure models of cyber infrastructure involved in the realising the functional block.
   c) Build the infinitesimal generator (Q matrix) for each failure model of the physical and cyber infrastructure.
   d) Calculate the dynamic probability of the physical and cyber infrastructure in being in all of the operational states defined in the failure model using the Eq. (2.10)-Eq. (2.16).
   e) Derive the MDRM using the dynamic state occupancy in the previous step, that helps in capturing the interactions of cyber and physical infrastructure.

4. Calculate the reliability of the functional block based on the MDRM generated in the previous step

5. Calculate the overall reliability of the DGA function
   a) The individual functional blocks are sequentially interacting with each other
   b) The scalar product of the reliability of the individual functional blocks calculated in Step 4 is the overall reliability of the DGA function .

In the first step the infrastructure operators/ experts identify the different functional blocks involved in realising a specific DGA function. The detailed deployment scheme of the different functional blocks is studied in the second step. The failure process of of each cyber/physical component is studied. Furthermore, any redundancy measures taken to provide alternate paths for communication or repair/replacement of specific physical component is necessary for the successful realisation of the individual functional blocks. The detailed CTMC failure model of the cyber and physical infrastructures considering the failure processes of each cyber/physical component, their redundancy/repair/replacement measures adopted for realising the functional block, is created. As an example, a system is considered where measurements from 3 different measurement devices (like PMUs) is collected at a Phasor Data Concentrator (PDC).

The measurement data is sent to the PDC by each measurement device by separate Communication Channels (CC). A pictorial representation of the the aforementioned automation system responsible for monitoring of distribution grids utilising the PMUs is shown in Fig. 2.6.

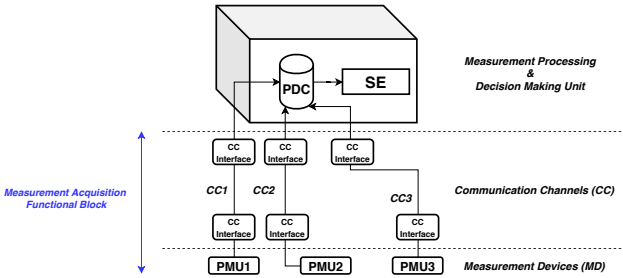


Figure 2.6: Exemplary automation infrastructure for monitoring of power grids with PMUs

In Step 3, the CTMC based failure model of the three measurement devices and their corresponding communication channels are built as shown in Fig. 2.7 and Fig. 2.8 respectively. Since there are three measurement devices and three communication channels involved in the measurement data acquisition, there are $2^3 = 8$ operational states for both the PMU infrastructure and the Communication infrastructure individually. As shown in Fig. 2.7, the circles represent the 8 operational states of the PMUs states and the transitions represent the failure of a specific PMU. The numbers mentioned in the subscript denote the specific PMU device that is functional. For e.g PMU_{123} corresponds to a state where all the three PMUs are functional, PMU_{12} corresponds to a state where only the PMU 1 and the PMU 2 are functional and so on. Finally the circle shaded black corresponds to the operational state where none of the PMUs are functional. The PMU_{iFail} is the failure rate of the i^{th} PMU as calculated in Eq. (2.26).

The failure of a PMU can either be caused by a hardware failure, time synchronization system failure or a software failure. The aforementioned failures can be considered as a random event. The PMU would fail as soon as any of the failure event occurs. Therefore, the probability of the i^{th} PMU to fail before time t ($Pr(X^{PMU_i} \leq t)$) is the probability that at least one failure event occurs before time t ($Pr(min(X^{HW}, X^{SW}, X^{SYNC}) \leq t)$). Where X^{PMU_i} is the actual time that the i^{th} PMU takes to fail and X^{HW}, X^{SW}, X^{SYNC} are the actual time that a hardware failure, software

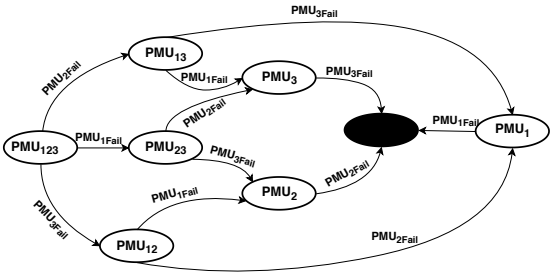


Figure 2.7: CTMC failure model of Measurement Devices (PMUs)

failure, and the time synchronization system takes to fail respectively. In this study component failure time is assumed to have an exponential Probability Density Function (PDF), as the study focuses on the operational life time of a component. The failure rate of the i^{th} PMU (λ_i^{PMU}) can be calculated as a function of the individual component failure rates as given in Eq. (2.26), based on the law that governs the calculation of the minima of a set of random variables with exponential PDF [TB17].

$$\lambda_i^{PMU} = \lambda_i^{HW} + \lambda_i^{SW} + \lambda_i^{SYNC} \tag{2.26}$$

In case of the communication channel, its failure is caused by the hardware/software failures of the CC-interface (which could be a switch/router/-modem) or the failure in the physical medium of communication (like damaged optic fibres, jamming of the wireless communication etc). As depicted in Fig. 2.8, similar to the failure model of the PMUs, the failure model of the communication channels has 8 operational states represented in circles, where the subscripts denote the specific communication channel that is functional. the circle shaded black corresponds to the state where none of the CCs are functional.

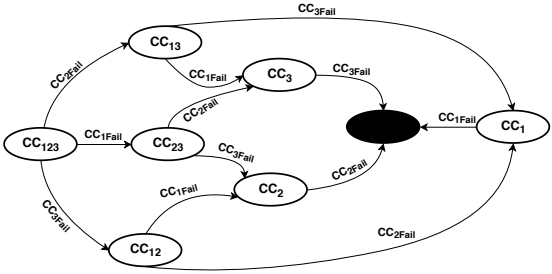


Figure 2.8: CTMC failure model of Communication Channels (CCs)

Furthermore, the transition from one state to another is caused by the failure of i^{th} Communication Cannel (CC). Each communication channel could be composed of a set of CC-interfaces (switches, routers, modems) and physical medium connecting the CC-interfaces. Therefore, the failure of a single CC can be caused by the failure of any of the CC-interfaces or the physical mediums. Therefore, the failure rate of the i^{th} CC is given by Eq. (2.27)

$$\lambda_i^{CC} = \sum_{j=1}^{r} \lambda_j^R + \sum_{k=1}^{m} \lambda_k^M + \sum_{u=1}^{s} \lambda_u^S + \sum_{l=1}^{q} \lambda_l^{PM} \tag{2.27}$$

where λ_j^R,λ_k^M, λ_u^S and λ_l^{PM} correspond to the failure of j^{th} relaying component,k^{th} modem, s^{th} switch and l^{th} physical medium link respectively.

The two CTMC failure models corresponding to the PMUs and their communication results in a multi-layered CTMC model including the cyber and physical infrastructure failure model. The next sub-step in Step 3 is the calculation of the of the dynamic state occupancy probabilities of the PMU devices and their communication channels. Firstly, the Q matrix is generated for each failure model by using the equations Eq. (2.26), Eq. (2.27) and Eq. (2.13). With the Q matrix the dynamic state occupancy probabilities denoting the probability of physical and cyber infrastructure to be in any specific operational state is calculated using the Eq. (2.16). The dynamic state occupancy probabilities of the physical and cyber infrastructure operation states is then used to create the Multi Domain Reliability Matrix (MDRM). The MDRM is generated to capture the interactions between the different CTMC failure models of cyber and physical infrastructure. The purpose of the MDRM is to provide the probability of the functional block to be in any of the possible operational

states of the cyber and physical infrastructures. The MDRM for acquisition of the PMU measurements is as given in Eq. (2.28)

$$
\begin{aligned}
&\boldsymbol{MDRM}(i,j)(t) = \mathbf{\Pi}^{PMU}(i)(t) * [\mathbf{\Pi}^{CC}(j)(t)]^T \\
&where \\
&\mathbf{\Pi}^{PMU}(i)(t) = \\
&[\pi_{123}^{PMU}(t), \pi_{12}^{PMU}(t), \pi_{13}^{PMU}(t), \pi_{23}^{PMU}(t), \\
&\pi_{1}^{PMU}(t), \pi_{2}^{PMU}(t), \pi_{3}^{PMU}(t), \pi_{Fail}^{PMU}(t)] \\
&\mathbf{\Pi}^{CC}(i)(t) = \\
&[\pi_{123}^{CC}(t), \pi_{12}^{CC}(t), \pi_{13}^{CC}(t), \pi_{23}^{CC}(t), \\
&\pi_{1}^{CC}(t), \pi_{2}^{CC}(t), \pi_{3}^{CC}(t), \pi_{Fail}^{CC}(t)]
\end{aligned}
\tag{2.28}
$$

The $\mathbf{\Pi}^{PMU}(i)(t)$ and $\mathbf{\Pi}^{PMU}(i)(t)$ are row matrices corresponding to the dynamic occupancy probabilities of the different operational states of the PMU devices and the communication channels respectively at a given point of time. The $MDRM$ is three dimensional matrix with one dimension being time (order of this dimension equal to the number of time instances considered within the time horizon for which the reliability analysis is performed) and the other two dimensions correspond to the physical infrastructural operational states and the cyber infrastructural operational states, respectively. In this example the physical infrastructural operational states corresponds to the 8 operational states of the PMU devices and the cyber infrastructural states correspond to the 8 operational states of the communication channels.

It should be noted that the entries in the $MDRM$ quantifies the probability of the combined cyber-physical infrastructure to be in a specific physical and cyber infrastructure operational state. For example $MDRM(1,1)$ corresponds to the dynamic probability (probability as a function of time) of the cyber-physical system state where all the PMUs and all the communication channels are functional. Similarly the $MDRM(2,3)$ corresponds to the dynamic probability of the cyber-physical system where the PMUs PMU_1 and PMU_2 are functional but only communication channels CC_1 and CC_3 are functional, and so on. It is important to notice that, in case of $MDRM(2,3)$ though PMU_1 and PMU_2 are functional , successful reception of only PMU_1 measurements is possible as in this combined

cyber-physical state the CC_2 is not functional and only CC_1 is functional.

$$MDRM(t) = \begin{bmatrix} p_0(t) & p_1(t) & p_2(t) & p_3(t) & p_4(t) & p_5(t) & p_6(t) & p_7(t) \\ p_8(t) & p_9(t) & p_{10}(t) & p_{12}(t) & p_{13}(t) & p_{14}(t) & p_{15}(t) & p_{16}(t) \\ p_{17}(t) & p_{18} & p_{19}(t) & p_{20}(t) & p_{21}(t) & p_{22}(t) & p_{23}(t) & p_{24}(t) \\ p_{25}(t) & p_{26} & p_{27}(t) & p_{28}(t) & p_{29}(t) & p_{30}(t) & p_{31}(t) & p_{32}(t) \\ p_{33}(t) & p_{34}(t) & p_{35}(t) & p_{36}(t) & p_{37}(t) & p_{38}(t) & p_{39}(t) & p_{40}(t) \\ p_{41}(t) & p_{42}(t) & p_{43}(t) & p_{44}(t) & p_{45}(t) & p_{46}(t) & p_{47}(t) & p_{48}(t) \\ p_{49}(t) & p_{50}(t) & p_{51}(t) & p_{52}(t) & p_{53}(t) & p_{54}(t) & p_{55}(t) & p_{56}(t) \\ p_{57}(t) & p_{58}(t) & p_{59}(t) & p_{60}(t) & p_{61}(t) & p_{62}(t) & p_{63}(t) & p_{64}(t) \end{bmatrix} \tag{2.29}$$

As shown in Eq. (2.29), there are 64 possible operational states of the combined cyber-physical infrastructure of the functional block. Out of all possible combination of operational states of cyber and physical states only a set of them would correspond to the operational state where the functional block is realisable. It should be noted that the $MDRM(t)$ also shows the probability of different performance classes of the functional block. There are four performance classes defined, which are depicted with 4 different colours in the $MDRM(t)$. The total probability of the cyber-physical system delivering a specific performance class is given as Eq. (2.30)

$$\begin{aligned} &\mathbf{\Pi}_k^{Performance-Class}(t) = \sum_{i=1}^{N} p_i(t) \\ &\forall(i) \in k^{th}\ Performance - Class \\ &where\ N = number\ of\ elements\ in\ MDRM(t) \end{aligned} \tag{2.30}$$

The entry shaded in green is the probability of receiving all the PMU measurements and correspond to the $PerformanceClass_1$. The entries shaded in blue are the probability of receiving any two PMU measurements and correspond to the $PerformanceClass_2$. The entries shaded in orange correspond to $PerformanceClass_3$ that denotes the probability of receiving measurements from any of the PMUs. Finally the $PerformanceClass_4$ corresponds to the probability of not receiving any of the PMU measurements are shaded in grey.

The reliability of the functional block is then calculated based on the specific performance classes that help in realising it. For example, if the measurements from all PMUs have to be received for proper functioning of the monitoring algorithm then probability of the cyber-physical

system being in the $\mathbf{\Pi}_1^{Performance-Class}(t)$ would be the reliability of the functional block of measurement acquisition. However, it is possible that the monitoring algorithm is robust and functions even if one of the PMU measurement is available, then the functional block can be considered reliable. In this case the reliability of the functional block is the probability of delivering a performance class of $\mathbf{\Pi}_1^{Performance-Class}(t)$ or $\mathbf{\Pi}_2^{Performance-Class}(t)$. Similarly, if reception of any PMU measurement is enough for the proper operation of the monitoring application, then the reliability of the functional block of measurement acquisition would be the probability of delivering a performance class of $\mathbf{\Pi}_1^{Performance-Class}(t)$ or $\mathbf{\Pi}_2^{Performance-Class}(t)$ or the $\mathbf{\Pi}_3^{Performance-Class}(t)$. In general, the reliability of the functional block $\boldsymbol{R_{PMU}^{FB}(t)}$ is given as in Eq. (2.31). The calculation of the reliability of $\boldsymbol{R_{PMU}^{FB}(t)}$ marks the end of Step 4.

$$\begin{aligned} \boldsymbol{R_{PMU}^{FB}(t)} &= \sum \mathbf{\Pi}_i^{Performance-Class}(t) \\ \forall\,(i) &\in Set(Reliable\ operation\ mode) \end{aligned} \tag{2.31}$$

Similar to the failure modelling of the PMU measurement acquisition system, the failure model of the Measurement Processing & Decision Making Unit should also be built. For this example, a two state CTMC model is built as shown in Fig. 2.9. The SE algorithm fails if the there is a hardware failure or the software failure of the device that is hosting it or if the PDC fails. There are only two states in the CTMC model. The SE_{up} corresponds to the state when the PDC, the hardware hosting the SE algorithm and its software are functioning properly. If any of the previously mentioned failure occurs, then the system goes to the SE_{Down} state. The probability of the Measurement Processing & Decision Making Unit to be in the SE_{up} is calculated according to the Eq. (2.13) and Eq. (2.16) where the Q is generated considering the failure rate of the hardware, software of the device and that of the PDC.

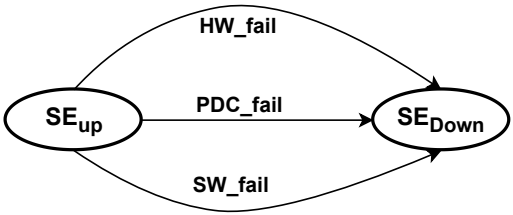


Figure 2.9: CTMC failure model of Measurement Processing and Decision Making Unit

In Step 5 the overall reliability of the cyber-physical system is calculated. Since there are only two functional blocks involved in realising the aforementioned exemplary automation function, the overall reliability of the automation function $\boldsymbol{R_{AF}(t)}$ is then calculated as shown in Eq. (2.32).

$$\begin{aligned} \boldsymbol{R_{AF}(t)} &= \prod_i \boldsymbol{R_i^{FB}(t)} \\ &= \boldsymbol{R_{PMU}^{FB}(t)} * \pi_{SE_{up}}(t) \end{aligned} \tag{2.32}$$

In the next sections two test cases are presented where the proposed reliability analysis method would be applied to evaluate the reliability of Real-Time Monitoring of distribution grids using Advance Metering Infrastructure (AMI) and PMUs, and Multi-Terminal Direct Current (MTDC) grids.

2.5 Test Case 1: Monitoring systems for distribution grids

2.5.1 Introduction

The distribution grids are becoming active with high penetration of distributed energy resources, rise of Prosumers, high integration of electric vehicles [Mar+14] and enforcement of the directives (like the winter package in Europe [Coma]) incentives for building local energy communities. The distribution grid of the future would be modernized with Advance Metering Infrastructure (AMI) and installation of low cost Phasor Measurement Unit (PMU)s and other local sensors and actuators responsible for monitoring and controlling local energy generation, storage and consumption, as shown in Fig. 2.10.

For the safe operation of the active distribution grid, Advance Distribution grid Automation (ADA) is necessary. One of the primary functions of the ADA is the real time monitoring of the distribution grid. This involves the acquisition of measurement data from measurement devices like the Smart Meter (SM) and low cost PMUs, processing them through State Estimation (SE), which estimates the status of the grid. With advancement in the ICT, operators of distribution grid have adopted heterogeneous ICT solutions for automating the distribution grid [GR15]. For example, the SM data from the SM is initially collected at a local smart meter data concentrator, before forwarding it to the Meter Data Management System (MDMS) hosted at the secondary substation/control centre of the distribution grids. Typically a set of communication infrastructures are used used to send the SM data to the MDMS through the

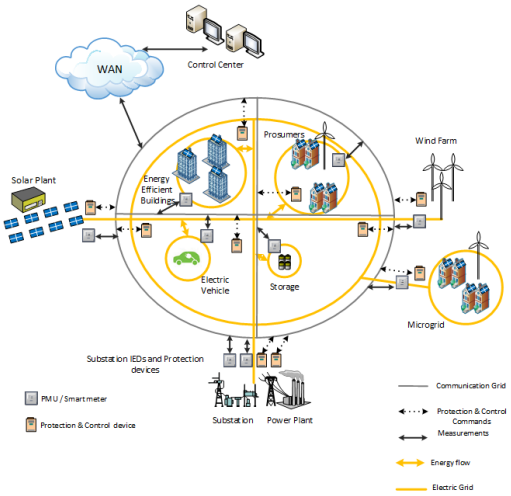


Figure 2.10: Active Distribution Grid

Meter Data Concentrator [GR15]. These could be a mix of the following communication technologies: ZigBee, Radio Frequency (RF), Worldwide Interoperability for Microwave Access (WiMax), Wireless Fidelity (Wi-Fi), Power Line Communication (PLC), Broadband over Power Lines (BPL), General Packet Radio Service (GPRS), Optical Fibers (FO) [Gar15] and also cellular networks like Long Term Evolution (LTE) and 5G [Suc].

Similarly, the acquisition of PMU measurements and other grid measurements from the street cabinets and substations would use any of the aforementioned type of communication technology. So the complete measurement acquisition system involving PMUs and SM and RTUs in substation is a part of a monitoring system that utilizes heterogeneous ICT infrastructure. Furthermore, the data acquisition involves multiple steps, where the data is aggregated at intermediary levels at some local data concentrators before it is forwarded to the control centre/substations where the State Estimation is hosted that predicts the status of the grid on the basis of the measurements received from the different measurement devices. So the measurement acquisition system responsible for real-time monitoring of distribution grids is a cyber-physical system.

The reliability analysis of the cyber-physical monitoring system is useful to evaluate not only the mean availability of monitoring functionality of the DGA but also the mean achievable accuracy of the SE given the failure

configuration of the different physical and cyber components involved in the measurement acquisition. Additionally, it should also be noted that, the impact of losing measurements from different measurement devices would have dissimilar impacts on the performance of the State Estimation. This is because the accuracy of the estimation is determined by the accuracy of the measurements (which are dissimilar for different measurement devices) and the electric quantity that they correspond to (like voltage, current, active power, reactive power etc.)[Pau+19a][Pau+19b][Sad+16].

In this study the reliability analysis of a completely repairable system, responsible for real-time monitoring of distribution grids (one MV grid section) that follows the IDE4L automation architecture [Ang+17] is presented. The proposed methodology could also be modularly extended for the complete distribution grid with multiple MV grid. The mean availability of the monitoring system and the achievable accuracy in estimating the state of the grid, considering the different stochastic failures of the cyber and physical components of the monitoring system is evaluated. The description of the test system, failure models of the cyber and physical components of the measurement acquisition systems and the results of the reliability analysis are provided in the upcoming subsections.

2.5.2 Test case description

Test case considered in this study is the real time monitoring of the low voltage distribution grid, automated in accordance to the IDE4L automation architecture [Rep+17]. The Fig. 2.11 shows the division of the active distribution grid according to the operational voltage levels, namely the Medium Voltage grid and Low Voltage grid sections. The distribution grids are usually operated with radial structure. A MV grid segment as shown in Fig. 2.11, has multiple MV/LV substation connected radially. Each of these substations are called secondary substations that are responsible to manage the downstream LV grid. In order to do so each of the MV/LV substation is equipped with Substation Automation Unit (SAU) named as LV-SAU. A LV-SAU hosts the necessary databases and the set of algorithms responsible for monitoring, control and protection of the LV grid.

For monitoring the LV grid, the SAU runs the SE algorithm to estimate the state of the grid in real time with SM and PMU measurements as inputs. SM and the PMU measurements are stored periodically in the MDMS and PDC respectively. The SE retrieves these measurements periodically from the databases to estimate the state of the grid. Furthermore, it retrieves the most updated topology of the grid and the electrical line parameters of the grid for the state estimation. Each of the LV-SAU then

updates the MV-SAU with the latest state estimate of its individual LV grid. The MV-SAU processes the state estimates of the individual LV grids in order to evaluate the state of the MV grid considering the network topology, the electrical line parameters and measurements collected from the measurement devices connected to the MV grid.

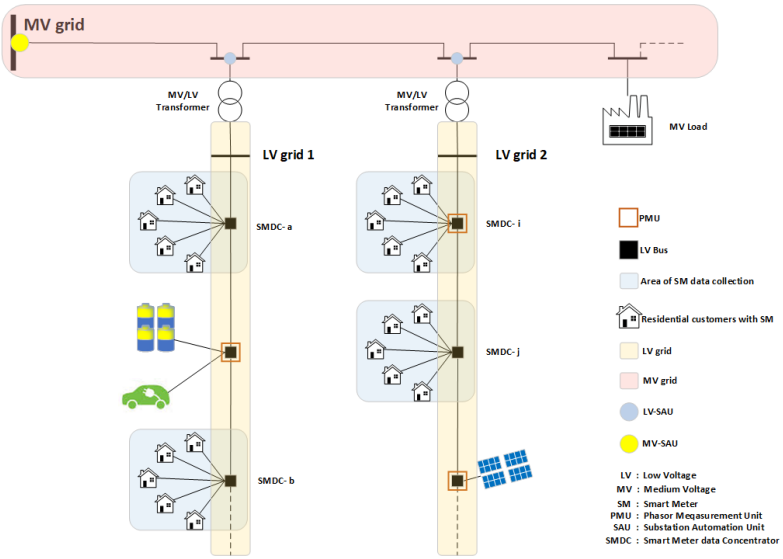


Figure 2.11: Exemplary distribution grid

The detailed flow of measurement data for real time monitoring of a single MV grid (with both MV and LV grid sections) is depicted in Fig. 2.12, which follows the IDE4L automation architecture [Rep+17]. A Smart Meter Data Concentrator (SMDC) collects SM data from the designated set of smart meters installed at the residential customers of a specific locality. It then forwards the smart meter data to the MDMS. The MDMS is the repository of measurements from all SMs. Typically, in most of the current installations of SM data collection system involving SMDC, the Power Line Communication (PLC) is utilized [Gar15]. Furthermore, cellular communication systems like the GPRS or LTE is used for the communication between the SMDC and the MDMS. In this specific study the MDMS (also PDC) is considered to be hosted by the LV-SAU, but it can be also deployed in a dedicated server to which the LV-SAU has network access.

In case of PMU measurement acquisition, as shown in Fig. 2.12, the PMUs send the measurements to the PDC via series of Ethernet and fibre optic router/switches. The measurements with their time tags are stored in their respective repositories. The SE algorithm hosted by LV-SAU periodically retrieves the latest SM and PMU measurements from the repositories via appropriate data fetching commands and estimates the state of the LV grid. In addition to the measurement repositories (MDMS and PDC) the LV-SAU also hosts the repository containing Network Infrastructure System (NIS). NIS typically has the data about the grid topology, line parameters and other electric component operational parameters like the winding ratio of transformers, circuit breaker/ switch positions and so on.

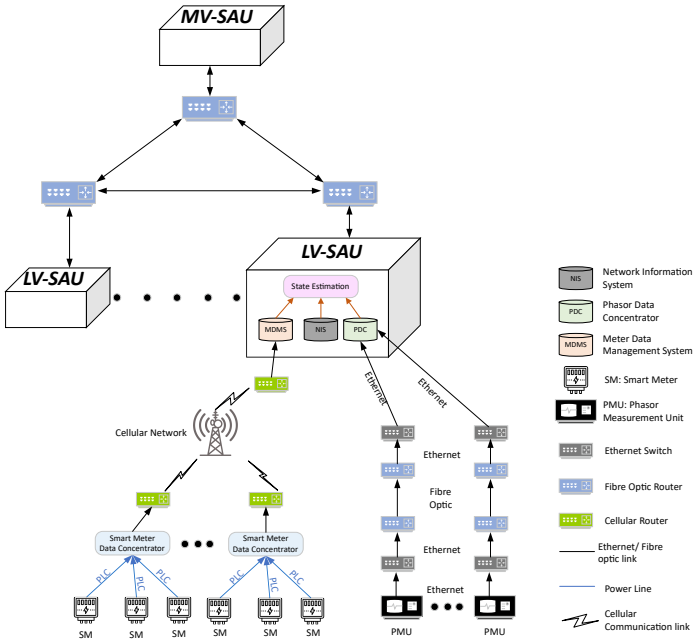


Figure 2.12: Data flow for real time monitoring of distribution grid with IDE4L automation architecture

The estimated states of the individual LV grid done by their respective LV-SAU is then forwarded to the MV-SAU via the fibre optic network. It then estimates the state of the whole MV grid considering the estimates

from the individual LV-SAUs and additional measurements sent from the MV/LV substations where the LV-SAU is hosted.

In this test case a single SMDC is configured to collect data from ten SMs and there are three SMDCs per LV grid. Additionally it is assumed that three low cost PMUs are installed for every LV grid. Furthermore, it is assumed that all measurements from SMs and PMUs are corresponding to the voltages at different locations of the LV grid. The accuracy class of the SM and PMU is assumed to be of class 2.0 and class 0.2 as per the IEC 62053-22:2003 and IEEE C.37.118.1:2018 respectively. Furthermore, it is also assumed that at least five smart meter measurements are required from each SMDC and at least one PMU measurement for ensuring the observability of each LV grid. For monitoring the MV grid, the complete state estimates from each LV-SAU are required for ensuring observability of the complete MV grid. It should be noted that the number of measurement devices assumed to be deployed in the distribution grid is not realistic in the current state of distribution grid automation. In some European countries like Italy massive deployment of SMs that can communicate over PLC [Gar15] has been done. Whereas, in Germany lower number of SM would be deployed as selected residential sites based on the average energy consumption, production and feasibility of installing additional communication interfaces [Gmb]. Similarly, deployment of the PMUs is considering a futuristic distribution grid where there is a requirement of synchronized measurement within a distribution grid for better monitoring and control of it. So the number of SMs and PMUs assumed are purely for demonstrating the applicability of the proposed method for the reliability analysis of distribution grid monitoring systems and further derive its statistical performance.

Detailed division of the monitoring system into individual functional blocks, their failure models and the evaluation of the over all reliability of the monitoring system using CTMC and MDRM would be presented in the upcoming subsections.

2.5.3 Functional blocks

The five functional blocks that are collectively responsible for realising the real time monitoring of distribution grids is as shown in Fig. 2.13. The SMs and the PLC infrastructure form the Functional Block 1(FB1). The main function of the FB1 is to facilitate the SM measurements to the SMDC using the PLC infrastructure. Therefore the reliability of the FB1 is only dependent on the reliability of the individual SM and the reliability of the PLC infrastructure used to deliver the SM data to a specific SMDC. It is worth to note that, one FB1 corresponds to the delivery of a specific

SMDC, but in a LV grid there could be multiple SMDCs deployed to collect SM data from different parts of the LVgrid. Therefore, the number of instances of FB1 would be equal to the number of SMDCs deployed in the grid. The reliability of each instance of FB1 my be identical or dissimilar to other instances of the FB1 depending upon the type of the SMs, PLC modems and electrical power line type and lengths used to transfer the data between the PLC modems deployed.

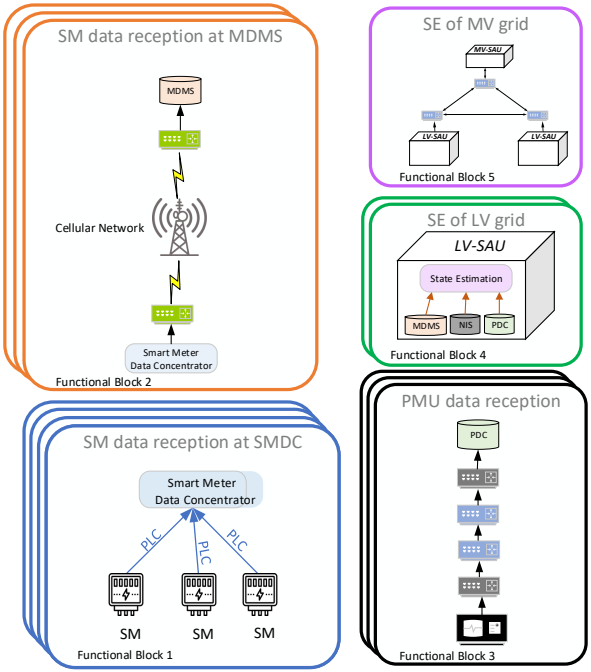


Figure 2.13: Functional blocks of real time monitoring of distribution grids

The FB2 is responsible for delivering the processed SM data from the SMDC to the MDMS. The reliability of the FB2 is determined by the reliability of the SMDC and the cellular communication infrastructure. The number of instances of FB2 correspond to the number of SMDCs deployed in each MV grid. The FB3 is responsible to deliver the PMU data to the PDC via the communication infrastructure involving Ethernet

and FO router and switches. Therefore, the reliability of FB3 is solely governed by the reliability of the PMU devices, Ethernet switches/routers, FO switches and failures of the physical medium that connects the different switches/routers. Similar to the FB1, there could be multiple instances of FB3, where the number corresponds to the number of the PMUs deployed in each LV grid. The FB4 is responsible for estimating the state of a specific LV grid. It should be noted that in this functional block the LV-SAU and servers hosting MDMS, NIS and PDC are involved. In this study, it is assumed that the MDMS, NIS and PDC are hosted by the computational resource that hosts also the grid management functions of the LV-SAU. Therefore, the reliability of the FB4 is dependent on the reliability of LV-SAU and the software that help in successfully realising all intended functions of LV-SAU. Finally, the FB5 is responsible to collect the information sent by the LV-SAUs and process them to estimate the state of the complete MV grid. The reliability of this FB is dependent on the reliability of the communication channel used by the LV-SAUs to report the state estimates of its LV grid to the MV-SAU and the reliability of the MV-SAU device.

2.5.4 Failure modes of the functional blocks

Once the functional blocks have been defined, the next step is to model the failure characteristics of each functional block. In this section the detailed failure models of each functional block is presented.

Failure modes of FB1: SM data reception at SMDC

In this study each SMDC is responsible to collect the data from 10 SM via the PLC infrastructure. The failure of FB1 is caused either by the failure of the SM or the PLC infrastructure. Firstly, the failure mode of the SM would be described followed by that of the PLC infrastructure.

The failure of the SM is caused either by the failure of its constituting hardware or the software components. In this study, the smart meter gateway which is responsible for ensuring cyber security of the SM and hosts software for communication protocol translation, is considered as an integral part of the SM. From now on the SM would be the composite system of the physical smart meter and the smart meter gateway. The hardware components of i^{th} SM and their associated failure rate and mean recovery times are as follows.

- Power supply with failure rate λ^i_{PS} and recovery time r^i_{PS}.

- Transducer measuring voltage/current/energy with failure rate λ_T^i and recovery time r_T^i.
- Transducer output signal processing board with failure rate λ_{SP}^i and recovery time r_{SP}^i.
- Processing board with failure rate λ_{PB}^i and recovery time r_{PB}^i.
- Data storage with failure rate λ_{DS}^i and recovery time r_{DS}^i.
- Communication interface with failure rate λ_{CM}^i and recovery time r_{CM}^i.

The software component of the SM and their associated failure and the mean recovery times are as follows.

- Firmware with failure rate λ_{FW}^i and recovery time r_{FW}^i.
- Measurement calculation from Transducer data with failure rate λ_M^i and recovery time r_M^i.
- Communication protocol translator with failure rate λ_{CM-PR}^i and recovery time r_{CM-PR}^i.

The failure of an individual component is a random event. Since the component failure time is assumed to have an exponential Probability Density Function (PDF), the failure rate of the subsystem (λ_i^{SM}) can be calculated as a function of the individual component failure rates as given in Eq. (2.33), based on the approximation of equivalent reliability of a systems with independently repairable components in series as explained in [BA92].

$$\lambda_{SM}^i = \lambda_{PS}^i + \lambda_T^i + \lambda_{SP}^i + \lambda_{PB}^i + \lambda_{DS}^i + \lambda_{CM}^i + \lambda_{FW}^i + \lambda_M^i + \lambda_{CM-PR}^i \quad (2.33)$$

Similarly, the mean repair time of the SM can also be approximated as given in Eq. (2.34), where r_{SM-HW}^i and r_{SM-SW}^i correspond to the contribution of the repair time of the hardware and software components of the i^{th} SM respectively [BA92].

$$\begin{aligned} & r_{SM}^i \simeq \frac{r_{SM-HW}^i + r_{SM-SW}^i}{\lambda_{SM}^i} \\ & \textit{where} \\ & r_{SM-HW} \simeq \lambda_{PS}^i * r_{PS}^i + \lambda_T^i * r_T^i + \lambda_{SP}^i * r_{SP}^i \\ & + \lambda_{PB}^i * r_{PB}^i + \lambda_{DS}^i * r_{DS}^i + \lambda_{CM}^i * r_{CM}^i \\ & r_{SM-SW} \simeq \lambda_{FW}^i * r_{FW}^i + \lambda_M^i * r_M^i + \lambda_{CM-PR}^i * r_{CM-PR}^i \end{aligned} \quad (2.34)$$

An exemplary configuration of the PLC infrastructure to collect the measurement data from 10 SMs by the SMDC is shown in Fig. 2.14.

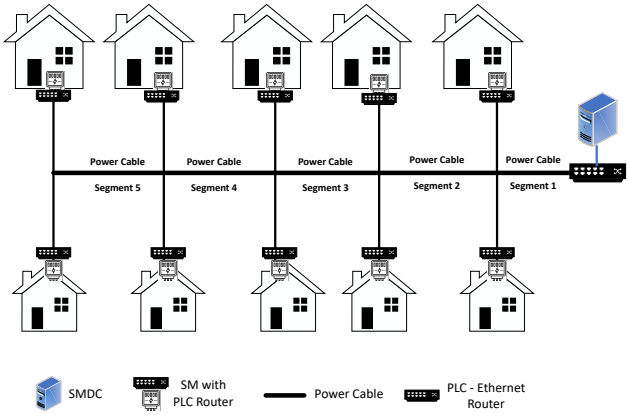


Figure 2.14: Configuration of PLC infrastructure for SM data aggregation by SMDC

Each of the smart meter sends the measurement data via Ethernet to the PLC modem which then forwards to the PLC modem connected to the SMDC via the power line. The reception failure of the data sent from i^{th} SM is caused by any of the following failures.

- Failure PLC modem connected to the i^{th} SM.
- Failure of any of the upstream power cable segments connecting the PLC modem of the SM and SMDC.
- Failure of PLC modem connected to the SMDC.

The failure rate and the mean recovery times of the components of the PLC infrastructure is as follows.

- PLC modem connected to the i^{th} SM with Failure rate λ^{i}_{PLC-SM} and recovery time r^{i}_{PLC-SM}.
- PLC modem connected to the SMDC with Failure rate $\lambda_{PLC-SMDC}$ and recovery time $r_{PLC-SMDC}$.
- Individual power cable segment with Failure rate $\lambda^{i}_{PWR-CBL}$ and recovery time $r^{i}_{PWR-CBL}$.

The equivalent failure rate of data transmission from the i^{th} SM to the SMDC (λ^i_{DT-PLC}) is given as per Eq. (2.35), where n corresponds to the number of power cable segments between the PLC modem connected to the SM and the one connected to the SMDC. The power cable connecting the houses to the main LV power cable is considered to have negligible failure rate and hence not considered in this analysis.

$$\lambda^i_{DT-PLC} = \lambda^i_{PLC-SM} + \sum_{i=1}^{n} \lambda^i_{PWR-CBL} + \lambda_{PLC-SMDC} \tag{2.35}$$

Similarly the mean repair time of a i^{th} data transmission link provided by the PLC infrastructure can be approximated as shown in Eq. (2.36). This approximation is valid for systems where its constituting components with very low γ where γ is the scalar product of their failure rate and repair time [BA92].

$$\begin{aligned} r^i_{DT-PLC} \simeq & \frac{\lambda^i_{PLC-SM} * r^i_{PLC-SM}}{\lambda^i_{DT-PLC}} \\ & + \frac{\sum_{i=1}^{n} \lambda^i_{PWR-CBL} * r^i_{PWR-CBL}}{\lambda^i_{DT-PLC}} \\ & + \frac{\lambda_{PLC-SMDC} * r_{PLC-SMDC}}{\lambda^i_{DT-PLC}} \end{aligned} \tag{2.36}$$

Failure modes of FB2 : SM data reception at MDMS

Once the SM data reaches the PLC modem connected to the SMDC, it forwards the data to the communication port of the SMDC (typically via Ethernet). The SMDC processes the data and then sends aggregated SM data to the MDMS via the cellular infrastructure. A modem provides the SMDC an interface to the cellular infrastructure. Similarly, a modem of the same kind provides interface for the MDMS to the cellular infrastructure.

The failure of the data reception at the MDMS would be caused either by the failure of the SMDC or the failure of any component involved in the communication of the data (modems or the components of the cellular infrastructure). The failure of the SMDC can be caused either by the failure of its hardware components or the software/firmware. Its major hardware components would be the power supply, communication interface, the processing board and the memory/data storage unit with a failure rate of $\lambda_{SMDC-PS}$, $\lambda_{SMDC-COM}$, $\lambda_{SMDC-PB}$ and $\lambda_{SMDC-DS}$ respectively and and mean repair time of $r_{SMDC-PS}$, $r_{SMDC-COM}$, $r_{SMDC-PB}$ and

$r_{SMDC-DS}$ respectively. The major software components of the SMDC would be the firmware, the data storage management system and the algorithms processing the individual SM data with a failure rate of $\lambda_{SMDC-FW}$, $\lambda_{SMDC-DB}$ and $\lambda_{SMDC-DA}$ and repair time of $r_{SMDC-FW}$, $r_{SMDC-DB}$ and $r_{SMDC-DA}$ respectively

Given the failure rate and the mean repair times of the hardware and software components, the equivalent failure rate and mean repair time of the i^{the} SMDC can be calculated as per Eq. (2.37) and Eq. (2.38) respectively [BA92].

$$\begin{aligned}\lambda^i_{SMDC} =& \lambda_{SMDC-PS} + \lambda^i_{SMDC-COM} + \lambda^i_{SMDC-PB} \\ &+ \lambda^i_{SMDC-DS} + \lambda_{SMDC-FW} \\ &+ \lambda_{SMDC-DB} + \lambda_{SMDC-DA}\end{aligned} \tag{2.37}$$

$$\begin{aligned}r^i_{SMDC} \simeq& \frac{r^i_{SMDC-HW} + r^i_{SMDC-SW}}{\lambda^i_{SMDC}} \\ &where \\ r_{SMDC-HW} \simeq& \lambda^i_{SMDC-PS} * r^i_{SMDC-PS} \\ &+ \lambda^i_{SMDC-COM} * r^i_{SMDC-COM} \\ &+ \lambda^i_{SMDC-PB} * r^i_{SMDC-PB} \\ &+ \lambda^i_{SMDC-DS} * r^i_{SMDC-DS} \\ r_{SMDC-SW} \simeq& \lambda^i_{SMDC-FW} * r^i_{SMDC-FW} + \lambda^i_{SMDC-DB} * r^i_{SMDC-DB} \\ &+ \lambda^i_{SMDC-DA} * r^i_{SMDC-DA}\end{aligned} \tag{2.38}$$

The failure of the modem can either be caused by the power supply failure, a hardware failure software failure. given the hardware and software failure rates as $\lambda_{M-CEL-PS}$, $\lambda_{M-CEL-HW}$, $\lambda_{M-CEL-SW}$ and repair rates as $r_{M-CEL-PS}$, $r_{M-CEL-HW}$, $r_{M-CEL-SW}$ respectively. The overall failure rate and repair time of the i^{th} cellular modem can be calculated as per Eq. (2.39) and Eq. (2.40) respectively [BA92].

$$\lambda^i_{M-CEL} = \lambda^i_{M-CEL-HW} + \lambda^i_{M-CEL-SW} + \lambda^i_{M-CEL-PS} \tag{2.39}$$

$$r^i_{M-CEL} \simeq \frac{\lambda^i_{M-CEL-PS} * r^i_{M-CEL-PS}}{\lambda^i_{M-CEL}} + \frac{\lambda^i_{M-CEL-HW} * r^i_{M-CEL-HW}}{\lambda^i_{M-CEL}} + \frac{\lambda^i_{M-CEL-SW} * r^i_{M-CEL-SW}}{\lambda^i_{M-CEL}} \tag{2.40}$$

A cellular communication infrastructure is a network of radio transciever base stations, that provide wireless link access to the cellular user equipment and manage their data flow. Typically a single radio transciever station is responsible for designated land areas called cells. Any cellular infrastructure (may it be GSM/UMTS/LTE or 5G) have the following basic components.

- Radio access network
- Core network

However, over the years with the advancement in signal processing, data processing and storage and in cloud based computational technology, the aforementioned four basic components of the cellular infrastructure have also evolved. The connections between the different components, their assigned roles and functions have also evolved thus enabling the development of the cellular infrastructure from GSM to 5G.

In this study the LTE(4G) is considered to be used as the cellular network for transmitting the data from the SMDC to MDMS. A short description of the components of the LTE architecture and their configuration is provided. Furthermore, failure rate (λ_{CEL}) and the repair time (r_{CEL}) of the LTE infrastructure as a function of the failure rates and repair times of its constituting components and their configuration would be explained subsequently in this section.

LTE stands for Long Term Evolution. The main drivers for its development were to enable increased volumes of data traffic, to reduce latency and to provide a packet optimised radio access network. LTE includes advanced technologies such as OFDMA (Orthogonal Frequency Division Multiple Access) and MIMO (Multiple Input Multiple Output). Since the first release of the LTE standards; release 8, the standard has been continuously evolving to further enhance system capacity. These releases further improve system capacity to extend the applicability of LTE for the use cases of smart grid applications, industrial automation and intelligent transportation systems.

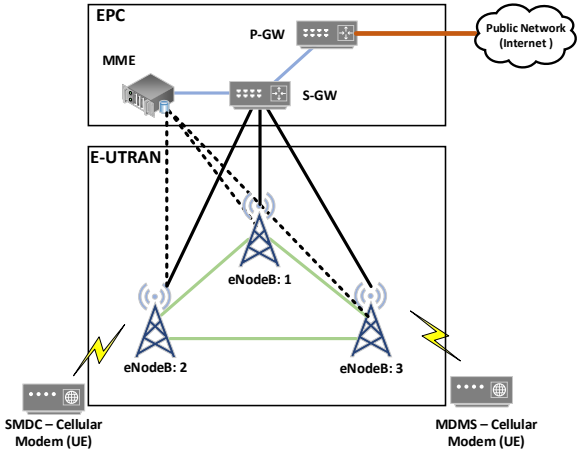


Figure 2.15: Overview of LTE architecture

The overall system architecture for LTE, as defined by 3GPP, including the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and enhanced core network known as the Evolved Packet Core (EPC) is as shown in Fig. 2.15. The UE is the User Equipment. Typically the UEs are the mobile devices that use the cellular network. However, in this study the UEs are the modems that provide cellular interface to the SMDC and MDMS. The dotted black lines correspond to the fibre optic connections to the MME from each eNodeB and the solid line correspond to the fibre optic connections to the S-GW from each eNodeB. The green lines correspond to the google X2 interface between the different gNodeBs for optimal resource allocation and data flow management between the different cells and also to the EPC. The components of the EPC namely the Mobility Management Entity (MME), The Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW) communicate with each other through Ethernet switches denoted by blue lines.

For the study an E-UTRAN with 3 eNodeBs are considered, where the cellular modem connected to SMDC (SMDC cellular modem) can be served by either eNodeB:2 or eNodeB:1 and the cellular modem connected to MDMS (MDMS cellular modem) is served by eNodeB:3 or eNodeB:1. Therefore, for successful transmission of the data between the SMDC and MDMS either just the eNodeB:1 should be functional or any two eNodeBs

or all of the eNodeBs should be functional. Additionally, the EPC and the corresponding communication links between eNodeBs and the components of EPC should be functional. A detailed CTMC model of the data link failure over the LTE infrastructure including the different redundant paths would be presented in the subsequent subsections. In this section the failure rate and repair time of each component of the E-UTRAN and EPC would be presented.

The E-UTRAN is the air interface of LTE and constitutes the access part of the Evolved Packet System (EPS). E-UTRAN network side is composed only of base station called eNodeB which are equipped with all radio interface-related functions. The actual deployment of the eNodeB consists of two parts, the Radio Remote Control (RRU) and the Base Band processing Unit (BBU). The BBU and RRU have a common power supply. The RRU is connected to the BBU via the Common Public Radio Interface (CPRI) cable. The BBU of the base station is the part that processes the original base band signal for physical interface. It is connected with the Radio Remote control Unit (RRU) on the radio mast via optical fibre. The BBU comprises a CPU, a signal processing unit and its own firmware. The failure rate (λ^i_{BBU}) and the repair time (r^i_{BBU}) of the BBU of i^{th} eNodeB can be calculated as per Eq. (2.41) and Eq. (2.42) according to the law of series system [BA92] respectively. Where $\lambda^i_{BBU-CPU}$, λ^i_{BBU-SP}, λ^i_{BBU-FW} correspond to failure rate of cpu, signal processing unit firmware of BBU respectively and $r^i_{BBU-CPU}$, r^i_{BBU-SP}, r^i_{BBU-FW} correspond to mean repair time of cpu, signal processing unit firmware of BBU respectively.

$$\lambda^i_{BBU} = \lambda^i_{BBU-CPU} + \lambda^i_{BBU-SP} + \lambda^i_{BBU-FW} \tag{2.41}$$

$$\begin{aligned} r^i_{BBU} \simeq & \frac{\lambda^i_{BBU-CPU} * r^i_{BBU-CPU} + \lambda^i_{BBU-SP} * r^i_{BBU-SP}}{\lambda^i_{BBU}} \\ & + \frac{\lambda^i_{BBU-FW} * r^i_{BBU-FW}}{\lambda^i_{BBU}} \end{aligned} \tag{2.42}$$

The RRU is the radio frequency processing part of the eNodeB. It comprises a frequency converter and a A/D-D/A-converter and its firmware.The failure rate (λ^i_{RRU}) and the repair time (r^i_{RRU}) of the RRU of i^{th} eNodeB can be calculated as per Eq. (2.43) and Eq. (2.44) according to the law of of series systems explained in [BA92]. Where λ^i_{RRU-FC}, λ^i_{RRU-AD}, λ^i_{RRU-FW} correspond to failure rate of frequency converter, A/D-D/A-converter and firmware of RRU respectively and r^i_{RRU-FC}, r^i_{RRU-AD},

r^i_{RRU-FW} correspond to mean repair time of cpu, signal processing unit firmware of RRU respectively.

$$\lambda^i_{RRU} = \lambda^i_{RRU-FC} + \lambda^i_{RRU-AD} + \lambda^i_{RRU-FW} \tag{2.43}$$

$$\begin{aligned} r^i_{RRU} \simeq & \frac{\lambda^i_{RRU-FC} * r^i_{RRU-FC} + \lambda^i_{RRU-AD} * r^i_{RRU-AD}}{\lambda^i_{RRU}} \\ & + \frac{\lambda^i_{RRU-FW} * r^i_{RRU-FW}}{\lambda^i_{RRU}} \end{aligned} \tag{2.44}$$

The failure of the E-UTRAN is caused by failure of the RRU or the BBU or the power supply providing power to both of them or the failure of the optic fibre connecting them. The failure rate of i^{th} eNodeB can be calculated as function of the failure rate of RRU (λ^i_{RRU}), failure rate of BBU (λ^i_{BBU}), failure rate of power supply ($\lambda^i_{eNodeB-PS}$) and fibre optic link between the BBU and RRU ($\lambda^i_{RRU-BBU-FO}$) as shown in Eq. (2.45) .

$$\lambda^i_{eNB} = \lambda^i_{RRU} + \lambda^i_{BBU} + \lambda^i_{eNodeB-PS} \tag{2.45}$$

The repair time of i^{th} eNodeB can then be approximated, for series system [BA92], based on the repair time of RRU (r^i_{RRU}), repair time of BBU (r^i_{BBU}) , repair time of power supply ($r^i_{eNodeB-PS}$) and and fibre optic link between the BBU and RRU ($r^i_{RRU-BBU-FO}$) as shown in Eq. (2.46) .

$$\begin{aligned} r^i_{eNB} \simeq & \frac{\lambda^i_{RRU} * r^i_{RRU} + \lambda^i_{BBU} * r^i_{BBU} + \lambda^i_{eNodeB-PS} * r^i_{eNodeB-PS}}{\lambda^i_{eNB}} \\ & + \frac{\lambda^i_{RRU-BBU-FO} * r^i_{RRU-BBU-FO}}{\lambda^i_{eNB}} \end{aligned} \tag{2.46}$$

The EPC is responsible for authentication and charging functionalities and it provides the setup of end to end connections. The EPC network architecture supports the E-UTRAN through a reduction in the number of network elements, simpler functionality and improved redundancy. The main components that exist in a typical EPC are:

- The Mobility Management Entity (MME): The MME is the key control-node for the LTE access-network controlling the high-level operation by means of signalling messages. It is responsible for user authentication and for regulating security parameters. Through logging into the MME, we can view the status of the devices logged

onto the core networks. It is hosted by a local server with its own firmware which have a failure rate λ_{MME-HW}, λ_{MME-FW} and repair time of r_{MME-HW}, r_{MME-FW} respectively. Therefore its equivalent failure rate can be calculated as in Eq. (2.47) and its mean repair time as in Eq. (2.48) based on the law for a system with components in series [BA92].

$$\lambda_{MME} = \lambda_{MME-HW} + \lambda_{MME-FW} \tag{2.47}$$

$$r_{MME} \simeq \frac{\lambda_{MME-HW} * r_{MME-HW} + \lambda_{MME-FW} * r_{MME-FW}}{\lambda_{MME}} \tag{2.48}$$

- The Serving Gateway (S-GW): The S-GW routes and forwards user data packets. It is the node that terminates the interface towards E-UTRAN and acts as the mobility anchor for the user plane during inter-eNodeB handovers and for compatibility between LTE and other 3GPP technologies.It is hosted by a local server with its own firmware which have a failure rate λ_{SGW-HW}, λ_{SGW-FW} and repair time of r_{SGW-HW}, r_{SGW-FW} respectively. Therefore its equivalent failure rate can be calculated as in Eq. (2.49) and its mean repair time as in Eq. (2.50) based on the law for a system with components in series [BA92].

$$\lambda_{SGW} = \lambda_{SGW-HW} + \lambda_{SGW-FW} \tag{2.49}$$

$$r_{SGW} \simeq \frac{\lambda_{SGW-HW} * r_{SGW-HW} + \lambda_{SGW-FW} * r_{SGW-FW}}{\lambda_{SGW}} \tag{2.50}$$

- The Packet Data Network Gateway (P-GW): The P-GW provides connectivity to the UE to external Packet Data Networks (PDNs) using the SGi interface. It is hosted by a local server with its own firmware which have a failure rate λ_{PGW-HW}, λ_{PGW-FW} and repair time of r_{PGW-HW}, r_{PGW-FW} respectively. Therefore its equivalent failure rate can be calculated as in Eq. (2.51) and its mean repair time as in Eq. (2.52) based on the law for a system with components in series [BA92].

$$\lambda_{PGW} = \lambda_{PGW-HW} + \lambda_{PGW-FW} \tag{2.51}$$

$$r_{PGW} \simeq \frac{\lambda_{PGW-HW} * r_{PGW-HW} + \lambda_{PGW-FW} * r_{PGW-FW}}{\lambda_{PGW}} \tag{2.52}$$

- EPC network switches : These switches7routers enable the communication between the MME, SGW and PGW, which have a failure rate λ_{EPC-SW} and repair time of r_{EPC-SW} respectively.

The equivalent failure rate and the mean repair time of the EPC can be calculated as in Eq. (2.53) and Eq. (2.54) based on the law for a system with components in series [BA92] respectively. Where n is the number of switches connecting the MME, S-GW and P-GW and the power supply of the EPC. Where the λ_{EPC-PS} and r_{EPC-PS} represent the failure rate and repair time of the power supply that provides the power to all components of the EPC.

$$\lambda_{EPC} = \lambda_{SGW} + \lambda_{PGW} + \lambda_{MME} + \lambda_{EPC-PS} + \sum_{k=1}^{n} \lambda_{EPC-SW} \tag{2.53}$$

$$\begin{aligned} r_{EPC} \simeq & \frac{\lambda_{SGW} * r_{SGW} + \lambda_{PGW} * r_{PGW} + \lambda_{MME} * r_{MME}}{\lambda_{EPC}} \\ & + \frac{\sum_{k=1}^{n} \lambda_{EPC-SW} * r_{EPC-SW} + \lambda_{EPC-PS} * r_{EPC-PS}}{\lambda_{EPC}} \end{aligned} \tag{2.54}$$

The failure rate and repair time calculated of the eNodeBs and the EPC would be used to build the complex CTMC failure model of the data transfer between a single SMDC and the MDMS in the Sect. 2.5.5.

Failure modes of FB3: PMU data reception by PDC

The FB3 corresponds to the data reception of a single PMU at the PDC. Therefore, its failure is either caused by the failure of PMU or the failure of communication channel used to send the synchrophasors. The equivalent failure rate and repair time of a single PMU and of the communication channel as a function of the failure rate and repair times of their constituting components is presented in this section.

The major components of the PMU are shown in Fig. 2.16. The analog signals from the transducer corresponding either to current or voltage measurement is filtered with an anti-aliasing filter after which its is digitized by the A/D converter. The sampling of the signal is done based on the

trigger impulses from the Phase Locked Loop (PLL) oscillator. The PLL is continuously synchronised by either of the two time synchronization systems. One of them is through the GPS unit that uses the 1PPS or IRIG-B signal to synchronize the PLL. The other is through the 1588 Precision Time Protocol (PTP) master that synchronises its slaves via Ethernet. The 1588 PTP slave of the PMU then internally synchronizes the PLL. In this study the GPS based synchronization is considered as the primary source of synchronization and the PTP based one as the auxiliary source of synchronization. The time stamped samples are provided to the processor that calculates the synchrophasor and publishes through its dedicated Ethernet port. The failure of the PMU can be caused by the failure of its constituting components.

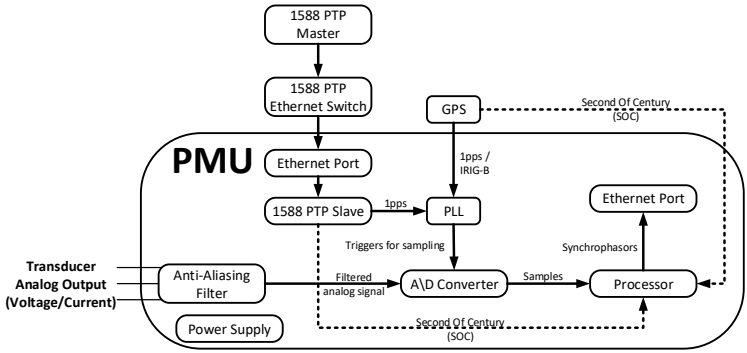


Figure 2.16: Components of a PMU with redundant time synchronization system

Primarily the PMU has the following components:

- Power supply with a failure rate of λ_{PMU-PS} and repair time of r_{PMU-PS}.
- Anti-aliasing filter with a failure rate of $\lambda_{PMU-AAF}$ and repair time of $r_{PMU-AAF}$.
- Analog to digital converter (A/D Converter) with a failure rate of $\lambda_{PMU-ADC}$ and a repair time of $r_{PMU-ADC}$.
- Processor with a failure rate of the λ_{PMU-P} and repair time of r_{PMU-P}.

- Ethernet port for publising the synchrophasor with a failure rate $\lambda_{PMU-Eth}$ and repair time of $r_{PMU-Eth}$.
- PLL with a failure rate of $\lambda_{PMU-PLL}$ and a repair rate of $r_{PMU-PLL}$.
- Time synchronization system with a failure rate of $\lambda_{PMU-SYNC}$ and a repair time of $r_{PMU-SYNC}$.

  It should be noted that, the PMU considered in this study has two sources of synchronization, namely through the GPS or through the Ethernet based 1588 PTP. Each of these two systems functions as redundant to each other. Therefore, these two systems form a parallel system where even when one of the synchronization system fails the other will still provide the synchronization signals to the PMU. The time synchronization fails only when both of the individual time synchronization systems fail completely. The failure rate of the PMU($\lambda_{PMU-SYNC}$) and its repair time ($r_{PMU-SYNC}$) can be calculated as a function of failure rate of GPS system and PTP system $\lambda_{PMU-GPS}$, $\lambda_{PMU-PTP}$ respectively and their repair times of $r_{PMU-GPS}$, $r_{PMU-PTP}$ respectively as per Eq. (2.55) and Eq. (2.56) respectively. An approximation of the parallel systems as explained in [BA92], is used to calculate the failure rate of the time synchronization system of the PMU .

$$\lambda_{PMU-SYNC} \simeq \lambda_{PMU-GPS} * \lambda_{PMU-PTP}(r_{PMU-GPS} + r_{PMU-PTP}) \tag{2.55}$$

$$r_{PMU-SYNC} = \frac{r_{PMU-GPS} * r_{PMU-PTP}}{r_{PMU-GPS} + r_{PMU-PTP}} \tag{2.56}$$

The failure rate ($\lambda_{PMU-GPS}$) and the repair time ($r_{PMU-GPS}$) of the GPS system can be derived as a function of the failure rate of the GPS ($\lambda_{GPS-Unit}$) unit and the fibre optic link (λ_{GPS-FO}) connecting GPS unit and the PMU as shown in Eq. (2.57). The repair time of the GPS base time synchronization system is calculated considering the GPS and the fibre optic to form a series system and hence the approximation of the series system as explained in [BA92] is used to calculate it and is shown in Eq. (2.58) with the repair time of GPS and the fibre optic link as $r_{GPS-Unit}$ and r_{GPS-FO} respectively.

$$\lambda_{PMU-GPS} = \lambda_{GPS-Unit} + \lambda_{GPS-FO} \tag{2.57}$$

$$r_{PMU-GPS} \simeq \frac{\lambda_{GPS-Unit} * r_{GPS-Unit} + \lambda_{GPS-FO} * r_{GPS-FO}}{\lambda_{PMU-GPS}} \tag{2.58}$$

The failure rate and the repair time of the 1588 PTP based synchronization system is a series system with the PTP Master, PTP supporting network switches, Ethernet port of the PMU and the PTP slave hosted in the PMU. Therefore the effective failure rate of the PTP based time synchronization system can be calculated as given in Eq. (2.59). Where λ_{PTP-MS}, λ_{PTP-SL}, λ^{i}_{PTP-SW} $\lambda_{PMU-PTP-Eth}$ correspond to the failure rate of PTP Master, PTP Slave, i^{th} Ethernet switch (in a string of n Ethernet switches) supporting PTP and the Ethernet port of the PMU that is configured to receive PTP messages.

$$\begin{aligned}\lambda_{PMU-PTP} =& \lambda_{PTP-MS} + \lambda_{PTP-SL} + \sum_{i=1}^{n} \lambda^{i}_{PTP-SW} \\ &+ \lambda_{PMU-PTP-Eth}\end{aligned} \tag{2.59}$$

Whereas its repair time can be approximated as per the Eq. (2.60), considering it as a series system as explained in [BA92]. where r_{PTP-MS}, r_{PTP-SL}, r^{i}_{PTP-SW} $r_{PMU-PTP-Eth}$ correspond to the repair time of PTP Master, PTP Slave, i^{th} Ethernet switch (in a string of n Ethernet switches) supporting PTP and the Ethernet port of the PMU that is configured to receive PTP messages.

$$\begin{aligned}r_{PMU-PTP} \simeq & \frac{\lambda_{PTP-MS} * r_{PTP-MS} + \lambda_{PTP-SL} * r_{PTP-SL}}{\lambda_{PMU-GPS}} \\ &+ \frac{\lambda_{PMU-PTP-Eth} * r_{PMU-PTP-Eth}}{\lambda_{PMU-PTP}} \\ &+ \frac{\sum_{i=1}^{n} \lambda_{PTP-SW} * r_{PTP-SW}}{\lambda_{PMU-PTP}}\end{aligned} \tag{2.60}$$

- Firmware of the PMU with a failure rate of λ_{PMU-FW} and repair time of r_{PMU-FW}

The equivalent failure rate of the PMU can be derived considering that its constituting components form a series system, where even failure of a single component reaults in the failure of the PMU. The equivalent failure

rate and the approximated repair time of the PMU can then be derived as per the Eq. (2.61) and Eq. (2.62) respectively.

$$\begin{aligned}\lambda_{PMU} =& \lambda_{PMU-PS} + \lambda_{PMU-AAF} + \lambda_{PMU-ADC} + \lambda_{PMU-P} \\ &+ \lambda_{PMU-PLL} + \lambda_{PMU-SYNC} + \lambda_{PMU-FW}\end{aligned} \tag{2.61}$$

$$\begin{aligned}r_{PMU} \simeq & \frac{\lambda_{PMU-PS} * r_{PMU-PS} + \lambda_{PMU-AAF} * r_{PMU-AAF}}{\lambda_{PMU}} \\ &+ \frac{\lambda_{PMU-ADC} * r_{PMU-ADC}}{\lambda_{PMU}} \\ &+ \frac{\lambda_{PMU-P} * r_{PMU-P} + \lambda_{PMU-PLL} * r_{PMU-PLL}}{\lambda_{PMU}} \\ &+ \frac{\lambda_{PMU-SYNC} * r_{PMU-SYNC} + \lambda_{PMU-FW} * r_{PMU-FW}}{\lambda_{PMU}}\end{aligned} \tag{2.62}$$

The synchrophasor data from each PMU are delivered to the PDC through a communication channel that is composed of a set switches, routers, modems and physical medium connecting them. Therefore the failure of the communication channel can be caused by the failure of any switching/routing devices or the physical mediums connecting them. Therefore, the failure rate of the communication channel used by a PMU is given by Eq. (2.63)

$$\lambda_{PMU-CC} = \sum_{j=1}^{r} \lambda_j^R + \sum_{k=1}^{m} \lambda_k^M + \sum_{u=1}^{s} \lambda_u^S + \sum_{l=1}^{q} \lambda_l^{PM} \tag{2.63}$$

where λ_j^R,λ_k^M, λ_u^S and λ_l^{PM} correspond to the failure of j^{th} relaying component,k^{th} modem, s^{th} switch and l^{th} physical medium link respectively. The repair time of the communication channel considering the repair times of its individual components can be calculated as Eq. (2.64). Where r_j^R,r_k^M, r_u^S and r_l^{PM} correspond to the repair time of j^{th} relaying component,k^{th} modem, s^{th} switch and l^{th} physical medium link respectively.

$$\begin{aligned}r_{PMU-CC} \simeq & \frac{\sum_{j=1}^{r} \lambda_j^R * r_j^R + \sum_{k=1}^{m} \lambda_k^M * r_k^M}{\lambda_{PMU-CC}} \\ &+ \frac{\sum_{u=1}^{s} \lambda_u^S * r_u^S + \sum_{l=1}^{q} \lambda_l^{PM} * r_l^{PM}}{\lambda_{PMU-CC}}\end{aligned} \tag{2.64}$$

In Sect. 2.5.5 a detailed CTMC failure model of receiving synchrophasor measurements from 3 different PMUs at the PDC would be presented, that would use the equivalent failure rate and repair times of the PMUs (λ_{PMU}, r_{PMU}) and that of the communication channel $(\lambda_{PMU-CC}, r_{PMU-CC})$ derived in this section as inputs.

Failure modes of FB4: SE of LV grid by LV-SAU

The failure of FB4 is either caused by the failure of LV-SAU, or any of the three data repositories namely the PDC, MDMS and NIS. The failure of the LV-SAU can be caused by the failure of its following components.

- Failure of the power supply with a failure rate of $\lambda_{LV-SAU-PS}$ and repair time of $r_{LV-SAU-PS}$.
- Failure of the processing and local memory management system with a failure rtae $\lambda_{LV-SAU-HW}$ and repair rate of $\lambda_{LV-SAU-HW}$.
- Failure of its firmware that has the SE algorithm embedded in it. The firmware also enables the real time operation of the SE and hosts the routines that fetch data in regular intervals from the three repositories and provide to the SE. The failure rate of the firmware is denoted as $\lambda_{LV-SAU-FW}$ and the repair time as $r_{LV-SAU-FW}$.

The overall failure rate of the LV-SAU and its approximate repair time can then be calculated as in Eq. (2.65) and Eq. (2.66) respectively.

$$\lambda_{LV-SAU} = \lambda_{LV-SAU-PS} + \lambda_{LV-SAU-HW} + \lambda_{LV-SAU-FW} \tag{2.65}$$

$$\begin{aligned} &r_{LV-SAU} \simeq \\ &\frac{\lambda_{LV-SAU-PS} * r_{LV-SAU-PS} + \lambda_{LV-SAU-HW} * r_{LV-SAU-HW}}{\lambda_{LV-SAU}} \\ &+ \frac{\lambda_{LV-SAU-FW} * r_{LV-SAU-FW}}{\lambda_{LV-SAU}} \end{aligned} \tag{2.66}$$

The equivalent failure rate of the LV-SAU performing the SE and the mean repair time for succesful estimation after a failure is as given in Eq. (2.67) and Eq. (2.68) respectively. Where λ_{MDMS}, λ_{NIS}, λ_{PDC} correspond to the software failures in MDMS, NIS and PDC and r_{MDMS}, r_{NIS}, r_{PDC} correspond to their mean repair times respectively.

$$\lambda_{LV-SE} = \lambda_{LV-SAU} + \lambda_{MDMS} + \lambda_{NIS} + \lambda_{PDC} \tag{2.67}$$

$$r_{LV-SE} \simeq \frac{\lambda_{LV-SAU} * r_{LV-SAU} + \lambda_{MDMS} * r_{MDMS}}{\lambda_{LV-SE}} + \frac{\lambda_{NIS} * r_{NIS} + \lambda_{PDC} * r_{PDC}}{\lambda_{LV-SE}} \tag{2.68}$$

Failure modes of FB5: SE of MV grid by MV-SAU

There are two major components in the FB5. Firstly, the individual data communication channel used by separate LV-SAU to send its estimates of the states of its LV grid. Secondly the hardware that hosts the MV-SAU and its firmware.

The failure of the communication channel can be caused by the failure of any switching/routing devices or the physical mediums connecting them. Therefore, the failure rate of the communication channel used by a LV-SAU is given by Eq. (2.63)

$$\lambda_{LV-SAU-CC} = \sum_{j=1}^{r} \lambda_j^R + \sum_{k=1}^{m} \lambda_k^M + \sum_{u=1}^{s} \lambda_u^S + \sum_{l=1}^{q} \lambda_l^{PM} \tag{2.69}$$

where λ_j^R,λ_k^M, λ_u^S and λ_l^{PM} correspond to the failure of j^{th} relaying component,k^{th} modem, s^{th} switch and l^{th} physical medium link respectively. The repair time of the communication channel considering the repair times of its individual components can be calculated as Eq. (2.70). Where r_j^R,r_k^M, r_u^S and r_l^{PM} correspond to the repair time of j^{th} relaying component,k^{th} modem, s^{th} switch and l^{th} physical medium link respectively.

$$r_{LV-SAU-CC} \simeq \frac{\sum_{j=1}^{r} \lambda_j^R * r_j^R + \sum_{k=1}^{m} \lambda_k^M * r_k^M}{\lambda_{LV-SAU-CC}} + \frac{\sum_{u=1}^{s} \lambda_u^S * r_u^S + \sum_{l=1}^{q} \lambda_l^{PM} * r_l^{PM}}{\lambda_{LV-SAU-CC}} \tag{2.70}$$

The failure of the MV-SAU can be caused by the failure of its following components.

- Failure of the power supply with a failure rate of $\lambda_{MV-SAU-PS}$ and repair time of $r_{MV-SAU-PS}$.
- Failure of the processing and local memory management system with a failure rate $\lambda_{MV-SAU-HW}$ and repair rate of $\lambda_{MV-SAU-HW}$.

- Failure of its firmware that has the SE algorithm embedded in it. The firmware also enables the real time operation of the SE and hosts the routines that fetch data in regular intervals from the repositories that store the estimates from each MV-SAU. The failure rate of the firmware is denoted as $\lambda_{MV-SAU-FW}$ and the repair time as $r_{MV-SAU-FW}$.

The overall failure rate of the MV-SAU and its approximate repair time can then be calculated as in Eq. (2.71) and Eq. (2.72) respectively.

$$\lambda_{MV-SAU} = \lambda_{MV-SAU-PS} + \lambda_{MV-SAU-HW} + \lambda_{MV-SAU-FW} \quad (2.71)$$

$$r_{MV-SAU} \simeq \frac{\lambda_{MV-SAU-PS} * r_{MV-SAU-PS} + \lambda_{MV-SAU-HW} * r_{MV-SAU-HW}}{\lambda_{MV-SAU}} + \frac{\lambda_{MV-SAU-FW} * r_{MV-SAU-FW}}{\lambda_{MV-SAU}} \quad (2.72)$$

In Sect. 2.5.5 the detailed CTMC model of the failure of MV grid SE done by MV-SAU with estimates from two different LV-SAUs will be presented.

2.5.5 CTMC failure models of the functional blocks

Once the failure modes of the individual components of a FB is determined (as presented in Sect. 2.5.4), the next step is to generate the appropriate CTMC failure models for each FB to evaluate its reliability. In this section the CTMC failure models for each FB would be presented chronologically. In all thos CTMC models, circles/elipses correspond to the different system operational/failure states and the arrows show the transition from one state to the other either due to failure of a component or recovery of a component. The failures transition are marked with a rate labelled with λ and recovery transitions are labelled using μ.

CTMC models of FB1: SM data reception at SMDC

The reliability of the FB1 is dependant on the CTMC failure models of each of the 10 SM and their respective data transmission link failure of the PLC infrastructure. The CTMC model of the i^{th} SM and that of the PLC data transmission link used by it to transfer the data to the SMDC are shown in Fig. 2.17 and Fig. 2.18 respectively.

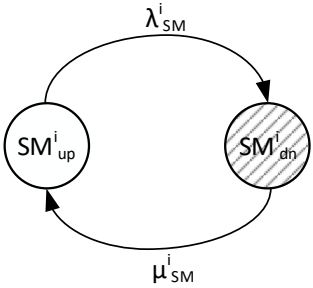


Figure 2.17: CTMC failure model of i^{th} Smart Meter (SM)

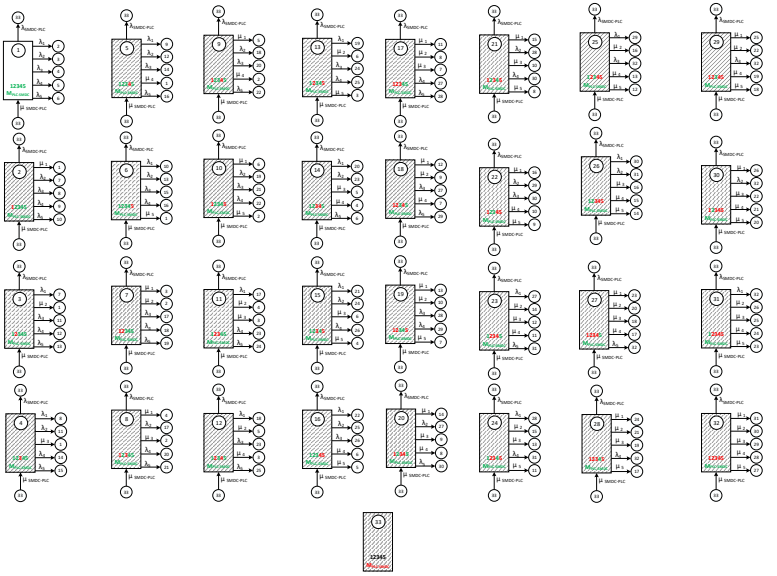


Figure 2.18: CTMC failure model of the data transmission link via the PLC infrastructure

In Fig. 2.17 the state SM^i_{up} corresponds to the operational state of the i^{th} SM where as the state shaded, SM^i_{dn} corresponds to the failed state of the SM. The i^{th} SM fails at a rate of λ^i_{SM} and has a repair rate of μ^i_{SM}, where $\mu^i_{SM} = \frac{1}{r^i_{SM}}$. The λ^i_{SM} and the r^i_{SM} are actually derived according to the Eq. (2.33) and Eq. (2.34) respectively.

Similarly, in Fig. 2.18, the state $DT - PLC^i_{up}$ corresponds to the operational state of the data transmission link used by the i^{th} SM to send the smart meter data to the SMDC via the PLC infrastructure. The states shaded in grey, $DT - PLC^i_{dn}$ corresponds to the failed states of the data transmission link (as it is assumed that, measurement from at least one SM connected at each power segment should be able to communicate). That means that all the segments should be functional along with the PLC modem connected at the SMDC side. The data transmission link fails at a rate of λ^i_{DT-PLC} and has a repair rate of μ^i_{DT-PLC}, where $\mu_i = \frac{1}{r_i}$ (r_i is its mean repair time). The λ_i and the r_i are actually derived according to the Eq. (2.35) and Eq. (2.36) respectively.

With these CTMC models the steady state probability of the SM and the data transmission link provided by the PLC to be in operational state can be calculated as per Eq. (2.22). The $\boldsymbol{\pi^i_{SM}}$ is a row vector of steady state probabilities of finding the i^{th} acrshortSM in operational state ($\pi^i_{SM_{up}}$) and in the failed state ($\pi^i_{SM_{dn}}$) as shown in Eq. (2.73).

$$\boldsymbol{\pi^i_{SM}} = [\pi^i_{SM_{up}}\ \pi^i_{SM_{dn}}] \tag{2.73}$$

Similarly, the $\boldsymbol{\pi^i_{DT-PLC}}$ is a row vector of steady state probabilities of finding the data transmission link used by the all the acrshortSM to report its measurements to the SMDC in operational state ($\pi^i_{DT-PLC_{up}}$) and in the failed state ($\pi^i_{DT-PLC_{dn}}$) as shown in Eq. (2.74).

$$\boldsymbol{\pi^i_{DT-PLC}} = [\pi^i_{DT-PLC_{up}}\ \pi^i_{DT-PLC_{dn}}] \tag{2.74}$$

The $\boldsymbol{\pi^i_{SM}}$ and $\boldsymbol{\pi^i_{DT-PLC}}$ enable the evaluation of the reliability of successful generation and transmission of the data from the i^{th} SM to the SMDC. In the Sect. 2.5.6 the overall reliability evaluation of each FB1, with 10 SMs, in a LV grid would be formulated. Thus enabling the evaluation of the reliability of reception of smart meter data from all the two areas powered by the LV grid.

CTMC models of FB2: SM data reception at MDMS

A single instance of the FB2 correspond to the successful reception of the aggregated SM data from a single SMDC at the MDMS. In this study

per LV grid there are three SMDCs deployed, which means that three instances of FB2 have to be considered in the reliability of the complete SM data transmission to the MDMS. The details of the reliability analysis of FB2 would be explained in detail in Sect. 2.5.6.

The reliability of a single FB2 instances can be calculated modelling the failure of three major components. These are the SMDC, cellular modems connected to the SMDC and MDMS, and finally the LTE infrastructure. The CTMC model depicting the failure characteristics of the SMDC is shown in Fig. 2.19. It is a two state CTMC model where the $SMDC^i_{dn}$ corresponds to the failed state of the i^{th} SMDC due to failure of its constituting components. Whereas, the $SMDC^i_{up}$ corresponds to the operational state of it. The state transition from the operational state to the failed state is triggered when any of its constituting component fails and is calculated as per Eq. (2.37). Whereas the recovery from the failed state happens at a rate of μ^i_{SMDC}, where $\mu^i_{DT-PLC} = \frac{1}{r^i_{SMDC}}$, where r^i_{SMDC} is its mean repair time, calculated as per Eq. (2.38).

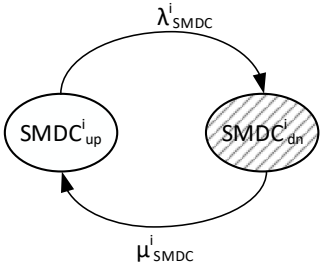


Figure 2.19: CTMC failure model i^{th} Smart Meter Data Concentrator (SMDC)

With this CTMC model the steady state probability of the SMDC to be in operational state can be calculated as per Eq. (2.22). The $\boldsymbol{\pi^i_{SMDC}}$ is a row vector of steady state probabilities of finding the i^{th} acrshortSMDC in operational state ($\pi^i_{SMDC_{up}}$) and in the failed state ($\pi^i_{SMDC_{dn}}$) as shown in Eq. (2.75).

$$\boldsymbol{\pi^i_{SMDC}} = [\pi^i_{SMDC_{up}} \pi^i_{SMDC_{dn}}] \tag{2.75}$$

The operational status of the system of two cellular modems (one connected to the SMDC and the other to the MDMS) can represented as shown in Fig. 2.20. There are four states corresponding to the four possible combinations of the operational states of both modems together. The non shaded state, $SMDC_{up}^{M-CEL}MDMS_{up}^{M-CEL}$, corresponds to the state where both the modems are functional at the same time. All the other states correspond to failure of at least one cellular modem. The transition from one state to the other is governed by the failure or repair of a specific cellular modem.

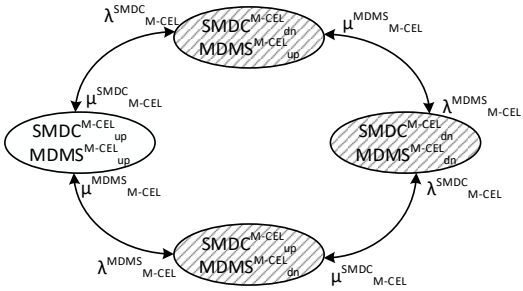


Figure 2.20: CTMC failure model of cellular modems connected to SMDC and MDMS

The failure rate of each cellular modem and its repair rate of each cellular modem (reciprocal of repair time) can be calculated as explained in Eq. (2.39) and Eq. (2.40) respectively. It should be noted that there are three states that are shaded. These states correspond to the failure of the data transmission between the SMDC and MDMS. In all these three shaded states at least one of the cellular modems is not functional rendering the data transmission failure. Therefore, in the evaluation of the reliability of the FB2, only the probability of being in the non shaded state ($SMDC_{up}^{M-CEL}MDMS_{up}^{M-CEL}$) would be considered as reliable operation of the cellular modem pair.

With this CTMC model the steady state probability of the cellular modems connected to SMDC and to MDMS to be in operational state can be calculated as per Eq. (2.22). The $\boldsymbol{\pi_{M-CEL}}$ is a row vector of steady

state probabilities of finding the system of two cellular modems in different operational states as shown in Eq. (2.76).

$$\boldsymbol{\pi_{M-CEL}} = [\pi^{M-CEL}_{SMDC_{up}MDMS_{up}} \; \pi^{M-CEL}_{SMDC_{up}MDMS_{dn}} \; \pi^{M-CEL}_{SMDC_{dn}MDMS_{up}} \; \pi^{M-CEL}_{SMDC_{dn}MDMS_{dn}}] \tag{2.76}$$

Finally the last component involved in the data transmission is the LTE infrastructure, whose CTMC failure model is as shown in Fig. 2.21. Each non shaded circle corresponds to the state where the EPC is functional and a set of the eNodeBs are functional. The exact eNodeBs that are functional are shown in the subscript. For example in the state $eNodeB_{13}EPC_{up}$ corresponds to the state where eNodeB:1 and eNodeB:3 are operational and the EPC is also functional. In this study, it is assumed that for improving

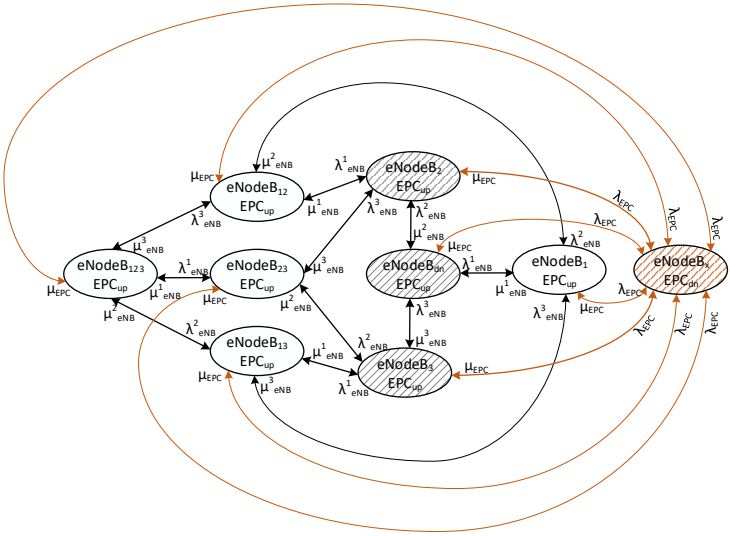


Figure 2.21: CTMC failure model of LTE infrastructure

the reliability of data transmission between the SMDC and MDMS cells of eNodeB:1, enodeB:2 and eNodeB:3 are so configured that the cellular modem of the SMDC is able to communicate with eNodeB:1 and enodeB:2 whereas the MDMS is able to communicate with eNodeB:1, enodeB:3,

provided that the EPC is always functional. Therefore, if the EPC fails, or every eNodeB fails when the EPC is functional(state $eNodeB_2EPC_{up}$), or only eNodeB:2 is functional (state $eNodeB_2EPC_{up}$) or just the eNodeB:3 is functional (state $eNodeB_3EPC_{up}$), the data transmission through the LTE infrastructure between the SMDC and MDMS fails. In the CTMC model the shaded states (black and brown) correspond to one of the failure states mentioned before. The state shaded in black correspond to the failure of data transmission due to failures in eNodeBs only (while the EPC is functional). The state shaded in brown, $eNodeB_xEPC_{dn}$ corresponds to the condition where the EPC has failed (irrespective of the condition of the eNodeBs that are functional). The failure of EPC triggers the transition from all other states (directed arcs coloured in brown) to this state at a rate of λ_{EPC}, calculated as per Eq. (2.53). The system goes back to the state where it came from (directed arcs coloured in brown) with a repair rate of $\mu_{EPC} = \frac{1}{r_{EPC}}$, where r_{EPC} is the mean repair time of the EPC calculated as per Eq. (2.54). The transition between the other states (except the state $eNodeB_xEPC_{dn}$) is caused by failure or recovery of i^{th} eNodeB denoted by the failure rate and recovery rate of λ^i_{eNB} and $\mu_{eNB} = \frac{1}{r^i_{eNB}}$, where r^i_{eNB} is its mean recovery time, which can be calculated as per Eq. (2.45) and Eq. (2.46) respectively.

With this CTMC model the steady state probability of the cellular infrastructure to be in the nine operational state can be calculated as per Eq. (2.22). The $\boldsymbol{\pi_{CEL}}$ is a row vector of steady state probabilities of finding the system of the cellular infrastructures in different operational states as shown in Eq. (2.77). Where the superscript of each element of the $\boldsymbol{\pi_{CEL}}$ correspond to the status of the eNodeBs and the subscript corresponds to the status of the EPC. In the equations the eNodeB is abbreviated as eNB.

$$\begin{aligned}\boldsymbol{\pi_{CEL}} = [&\pi^{eNB_{123}}_{EPC_{up}}\ \pi^{eNB_{12}}_{EPC_{up}}\ \pi^{eNB_{23}}_{EPC_{up}}\ \pi^{eNB_{13}}_{EPC_{up}}\\ &\pi^{eNB_{1}}_{EPC_{up}}\ \pi^{eNB_{2}}_{EPC_{up}}\ \pi^{eNB_{3}}_{EPC_{up}}\\ &\pi^{eNB_{dn}}_{EP_{up}}\ \pi^{eNB_{x}}_{EP_{dn}}]\end{aligned} \tag{2.77}$$

With the probability vectors $\boldsymbol{\pi^i_{SMDC}}$, $\boldsymbol{\pi_{M-CEL}}$ and $\boldsymbol{\pi_{CEL}}$ the overall reliability of the transmission of the data from a single SMDC to the MDMS via the cellular infrastructure can be calculated. The detailed calculation would be presented in Sect. 2.5.6.

CTMC models of FB3: PMU data reception by PDC

In this test case three PMUs along with their independent Communication Channels (CCs) are assumed to be deployed for each LV grid. A CTMC

model depicting the status of the three PMUs is shown in Fig. 2.22. The ellipses represent the 8 operational states of the PMUs and the transitions represent the failure of a specific PMU or a recovery of it. The numbers mentioned in the subscript denote the specific PMU device that is functional. For e.g PMU_{12} corresponds to a state where only the PMU 1 and the PMU 2 are functional. Finally the ellipse shaded in grey (PMU_{dn}) corresponds to the operational state where none of the PMUs are functional. The λ^i_{PMU} is the failure rate of the i^{th} PMU as calculated in Eq. (2.61) and the repair rate $\mu^i_{PMU} = \frac{1}{r^i_{PMU}}$, where r^i_{PMU} is the mean repair time of the PMU calculated as per Eq. (2.62).

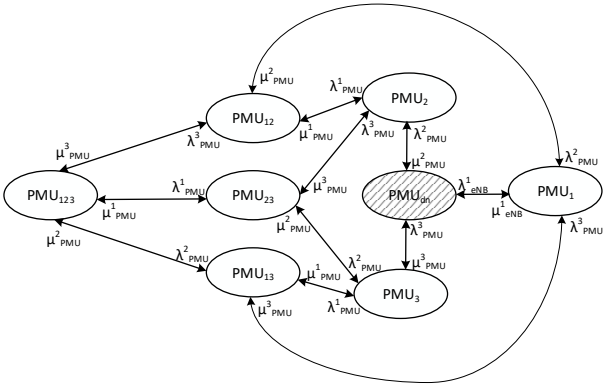


Figure 2.22: CTMC failure model of the three PMUs

Similarly since each PMU is assumed to have independent communication channel to the PDC the failure model of the communication channels of the PMUs (PMU-CC) also has 8 operational states in total as shown in Fig. 2.23. Similar to the CTMC model of the PMUs the state transition is triggered either by the failure or recovery of a specific communication channel. The state shaded in grey corresponds to the operational state where none of the communication channels are functional.

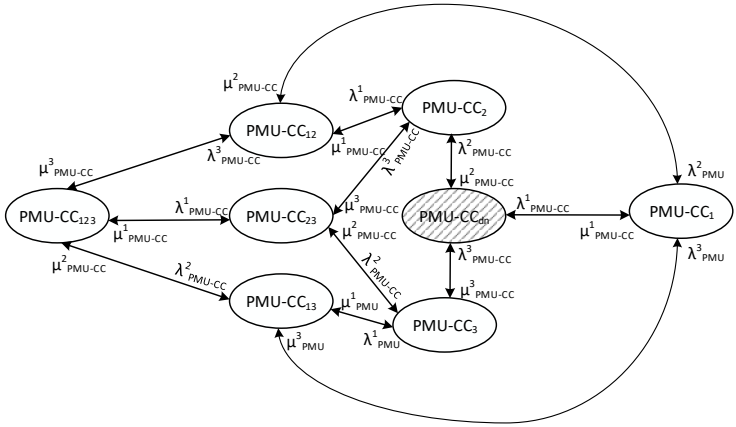


Figure 2.23: CTMC failure model of the communication channels of the three PMUs

The (λ^i_{PMU-CC}) is the failure rate of the communication channel used by the i^{th} PMU, which can be calculated as per Eq. (2.63). The repair rate of the communication channel used by the i^{th} PMU is $\mu^i_{PMU-CC} = \frac{1}{r^i_{PMU-CC}}$, where r^i_{PMU-CC} is the mean repair time of the communication channel calculated as per Eq. (2.64).

The steady state probability of the number of PMUs functional $(\boldsymbol{\pi_{PMU}})$ can be deduced with the CTMC model depicted in Fig. 2.22 as per Eq. (2.22). The $\boldsymbol{\pi_{PMU}}$ is a row vector of steady state probabilities the system of three PMUs in different operational states as shown in Eq. (2.78).

$$\boldsymbol{\pi_{PMU}} = [\pi^{PMU}_{123} \ \pi^{PMU}_{12} \ \pi^{PMU}_{13} \ \pi^{PMU}_{23} \ \pi^{PMU}_{1} \ \pi^{PMU}_{2} \ \pi^{PMU}_{3} \ \pi^{PMU}_{dn}] \quad (2.78)$$

.

Similarly, the steady state probability of the communication channels of the PMUs PMUs functional $(\boldsymbol{\pi_{PMU-CC}})$ can be deduced with the CTMC model depicted in Fig. 2.23 as per Eq. (2.22). The $\boldsymbol{\pi_{PMU-CC}}$ is a row vector of steady state probabilities the system of the PMUs in different operational states as shown in Eq. (2.79).

$$\boldsymbol{\pi_{PMU-CC}} = [\pi_{123}^{PMU-CC}\ \pi_{12}^{PMU-CC}\ \pi_{13}^{PMU-CC}\ \pi_{23}^{PMU-CC} \\ \pi_{1}^{PMU-CC}\ \pi_{2}^{PMU-CC}\ \pi_{3}^{PMU-CC}\ \pi_{dn}^{PMU-CC}] \tag{2.79}$$

.

These probabilities are then used to evaluate the reliability of the PMU data generation and transmission and thus determine the overall reliability of the functional block FB3. The Sect. 2.5.6 would present this in a bit more detail.

CTMC models of FB4: SE of LV grid by LV-SAU

The CTMC model to evaluate the probability of executing the LV-SE by the LV-SAU along with its repositories and the firmware hosting the algorithm for SE is depicted in Fig. 2.24.

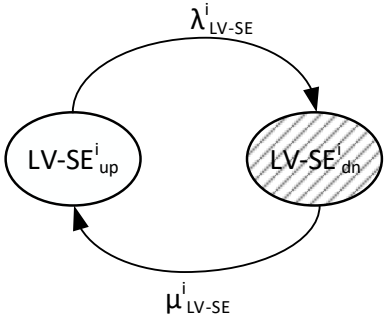


Figure 2.24: CTMC failure model of LV-SE

The CTMC model has only two states one being the state where the LV-SE is operational ($LV - SE_{up}^{i}$) and the other when it has failed due to various reasons as explained in Sect. 2.5.4. The SE of the i^{th} LV grid fails at a rate of λ_{LV-SE}^{i} calculated as per Eq. (2.67). The LV-SE recovers from the failed state to fully operational state at a rate of $\mu_{LV-SE}^{i} = \frac{1}{r_{LV-SE}^{i}}$, where r_{LV-SE}^{i} is the mean repair time of the communication channel calculated as per Eq. (2.68).

With this CTMC model the steady state probability of the successful state estimation performed by the LV-SAU can be calculated as per

Eq. (2.22). The $\boldsymbol{\pi^i_{LV-SE}}$ is a row vector of steady state probabilities of successful state estimation performed by the i^{th} LV-SAU ($\pi^i_{LV-SE_{up}}$) and unsuccessful state estimation ($\pi^i_{LV-SE_{dn}}$) only caused by the failure of the i^{th} LV-SAU.

$$\boldsymbol{\pi^i_{LV-SE}} = [\pi^i_{LV-SE_{up}} \pi^i_{LV-SE_{dn}}] \tag{2.80}$$

CTMC models of FB5: SE of MV grid by MV-SAU

The reliability of the SE of the MV grid depends on the reliability of the data communication channel between the LV-SAU and MV-SAU and the reliability of MV-SAU that hosts the SE functionality. The CTMC failure model of the system of two separate communication channels that are individually used by the two LV-SAUs to communicate with the MV-SAU is as shown in Fig. 2.25. The CTMC model has four operational states,

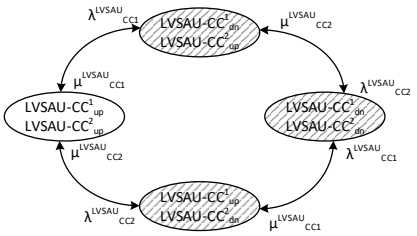


Figure 2.25: CTMC failure model of communication channels between LV-SAU and MV-SAU

where, $LVSAU - CC^1_{up} LVSAU - CC^2_{up}$ corresponds to the state where both the communication channels are functional. In the other states either one of the channels are not functional or both are not functional triggered by the failure of any of the components that form the communication channel. The subscripts *up* and *dn* correspond to the functional status of each communication channel , namely up or down respectively. The superscripts 1 and 2 correspond to the index of the communication channel. The state transition is either caused by the failures of communication channels 1 and 2 with a failure rate of λ^{LVSAU}_{CC1} and λ^{LVSAU}_{CC2} respectively or their recovery with a rate of $\mu^{LVSAU}_{CC1} = \frac{1}{r^{LVSAU}_{CC1}}$ and $\mu^{LVSAU}_{CC2} = \frac{1}{r^{LVSAU}_{CC2}}$ respectively. The r^{LVSAU}_{CC1} and r^{LVSAU}_{CC2} correspond to the mean repair time of the communication channel as calculated in Eq. (2.70). For the

reliability analysis the state $LVSAU - CC^1_{up} LVSAU - CC^2_{up}$ would be considered as the functional state and the rest of the states (shaded) would be considered as failure state. This is because for successful state estimation of the MV grid data from both the LV-SAUs are absolutely necessary.

With this CTMC model the steady state probability of the communication channels used by the LV-SAU to report the state estimates to the MV-SAU, to be in operational state can be calculated as per Eq. (2.22). The $\boldsymbol{\pi_{LV-MV-CC}}$ is a row vector of steady state probabilities of the different operational states of the two communication channels that are individually used by two separate LV-SAUs to communicate with the MV-SAU is shown in Eq. (2.81).

$$\boldsymbol{\pi_{LV-MV-CC}} = [\pi^{LVSAU}_{CC1_{up}CC2_{up}} \; \pi^{LVSAU}_{CC1_{up}CC2_{dn}} \; \pi^{LVSAU}_{CC1_{dn}CC2_{up}} \; \pi^{LVSAU}_{CC1_{dn}CC2_{dn}}] \tag{2.81}$$

The CTMC model of the successful state estimation of the MV grid by the MV-SAU is depicted in Fig. 2.26. The CTMC model has just two

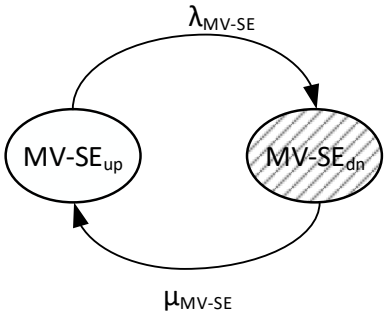


Figure 2.26: CTMC failure model of the MV-SAU

states, one corresponds to the MV-SAU being operational to carry out the SE algorithm ($MVSE_{up}$) and the other state that corresponds to the failure in the state estimation ($MVSE_{dn}$). It should be noted that this CTMC model only encapsulated the failure in performing the SE just due to the failure of the MV-SAU.

With this CTMC model the steady state probability of the successful state estimation performed by the MV-SAU can be calculated as per Eq. (2.22). The $\boldsymbol{\pi_{MV-SE}}$ is a row vector of steady state probabilities of successful state estimation performed by the MV-SAU ($\pi_{MV-SE_{up}}$) and unsuccessful state estimation ($\pi_{MV-SE_{dn}}$) caused only by the failure of the LV-SAU.

$$\boldsymbol{\pi_{MV-SE}} = [\pi_{MV-SE_{up}}\ \pi_{MV-SE_{dn}}] \tag{2.82}$$

The $\boldsymbol{\pi_{LV-MV-CC}}$ and $\boldsymbol{\pi_{MV-SE}}$ would be used to determine the overall reliability of the FB5. A detailed explanation of the reliability evaluation would be presented in Sect. 2.5.6. In this study two LV grids are considered to be part of the MV grid. In reality it could be more, but for this study it has been limited to just two. With increase in the number of LV grids in the MV grid, neither the process of evaluating the reliability of FB 5 would change nor the number of CTMC failure models required for its reliability evaluation. The only thing that would change with the increase in the number of LV grids per MV grid, is the size of the CTMC model corresponding to the communication channels between the LV-SAU and MV-SAU. If there are k LV grids in a MV grid then the size of the CTMC model of the communication channels shown in Fig. 2.25 would have 2^k states.

2.5.6 Reliability evaluation

In this section the detailed MDRM would be derived for all FBs. Furthermore, the mathematical formulation for evaluating the reliability of each FB would be presented. The CTMC models presented in Sect. 2.5.5 would be used as inputs. Furthermore, depending upon the requirements of the SE algorithm regarding the minimum measurements required for observability the appropriate elements of the MDRM would be selected for the reliability evaluation of each FB. Additionally, given the failure characteristics of the different components in the measurement acquisition system, the average availability of the different measurements at the LV-SAU can be calculated. With the average availability of each measurement, the mean accuracy achievable in estimating the state of the LV grid would be presented.

Reliability evaluation of FB1

For each LV grid there are three instances of FB1 involved. Where each FB1, corresponds to the reporting of the ten SM measurements from an area to their respective SMDCs. Since there are three different areas

considered in per LV grid, three instances of FB1 have to be included in the reliability analysis for the reception of the complete SM data at their SMDCs. It should also be considered that the ten SMs are geographically placed so that they are evenly spread along the different segments of the radial power line. In this study there are 5 segments of power lines connected radially and there are 2 SM connected at every segment of the power line (denoted with a and b) as shown in Fig. 2.27.

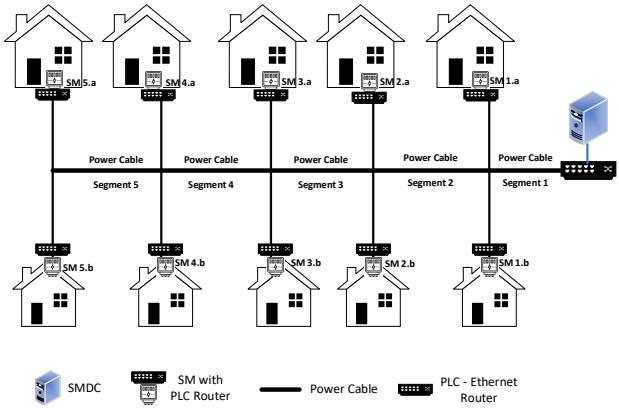


Figure 2.27: Distribution of SM in an area that send its measurements to the same SMDC

The MDRM for the transfer of measurements from at least one SM connected to the i^{th} power line segment to its SMDC is as given in Eq. (2.83). Where n is the total number of power line segments considered in the radial grid, s_{DT-PLC} is number of states in CTMC failure model of the data transmission link via the PLC infrastructure (Fig. 2.18)

$$MDRM_{SM}(j) = (\prod_{i=0}^{n}(1 - (\pi_{SM_{dn}}^{i.a} * \pi_{SM_{dn}}^{i.b}))) * \boldsymbol{\pi_{DT-PLC}^{i}}(j) \tag{2.83}$$

where

$1 \leq j \leq s_{DT-PLC}$;

The overall reliability of the FB1 is then calculated as per Eq. (2.84). The reliability of each FB1 instance is the probability that measurements from

at least five SMs connected in different power line segments are received, taking into account that from an area measurements from maximum of ten SMs could be received at the SMDC.

$$R_{FB1} = MDRM_{SM}(1) \tag{2.84}$$

Considering that there are l number of instances of FB1 in a system then the total reliability of the l FBs functioning together can then be calculated as shown in Eq. (2.85).

$$R_{FB1}^{Total} = \prod_{k=1}^{l} R_{FB1}^{k} \tag{2.85}$$

Reliability evaluation of FB2

The reliability of the FB2 is determined by the reliability of the SMDC, the cellular modems connected to the SMDC and MDMS, and the cellular infrastructure. Each FB2 instance is responsible for the data transmission between a specific SMDC and the MDMS. For its reliability evaluation, firstly the MDRM of the i^{th} FB2 (responsible for enabling data transmission between the $i1th$ SMDC and MDMS) is calculated as shown in Eq. (2.86) using Eq. (2.75),Eq. (2.76),Eq. (2.77). Where s_{CEL} is the number of states in the CTMC failure model of the cellular infrastructure as depicted in Fig. 2.21.

$$\begin{aligned}
&MDRM_{FB2}(1,j) = \boldsymbol{\pi}^{\boldsymbol{i}}_{\boldsymbol{SMDC}}(1,1) * \boldsymbol{\pi}_{\boldsymbol{M-CEL}}(1,1) * \boldsymbol{\pi}_{\boldsymbol{CEL}}(1,j) \\
&where \\
&1 \leq k \leq s_{CEL}; \\
&\boldsymbol{\pi}^{\boldsymbol{i}}_{\boldsymbol{SMDC}} = [\pi^{i}_{SMDC_{up}}\ \pi^{i}_{SMDC_{dn}}]; \\
&\boldsymbol{\pi}_{\boldsymbol{M-CEL}} = [\pi^{M-CEL}_{SMDC_{up}MDMS_{up}}\ \pi^{M-CEL}_{SMDC_{up}MDMS_{dn}} \\
&\qquad\qquad \pi^{M-CEL}_{SMDC_{dn}MDMS_{up}}\ \pi^{M-CEL}_{SMDC_{dn}MDMS_{dn}}]; \\
&\boldsymbol{\pi}_{\boldsymbol{CEL}} = [\pi^{eNB_{123}}_{EPC_{up}}\ \pi^{eNB_{12}}_{EPC_{up}}\ \pi^{eNB_{23}}_{EPC_{up}}\ \pi^{eNB_{13}}_{EPC_{up}} \\
&\qquad\qquad \pi^{eNB_{1}}_{EPC_{up}}\ \pi^{eNB_{2}}_{EPC_{up}}\ \pi^{eNB_{3}}_{EPC_{up}} \\
&\qquad\qquad \pi^{eNB_{dn}}_{EP_{up}}\ \pi^{eNB_{x}}_{EP_{dn}}]
\end{aligned} \tag{2.86}$$

As described in Sect. 2.5.5, the states $\pi^{eNB_2}_{EPC_{up}}$, $\pi^{eNB_3}_{EPC_{up}}$, $\pi^{eNB_{dn}}_{EP_{up}}$, $\pi^{eNB_x}_{EP_{dn}}$ correspond to the failed operational state of the cellular infrastructure. Therefore, as per Eq. (2.86), the elements $MDRM_{FB2}(1,1)$ to $MDRM_{FB2}(1,5)$

correspond to the reliable operation of the FB2. Hence, the reliability of the FB2 is calculated as per Eq. (2.87).

$$R_{FB2} = \sum_{j=1}^{5} MDRM_{FB2}(1,j) \tag{2.87}$$

Considering that there are l number of instances of FB2 in a system then the total reliability of the l FBs functioning together can then be calculated as shown in Eq. (2.88).

$$R_{FB2}^{Total} = \prod_{k=1}^{l} R_{FB2}^{k} \tag{2.88}$$

Reliability evaluation of FB3

The reliability of reception of the measurements from three PMUs data at the PDC can be derived by first constructing the MDRM as per Eq. (2.89) using Eq. (2.78) and Eq. (2.79). Where s_{PMU} and s_{PMU-CC} is the number of states in the CTMC failure model of PMUs as depicted in Fig. 2.22 and its communication channels as depicted in Fig. 2.23 respectively.

$$\begin{aligned} &MDRM_{FB3}(i,j) = \boldsymbol{\pi_{PMU}}(1,i) * \boldsymbol{\pi_{PMU-CC}}(1,j) \\ &where \\ &1 \leq i \leq s_{PMU} \\ &1 \leq j \leq s_{PMU-CC} \end{aligned} \tag{2.89}$$

In this test case it is assumed that reception of at least two PMU measurements at the PDC would ensure reliable operation of the state estimator. Therefore, as shown in Eq. (2.90), the entries coloured in green and blue together correspond to the reliable operation of the complete PMU infrastructure.

$$MDRM_{FB3}= \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 \\ p_9 & p_{10} & p_{11} & p_{12} & p_{13} & p_{14} & p_{15} & p_{16} \\ p_{17} & p_{18} & p_{19} & p_{20} & p_{21} & p_{22} & p_{23} & p_{24} \\ p_{25} & p_{26} & p_{27} & p_{28} & p_{29} & p_{30} & p_{31} & p_{32} \\ p_{33} & p_{34} & p_{35} & p_{36} & p_{37} & p_{38} & p_{39} & p_{40} \\ p_{41} & p_{42} & p_{43} & p_{44} & p_{45} & p_{46} & p_{47} & p_{48} \\ p_{49} & p_{50} & p_{51} & p_{52} & p_{53} & p_{54} & p_{55} & p_{56} \\ p_{57} & p_{58} & p_{59} & p_{60} & p_{61} & p_{62} & p_{63} & p_{64} \end{bmatrix} \tag{2.90}$$

Therefore, the total reliability of FB3 is as given in . Where N is the number of elements in Set of Reliable operation mode: green and blue shaded elements.

$$R_{FB3}^{Total} = \sum_{j=1}^{N} p_(j)$$
$$where$$
$$\forall\,(j) \in Set(Reliable\ operation\ mode : green\ and\ blue\ shaded\ elements) \tag{2.91}$$

Reliability evaluation of FB4

The FB4 is responsible for successful operation of the LV-SAU so that it can perform the state estimation. The $\boldsymbol{\pi_{LV-SE}^{i}}(1,1) = \pi_{LV-SE_{up}}^{i}$ as per Eq. (2.80) corresponds to the probability of successful operation of the i^{th} LV-SAU. The complete reliability of the state estimation of the i^{th} LV grid considering the reliability of the FB1, FB2, and FB3 can then be calculated as per Eq. (2.92). The total reliability of successful state estimation of n such LV grids in an MV grid can then be calculated as shown in Eq. (2.93).

$$R_{FB4}^{i} = R_{FB1_i}^{Total} * R_{FB2_i}^{Total} * R_{FB3_i}^{Total} * \pi_{LV-SE_{up}}^{i} \tag{2.92}$$

$$R_{FB4}^{Total} = \prod_{k=1}^{n} R_{FB4}^{k} \tag{2.93}$$

Reliability evaluation of FB5

The reliability of the communication channels used by the two LV-SAUs and the MV-SAU determines the reliability of the FB5. The MDRM for the transfer of LV grid state estimates to the MV-SAU is as given in Eq. (2.94)using the Eq. (2.82) and Eq. (2.81). Where s_{MV-SE} and $s_{LV-MV-CC}$ correspond to the number of states in the CTMC failure model of the MV-SAU as depicted in Fig. 2.26 and CTMC failure model of the two communication channels individually used by two separate LV-SAUs as depicted in Fig. 2.25 respectively.

$$
\begin{aligned}
&MDRM_{FB5}(k,j) = \boldsymbol{\pi_{MV-SE}}(k) * \boldsymbol{\pi_{LV-MV-CC}}(j) \\
&where \\
&1 \leq k \leq s_{MV-SE}; \\
&1 \leq j \leq s_{LV-MV-CC};
\end{aligned}
\tag{2.94}
$$

Since the $\boldsymbol{\pi_{MV-SE}}(1,1)$ and $\boldsymbol{\pi_{LV-MV-CC}}(1,1)$ correspond to the state where the MV-SAU and both the communication channels are functional. Therefore, the reliability of just the FB5 is as shown in Eq. (2.95).

$$R_{FB5} = MDRM_{FB5}(1,1) \tag{2.95}$$

The total reliability of successful state estimation of the MV grid given the reliability of the successful state estimation of its LV grids can then be calculated as in Eq. (2.96). The R_{FB5}^{Total} corresponds to the over all reliability of performing the state estimation of a MV grid considering the failure characteristics of all its constituting cyber-physical components responsible for measurement generation, transmission and processing that includes the components of the LV grid.

$$R_{FB5}^{Total} = R_{FB5} * R_{FB4}^{Total} \tag{2.96}$$

2.5.7 Test scenario and Results

For the test scenario, the failure rates of the different components have been derived according to the SN29500 and MIL-HDBK-217 standards. However, for each device in a specific FB, the assumed availability of its constituting components is different. The assumed availability of the components constituting the different devices are as given below.

- Components of SM : 99.00 %.
- Components of PLC modem : 99.90 %.
- Components of SMDC : 99.90 %.
- Components of eNodeB-LTE : 99.99 %.
- Components of EPC-LTE : 99.99 %.
- Components of PMU : 99.90 %.
- Components of PMU communication channel :99.99 %.

- Components of LV-SAU : 99.99 %.
- Components of LV-SAU communication channel to MV-SAU : 99.99 %.
- Components of MV-SAU : 99.99 %.

The assumption of the availability is necessary to derive the repair time of each component according to the Eq. (2.1). The repair time and the failure rate of the components determine the reliability of each device of a specific FB. The reliability of the device can be represented as a function of failure rate and repair time of each device, which is then used to calculate the reliability of each FB as described in Sect. 2.5.6. The reliability evaluation of the individual FBs would be presented in the subsequent subsection and finally the reliability of the heterogeneous monitoring system to estimate the state of the LV grid by the LV-SE hosted by LV-SAU using the measurements from SMs and PMUs is presented. Furthermore, the reliability of the monitoring of the complete MV grid using the state estimates from individual LV grids by the MV-SAU is also presented.

Reliability of FB1

The FB1 is composed of the smart meters and the PLC infrastructure. The reliability of the individual smart meters and the complete PLC infrastructures, that enables data transfer of measurements from at least one SM is as depicted in Tab. 2.1 and in Tab. 2.2.

The complete reliability of the functional block is calculated and depicted in comparison with the other functional blocks as shown in Tab. 2.3

Reliability of FB2

The functional block FB2 consists of the SMDC and the cellular infrastructure. The reliability of the SMDC is depicted in Tab. 2.4. The reliability of the LTE infrastructure is depicted in Tab. 2.5. The reliability of the modems that connect the SMDC and the MDMS to the cellular network is shown in Tab. 2.6.The overall reliability of the functional block which

Table 2.1: Reliability of Smart Meter

CTMC States	SM_{up}	SM_{dn}
Steady state probability	0.9162	0.0838

Table 2.2: Reliability of PLC Infrastructure

CTMC States	PLC_{up}	PLC_{dn}
Steady state probability	0.97	0.03

Table 2.3: Reliability Functional Blocks

Functional Blocks	$FB1$	$FB2$	$FB3$	$FB4$	$FB5$
Steady state probability	0.9365	0.9427	1	0.9994	0.9979

is the combination of the reliability of the SMDC, Cellular modems and LTE is given in Tab. 2.3.

Reliability of FB3

The reliability of the FB3 is composed of the reliability of the PMUs and the communication channel that each PMU uses to communicate to the PDC. The FB3 is considered to be reliable if even one of the PMU measurements is reliably transferred to the PDC. The reliability of PMUs where at least one PMU is functional with its communication channel is depicted in Tab. 2.7 and in Tab. 2.8.

Thus reducing the number of down states to be considered for the CTMC models for PMUs and their communication channels, as depicted in Tab. 2.3, the overall availability of FB3 is comparatively higher compared to the other FBs.

Reliability of FB4 and FB5

The reliability of FB4 is the reliability of the LV-SAU. The Overall reliability of the SAU performing the state estimation is depicted in Tab. 2.9.

The reliability of transferring the estimates of the states from at least one LV-SAU is depicted in Tab. 2.10.

The reliability of the state estimation performed by the MV-SAU is depicted in Tab. 2.11.

Table 2.4: Reliability of Smart Meter Data Concentrator (SMDC)

CTMC States	$SMDC_{up}$	$SMDC_{dn}$
Steady state probability	0.9941	0.0059

Table 2.5: Reliability of LTE/4G (Long Term Evolution)

CTMC States	Steady state probability
$eNB_{123} - EPC_{up}$	0.9585
$eNB_{12} - EPC_{up}$	0.00983
$eNB_{23} - EPC_{up}$	0.00983
$eNB_{13} - EPC_{up}$	0.00983
$eNB_{1} - EPC_{up}$	0.00125
$eNB_{2} - EPC_{up}$	0.00125
$eNB_{3} - EPC_{up}$	0.00125
$eNB_{dn} - EPC_{up}$	0.00060
$eNB_{dn} - EPC_{up}$	0.00767

Table 2.6: Reliability of Cellular Modems

CTMC States	Steady state probability
$M - CEL_{12}$	0.959
$M - CEL_{1}$	0.0204
$M - CEL_{2}$	0.0204
$M - CEL_{dn}$	0.0004

Table 2.7: Reliability of PMUs

CTMC States	Steady state probability
PMU_{123}	0.9995
PMU_{12}	0.00017
PMU_{23}	0.00017
PMU_{13}	0.00017
PMU_{1}	2.857e-8
PMU_{2}	2.857e-8
PMU_{3}	2.857e-8
PMU_{dn}	4.83e-12

Table 2.8: Reliability of PMU communication channel

CTMC States	Steady state probability
$PMU - CC_{123}$	0.9973
$PMU - CC_{12}$	0.000897
$PMU - CC_{23}$	0.000897
$PMU - CC_{13}$	0.000897
$PMU - CC_{1}$	8.08e-7
$PMU - CC_{2}$	8.08e-7
$PMU - CC_{3}$	8.08e-7
$PMU - CC_{dn}$	7.273e-10

Table 2.9: Reliability of LV-SAU to perform LV-SE

CTMC States	$LVSE_{up}$	$LVSE_{dn}$
Steady state probability	0.9994	0.0006

Table 2.10: Reliability of Communication channel from LV-SAU to MV-SAU

CTMC States	Steady state probability
$LVSAU - CC_{12}$	0.9982
$LVSAU - CC_{1}$	0.0009
$LVSAU - CC_{2}$	0.0009
$LVSAU - CC_{dn}$	8.087e-7

Table 2.11: Reliability of MV-SE by MV-SAU

CTMC States	$MVSE_{up}$	$MVSE_{dn}$
Steady state probability	0.9997	0.0003

Table 2.12: Reliability of DGA monitoring system

CTMC States	$DGA - Mon_{up}$	$DGA - Mon_{dn}$
Steady state probability	0.7773	0.2227

Finally the total reliability of the DGA monitoring system considering all five functional blocks is depicted in Tab. 2.12

2.5.8 Conclusion

With this test case it is shown that even a complex automation function realised by heterogeneous communication infrastructures and diverse automation devices can be evaluated using the proposed methodology. The complete monitoring function was divided into five functional blocks that are independent to each other, with respect to the failure characteristics. The failure rates of each automation device and the communication infrastructure have been modelled using the CTMC formalism. The failure models of heterogeneous communication infrastructures ranging from wired systems like the Ethernet and PLC till the wireless cellular systems like the LTE/4G systems have been developed. The MDRM for each functional blocks have been calculated to evaluate the reliability of the individual FBs. The reliability of individual functional blocks have been combined to evaluate the reliability of the complete monitoring function realisation of the DGA system.

2.6 Test Case 2 : Cyber-physical MTDC grid control

2.6.1 Introduction

The MTDC grids are gaining popularity in the transmission sector, for their higher power transfer capability, reliability, and flexibility in integrating large off-shore wind farms, interconnection of weak ac grids and cross oceanic ac grids[Zha+17][Cha+14]. Furthermore, MTDC grids are also being considered for the modernization of distribution grids with higher penetration of Distributed Energy Resources (DERs) to provide support for ac grid control[Bra+12][Che+19][Kor+15] and serve as controllable links between different sections of the ac system. The scale of the installation is rising as MTDC grids upto 6 terminals are being constructed [RR17]. Furthermore, the MTDC grids ensure the stability of the power grid under high volatility of energy generation[KM17][Kum+19]. Thus, helping to meet the ambitious goals of achieving higher share of energy generated from renewable energy resources to meet stringent climate change policy. Since the number of installations of MTDC grid have been increasing in the world [RR17], the reliability of the MTDC grids will influence the overall reliability of the power grids.

In this subsection, reliability analysis of cyber-physical MTDC grid, based on proposed CTMC based methodology is presented. A detailed

description of the failure models of the cyber-physical components of the control of the MTDC grid is presented. Furthermore, a multi-layered CTMC model is presented that represents the system failure modes of a MTDC grid for a specific control strategy. Finally, the impact of different redundancy measures deployed in the cyber infrastructure on the overall reliability of the MTDC grid control is presented. The failure rates assumed for the components are in accordance to the standard [IEC90] for the cyber components, sensors, and controller and MIL-HDBK-217 guidelines for the converter components. The MIL-HDBK-217 is the most widely accepted standard for reliability evaluation and prediction of power electronic equipment [SW13]. However, this standard is being currently revised to accommodate time dependant failures of power electronic devices [Wan+14].

2.6.2 Test case description

The reliability of MTDC grid heavily depends on the reliability of its control strategy. The MTDC grid with master-slave control has a single master that controls different slave converters, whose failure jeopardises the operation of complete MTDC grid[Zha+17]. The voltage margin is an improved version of master-slave control that relies on low-speed communication infrastructure with a central master controller for coordinated power flow in the MTDC grid. The droop control strategy is traditionally distributed control and does not depend on communication infrastructure for its operation. However, new methodologies of the droop control are proposed that uses communication infrastructure to communicate with a supervisory controller for optimal power flow coordination[HU12]. Therefore, the MTDC grid with the infrastructure that realizes the aforementioned control strategies can be considered as a cyber-physical infrastructure. An exemplary cyber-physical three terminal dc grid is shown in Fig. 2.28. The MTDC grid has three Converter Station(CS) CS1-CS3, their individual Data Transmission (DT) links to the Supervisory Control Unit(SCU). The different cyber and physical components of the MTDC grid are depicted in Fig. 2.29. The MTDC grid, converter and its controller, the sensors and the gate drivers form the physical part of the Cyber-Physical System (CPS) whereas the communication channel and the Supervisory Control Unit (SCU) constitute the cyber part of the CPS. This study focuses on the reliability of this exemplary three terminal dc grid with optimal droop control as presented in [HU12] . According to this method, the SCU hosts the tertiary control that generates voltage and power set-points for the VSC converters in the MTDC grid for optimal power sharing among the terminals and to maintain the voltage. The set-points are sent to the VSC

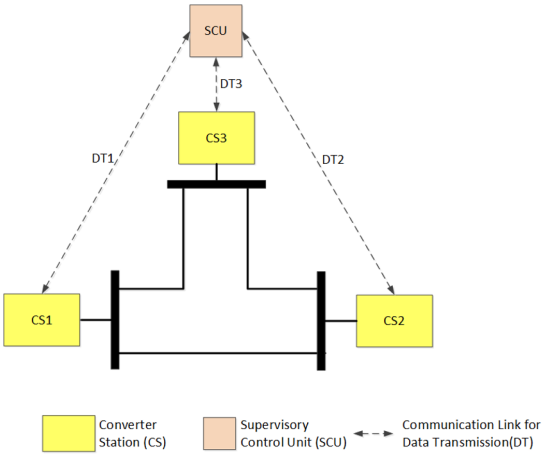


Figure 2.28: Exemplary cyber-physical three terminal MTdc grid configuration

converter controller via the communication infrastructure (of the cyber layer)[BVB11][HU12]. The VSC converters are operated in three different modes for achieving the precise control of power flow as per the method developed in [HU12]. These are 1) Power control mode, 2) Droop control mode and 3) Voltage control mode. The Voltage Source Converters (VSC) converters that are operated in power control mode and droop control mode receive power set-points and droop coefficients respectively from the tertiary control (hosted by SCU). These set points are forwarded to the local secondary control of converters. The secondary control generates a voltage set-point for the primary control of the VSC converter. The controller of the VSC converter following voltage-control mode receives the voltage set-point directly from the tertiary control hosted by SCU and performs the local primary control based on the set points received. The primary and the secondary control of VSC converters irrespective of their operating modes are implemented within the local controller of the VSC converter.

It should be noted that the proposed reliability analysis method can be used for MTDC grid with its control system, irrespective of number of MTDC terminals with appropriate measures to tackle the computational cost in analysing large CTMCs [Buc95][Son99][DHS03]. A detailed failure

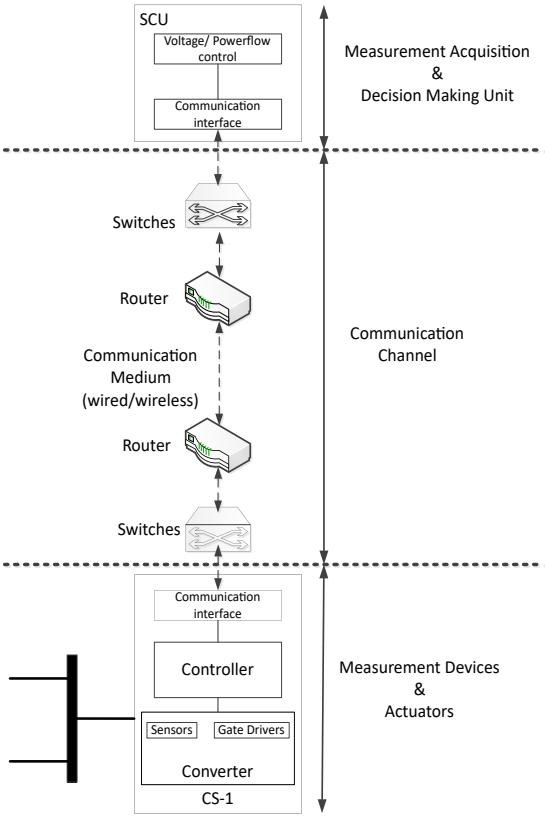


Figure 2.29: Cyber-physical components of MTdc grid

modeling of cyber-physical components and the system failure models based on CTMC are presented in the subsequent sections.

2.6.3 Failure modes of the functional blocks

There are different cyber-physical components involved in the system level control of the MTDC grids. These are:

- Converters and their controllers
- Communication infrastructure
- SCU

These components can be classified into two basic functional blocks, namely the Physical infrastructure and Cyber infrastructure as detailed in subsequent subsections. The reliability of the MTDC grid operation depends on the reliability of its components. Therefore, it is important to define the failure models of the individual components. This study considers that all the components of the system are in a useful period of their life cycle and thus have a constant failure rate. It should be noted that the components mentioned above, that may be just a part of the MTDC grid operation, are also composed of sub-components whose failure rate is a function of its constituting sub-components. The determination of the component failure rate of the MTDC grid components is presented in this section. With the derived component failure rates, the overall reliability of the MTDC grid and its control is quantified. Irrespective of the component being a part of physical infrastructure or the cyber infrastructure, its failure impacts the reliability of the MTDC grid in energizing its loads.

Physical infrastructure failure

The physical infrastructure is the converter station that includes the converter and its controller. The converter functionality is based on the topology of the number of active elements like diodes, switches (IGBT/-MOSFET or power electronic switches), gate drivers,and passive elements like the capacitors and inductors. Furthermore, they would also differ in the switching strategy employed. The second physical component of the converter station is the controller. The converter station ceases to operate if one of these two components fail. The determination of the failure rates of the converter, converter controller, and finally, the overall converter station is given below.

Converter failure model: The authors in [SW13] present a methodology to quantify the reliability of the converter and its MTTF, based on the failure rates of the active and passive components of the converter. The switching strategy of the converter depends upon the design of the topology and the operation scheme of the converter. A CTMC model is developed for different topologies. The reliability of each converter topology and its MTTF is calculated. For our study, we assume that the MTTF of the converter is either known apriori or could be calculated as presented in[SW13]. The failure rate of the i^{th} converter station would be represented in this study as λ_i^C.

Converter controller failure model: The converter controller sub-system consists of microprocessors (like the Digital Signal Processing (DSP) or a Field Programmable Gate Array (FPGA) processor board), sensors and their peripherals, gate drivers (if they are not integrated with switches directly). A detailed analysis of the software and hardware failures of processing boards can be found in [Joh89][Geo17]. In this study, the sensors and gate drivers along with their peripherals are also considered to be part of the Converter Controller Subsystem (CCS). The failure of an individual component is a random event. The subsystem is assumed to fail as soon as any of the individual component fails. Therefore, the probability of the subsystem to fail before time t ($Pr(X_f^{CCS} \leq t)$) is the probability that at least one component fails before time t ($Pr(min(X_f^s, X_f^{gd}, X_f^{p-h}, X_f^{p-s}) \leq t)$). This can be represented as in Eq. (2.97).

$$\begin{aligned} &Pr(X_f^{CCS} \leq t) \\ &= Pr(min(X_f^s, X_f^{gd}, X_f^{p-h}, X_f^{p-s}) \leq t) \end{aligned} \tag{2.97}$$

where X_f^{CCS} is the actual time that the CCS takes to fail and $X_f^s, X_f^{gd}, X_f^{p-h}$ and X_f^{p-s} are the actual time that the sensors, gate driver, processor hardware and processor software fail respectively. Since the component failure time is assumed to have an exponential Probability Density Function (PDF), the failure rate of the subsystem (λ_i^{CCS}) can be calculated as a function of the individual component failure rates as given in Eq. (2.98), based on the law that governs the calculation of minima of a set of random variables with exponential PDF [TB17].

$$\lambda_i^{CCS} = \lambda_i^s + \lambda_i^{gd} + \lambda_i^{p-h} + \lambda_i^{p-s} \tag{2.98}$$

The failure of the i^{th}, sensor , gate driver and processor boards (both hardware & software) of the controllers is a random variable with an exponential PDF having the rate λ_i^s,λ_i^{gd} ,λ_i^{p-h} and λ_i^{p-s} respectively.

Similarly the overall failure rate of the i^{th} converter station (λ_i^{CS}) can be derived as a function of the converter failure rate (λ_i^{C}) and its CCS failure rate (λ_i^{CCS}) as shown in Eq. (2.99).

$$\lambda_i^{CS} = \lambda_i^{C} + \lambda_i^{CCS} \tag{2.99}$$

This simplification is possible with the assumption that the converter station fails when either the converter or the converter controller subsystem fails.

Cyber infrastructure failure

The cyber infrastructure consists of the communication infrastructure and the hardware & software that realizes the SCU of the MTDC grids. It should be noted that not all control strategies employ the cyber infrastructure; however, its reliability should be incorporated in the control strategies. The determination of the data transmission failure rate due to the failure of the communication infrastructure components is explained below. Furthermore, the failure rate of the SCU system is also presented.

Communication infrastructure failure model: Data transmission failure: The purpose of the communication infrastructure is to enable the data exchange between the converter controller and the MTDC grid SCU. Typically, data relaying components (like the router, switches), modems, and the physical communication medium constitute the communication infrastructure. Normally, the physical medium could be Ethernet cables, Optic fibers, Power Lines (for power line communication), or over the air (for cellular and other wireless communication links). The overall failure rate of the data transmission (λ^{DT}) that utilizes r relaying components, m modems, and q physical communication links is given by Eq. (2.100), as per the law for systems with components connected in series [SW13][TB17].

$$\lambda_i^{DT} = \sum_{j=1}^{r} \lambda_j^{R} + \sum_{k=1}^{m} \lambda_k^{M} + \sum_{l=1}^{q} \lambda_l^{PM} \tag{2.100}$$

where λ_j^{R},$\lambda_k^{M}$and λ_l^{PM} correspond to the failure of j^{th} relaying component,k^{th} modem and l^{th} physical medium link respectively.

SCU failure model: A SCU is required depending on the design of the control strategy for the MTDC grids. The main function of the SCU is to provide appropriate control setpoints to the converter controllers based on the measurements received from the converter station. The purpose of the SCU between the converters is to ensure optimal power flow within

MTDC as presented in [HU12], or a strict requirement from the control strategy as presented in [NI99]. Nonetheless, if the SCU is employed, the reliability of the MTDC grid operation would also depend on its reliability. Typically the SCU fails if the hardware that hosts its function fails or the software that implements these functions produces erroneous outputs due to software corruption. The overall failure rate of the SCU (λ^{SCU}) is derived as function of hardware and software failure rates (λ^{SCU-H} & λ^{SCU-S} respectively), as given in Eq. (2.101).

$$\lambda^{SCU} = \lambda^{SCU-H} + \lambda^{SCU-S} \tag{2.101}$$

2.6.4 CTMC models of the functional blocks

The proposed reliability analysis is performed for the control of the three terminal dc grid, as depicted in Fig.2.28. The specific CTMCs of physical infrastructure, communication infrastructure, and supervisory control unit are presented below.

Physical Infrastructure CTMC

The CTMC of the physical infrastructure failure is depicted in Fig. 2.30.The black circle denotes the failure of all Converter Stations (CS). All the other states represent the operational status of the CS in the grid, where the numbers specify the CSs that are operational.The Fig. 2.30 is interpreted as follows, the state (CS-123)corresponds to a state where CS-1,CS-2 and CS-3 are functional, the state transits to CS-12, CS-23 and CS-13 when CS-3,CS-1 and CS-2 fail respectively. Similarly, from states CS-12, CS-23 and CS-13 the system sequentially transit to states CS-1, CS-2 and CS-3 when further CSs fail. Finally, when all the CSs fail the system transits to complete failure state denoted by the black circle.The i^{th} CS failure rate is represented as λ_i^{CS} in the Fig. 2.30. The rate of converter station failure is calculated according to the Eq. (2.99)).

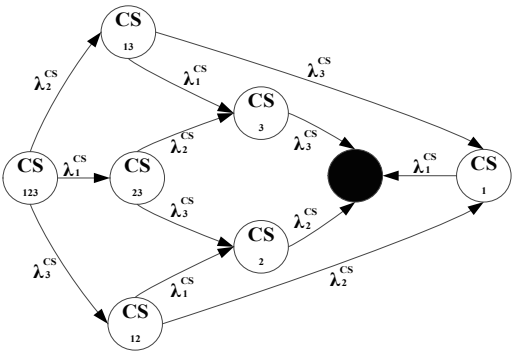


Figure 2.30: Physical infrastructure CTMC

Communication Infrastructure CTMC

The CTMC of communication infrastructure with 3 communication links is depicted in Fig. 2.31. The states(represented as circles) correspond to the set of data transmission links that are functional. The numbers specified in the circles (states) denote the specific DT link that are functional.The black circle represents a system state where none of the DT links are functional. The state transition is triggered by the failure of the i^{th} DT link with a rate of λ_i^{DT}. It should be noted that the failure rate of each DT link is calculated as per the Eq. (2.100). The CTMC model of the

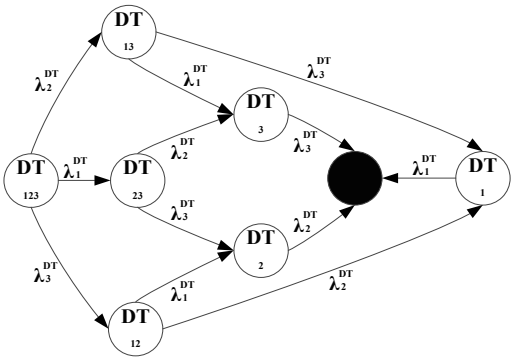


Figure 2.31: CTMC of communication channel infrastructure

communication infrastructure with a single redundant data transmission

link from each CS to the SCU is depicted in Fig.2.32.The Λ_i^{DT} represents the rate at which one of the two DT links between the i^{th} CS and the SCU fails. Such that, $\Lambda_i^{DT} = \lambda_i^{DT-1} + \lambda_i^{DT-2}$, where $\lambda_i^{DT-1}, \lambda_i^{DT-2}$ correspond to the failure rate of the two DT links respectively.This is because when multiple competing transitions (failure of either DT link 1 or DT link 2) trigger the same state transition and when the transition rate is constant (failure event has an exponential probability density function) as in this case then the total transition rate is just the sum of the transition rates [TB17]. It is assumed that both of the links are active and data is sent via one of the links at any point of time.

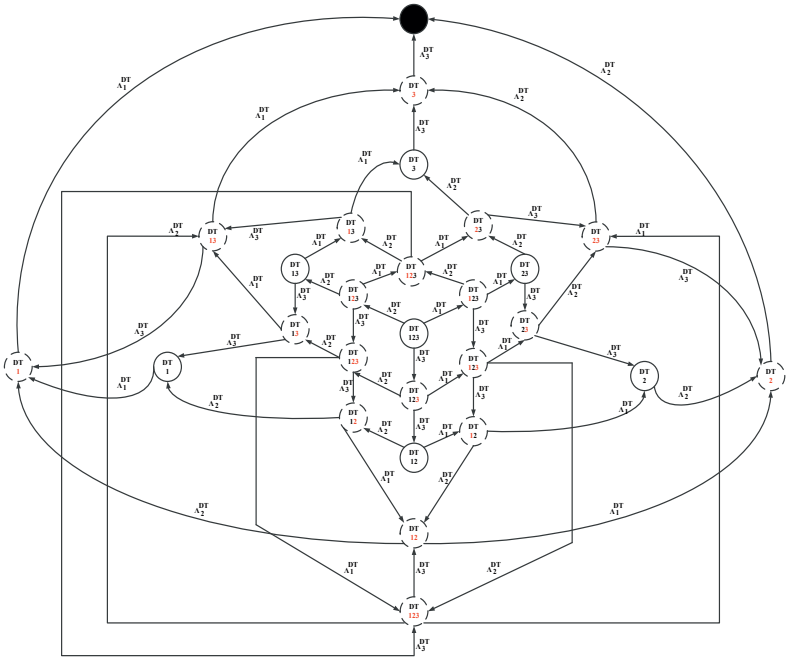


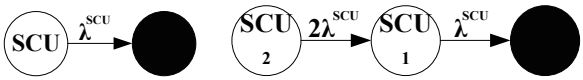
Figure 2.32: CTMC of communication infrastructure with single redundancy of individual DT links

The number in red colour within the dashed circles represent the failure of one of the DT links between i^{th} CS and the SCU. The system transits from a functional state to an intermediary states(represented in dashed circles), when one of the DT link between any CS with the SCU fails.

Only when both DT links fail, the system transits to the next functional state. For the reliability analysis, the probability of occupancy of the intermediary states will be added to the state occupancy probability of the parent functional states from which the transition to the intermediary state was triggered.

SCU CTMC

The CTMC depicting the status of the SCU is depicted inFig. 2.33. The Fig. 2.33a represent the failure of the SCU when only one SCU is deployed for supervisory control of the MTDC grids. If an identical SCU is deployed as a standby SCU then the CTMC of the failure of the SCUs is depicted in Fig. 2.33b.The black circle denotes the failure of supervisory control.



a)Single SCU b)SCU with single redundancy

Figure 2.33: SCU CTMC

2.6.5 Reliability evaluation

As mentioned in Sect. 2.4, the first step in the reliability analysis is to identify the functional blocks. For the case of MTDC grid operation all the three functional blocks, namely, the measurement acquisition, measurement data processing and decision making and the actuation of the control action are involved. However, the physical infrastructure (CS) and the communication infrastructure (Data Transmission links) are responsible for both the measurement acquisition and actuation of control action. The CTMC failure models of the physical and cyber infrastructures is shown in Fig. 2.34 form the multi layered failure model of the MTDC grid operation. The physical infrastructure failure model and the communication infrastructure failure model together determine the reliability of the measurement acquisition and control command actuation functional block as the same components are used for both functional blocks. The states in the physical infrastructure represent the collective operational status of all the converter stations that form the MTDC grid. The arcs represent the failure of a specific converter station. The failure rate of the specific converter station is as calculated in Eq. (2.99). Similarly, the states in the communication infrastructure CTMC represent

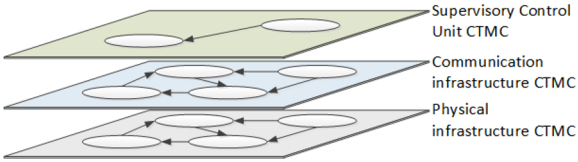


Figure 2.34: Multi-Level CTMC model for cyber-physical system reliability analysis

the collective operational status of the communication links from all the converter stations to the SCU. The arcs in this CTMC model represent the failure in data transmission, as calculated in Eq. (2.100). Finally, the two states in the SCU CTMC model correspond to the status of the component that hosts the algorithms/functions of the SCU.

The next step in calculating reliability of the MTDC grid operation is to calculate the reliability of the functional block , measurement aquisiton and control command actuation, for which, the MDRM has to be built. To build the MDRM, the dynamic state occupancy probabilities of the physical and the communication infrastructures need to be calculated as per the equations Eq. (2.10)-Eq. (2.16). The states in each CTMC model, represent the operational status of the components in each infrastructure. This means that the states also represent the failure configuration of the components in each infrastructure. Therefore, in order to evaluate the reliability of the CPS MTDC for physical and communication infrastructure failure configuration, the individual CTMC has to be initialized with appropriate entry of $\boldsymbol{\pi}_i(0) = 1$ that corresponds to i^{th} failure state, and all the other entries to 0 while calculating the dynamic state occupancy probabilities of the physical. The equations Eq. (2.102)-Eq. (2.103) represent the transient probabilities of the two infrastructures being in any of the failure states, that are responsible for realising the specific functional block.

$$\boldsymbol{\Pi}^{PH}(t) = [\pi^1_{ph}(t), \pi^2_{ph}(t)..., \pi^M_{ph}(t)] \tag{2.102}$$

$$\boldsymbol{\Pi}^{CM}(t) = [\pi^1_{cm}(t), \pi^2_{cm}(t)..., \pi^N_{cm}(t)] \tag{2.103}$$

Similarly, the probability of the SCU could also be calculated. The transient state occupancy probability for the SCU is as shown in Eq. (2.104).

$$\boldsymbol{\Pi}^{SCU}(t) = [\pi^{up}_{scu}(t), \pi^{down}_{scu}(t)] \tag{2.104}$$

The MDRM, a MxN matrix, is constructed as given in Eq. (2.105). It is a compact representation of all possible combination of operational

states of the communication and physical infrastructure. Each element in MDRM represents the probability of being in the multi-domain operation state.

$$\boldsymbol{MDRM}(i,j)(t) = \boldsymbol{\Pi}^{PH}(i)(t) * \boldsymbol{\Pi}^{CM}(j)(t) \tag{2.105}$$

It should be noted that a set of the multi-domain operation states (entries in MDRM) could be categorized into performance classes that denote the health of the operation, for which mapping of the entries in the MDRM to specific performance classes needs to be predefined. If there are k performance classes defined by the operator, then the final probability of the system being operated in a specific performance class is given by the Eq. (2.106).

$$\begin{aligned} \boldsymbol{\Pi}_k^{Performance-Class}(t) &= \sum_{i=1}^{M}\sum_{j=1}^{N} \boldsymbol{MDRM}(i,j)(t) \\ &\forall (i,j) \in k^{th} class \end{aligned} \tag{2.106}$$

The reliability of the functional block is the probability of being in one of these aforementioned performance class or in a set of them. It is calculated as a function of $\boldsymbol{\Pi}_k^{Performance-Class}(t)$ as given in Eq. (2.107).

$$\begin{aligned} &\boldsymbol{R}_{\boldsymbol{MA-CA}}^{\boldsymbol{FB}}(\boldsymbol{t}) = \sum \boldsymbol{\Pi}_i^{Performance-Class}(t) \\ &\forall\,(i) \in Set(Reliable\ operation\ mode) \end{aligned} \tag{2.107}$$

The selection of performance classes to be considered as one of the reliable operation modes is at the discretion of the grid operator. The criteria for this selection can be based on the cost of energy not supplied due to converter station failure,total energy loss or on other standard power quality metrics that the operator must adhere to. The analysis of such a selection criteria is out of the scope for the current study. Finally the overall reliability of the cyber-physical MTDC grid operation is then given by the Eq. (2.108). Therefore, the reliability of the functional block (responsible for measurement acquisition and control command actuation) and the reliability of the SCU is combined to derive the overall reliability of the MTDC grid operation.

$$\begin{aligned} \boldsymbol{R}_{\boldsymbol{MTDC}}^{\boldsymbol{CPS}}(\boldsymbol{t}) &= \prod_i \boldsymbol{R}_{\boldsymbol{i}}^{\boldsymbol{FB}}(\boldsymbol{t}) \\ &= \boldsymbol{R}_{\boldsymbol{MA-CCA}}^{\boldsymbol{FB}}(\boldsymbol{t}) * \pi_{scu}^{up}(t) \end{aligned} \tag{2.108}$$

where, $\boldsymbol{R}_{\boldsymbol{MTDC}}^{\boldsymbol{CPS}}(\boldsymbol{t})$, is the reliability of the cyber-physical MTDC grid, $\boldsymbol{R}_{\boldsymbol{i}}^{\boldsymbol{FB}}(\boldsymbol{t})$ reliability of each functional block and $\boldsymbol{R}_{\boldsymbol{MA-CCA}}^{\boldsymbol{FB}}(\boldsymbol{t})$ is the

reliability of the functional block responsible for Measurement Acquisition and Control Command Actuation. Apart from the reliability, additional performance indices like the Energy Not Supplied (ENS) can also be calculated as shown in Eq. (2.109), where ξ_k^{P-C} is the percentage of load demand that was not met due to the failure configuration of the converter station corresponding to the k^{th} performance classes.

$$ENS(t) = \sum_{i=1}^{k} \xi_k^{P-C} \mathbf{\Pi}_k^{Performance-Class}(t) * \pi_{scu}^{up}(t) \tag{2.109}$$

In the upcoming section detailed CTMC models of the CPS of a three terminal dc grid is presented. The specific selection of performance classes and the mapping to MDRM is also explained. Furthermore, key performance indices based on the reliability of the CPS calculated as per equations Eq. (2.102)-Eq. (2.108) would be presented in the subsequent subsections.

2.6.6 Test scenarios and Results

For the exemplary three terminal MTDC grid, its reliability evaluation is provided in this subsection. Furthermore, the impact of a redundant SCU and DT links in the reliability of the control of the cyber-physical MTDC grid is presented.

Test Parameters : Failure rates of physical infrastructure components

Different failure rates are assumed for the different CSs and they are $\lambda_1^C = 0.000003hr^{-1}$, $\lambda_2^C = 0.00003hr^{-1}$ and $\lambda_3^C = 0.000001hr^{-1}$.The failure rate of controller hardware (λ^{p-h}), controller software (λ^{p-s}), sensors (λ^s) and gate driver (λ^{gd}) are assumed to be of reliability class R3 as per the IEC 60870-4 standard [IEC90], where $\lambda^{p-h} = \lambda^{p-s} = \lambda^s = \lambda^{gd} = 0.00001hr^{-1}$. Thus the failure rate of the i^{th} CS as per equations Eq. (2.98)-Eq. (2.99) is given as $\lambda_1^{CS} = 0.000043hr^{-1}$, $\lambda_2^{CS} = 0.00007hr^{-1}$ and $\lambda_3^{CS} = 0.000041hr^{-1}$.

Test Parameters : Failure rates of communication infrastructure components

Each DT link between the CSs and the SCU is assumed to be composed of non identical number sub-components. The first DT link is composed of two modems, four relaying components, and seven physical medium links and the redundant DT link is composed of two modems, one relaying component and four physical medium links. These components are assumed

to be of class R3 as per the IEC 60870-4 standard [IEC90] with the failure rates $\lambda^R = \lambda^M = \lambda^{PM} = 0.00001hr^{-1}$. Hence the overall DT link failure rate can be calculated as per Eq. (2.100) as$\lambda^{DT-1} = 0.00013hr^{-1}$ and $\lambda^{DT-2} = 0.0007hr^{-1}$. Furthermore the failure of redundant DT links is $\Lambda^{DT} = \lambda^{DT-1} + \lambda^{DT-2} = 0.00020hr^{-1}$. Here same DT links configuration has been assumed for all DT links of the system . However, they can be assumed different which might impact the overall reliability. For the test case without the redundant DT link the failure rate of the DT link between the CS and SCU is considered to be equal to the failure rate of Λ^{DT-1}.

Test Parameters : Failure rates of SCU infrastructure components

The hardware and software of the SCU is assumed to be of R3 reliability class [IEC90], with failure rates of the SCU $\lambda^{SCU-H} = \lambda^{SCU-S} = 0.00001hr^{-1}$ respectively.The total SCU failure rate is $\lambda^{SCU} = 0.00002hr^{-1}$ as per Eq. (2.101).

Definition of Performance Classes and Reliable set

The specific performance classes that are being considered as stable operation condition has to be specified. The exact rule for the assignment of a specific PC to be reliable is out of the scope of this study. However, an exemplary rule has been presented just to show the process of evaluation of the reliability of MTDC grid operation. For the test case considered, four PCs are defined. PC-1 corresponds to the operational state where all the three CSs, their corresponding DT links to the SCU, and SCU are operational. The percentage ENS in this case is zero. It means that the complete MTDC grid is controllable. PC-2 corresponds to the operation condition where any two of CSs are operational along with their DT links to SCU, and the SCU is operational. It is a sub-optimal operational status of the MTDC grid where 66% of energy demand is met (33% ENS). PC-3 corresponds to a least performing condition where only one of the CSs, its DT link to SCU, and SCU are functional where only 33% energy is met (66% ENS). All the other operational condition is considered to be failure of the three terminal dc grid operation and represented as belonging to the PC-4 with 100% ENS. For calculating the reliability of the MTDC grid control, the PC-1 is considered as the only reliable operation mode.

Test Scenario 1: No redundancy

The reliability of the three terminal dc grid with a single DT link per CS with a single SCU is calculated. The probability of being in the

four performance classes (PC1-PC4) as a function of time is depicted in Fig. 2.35. The reliability of the MTdc grid control without any redundancy

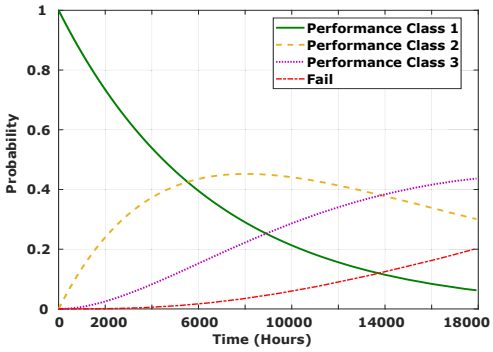


Figure 2.35: Probability of MTDC grid control in being in different Performance Classes

measures taken for the DT links and SCU is shown in Fig. 2.37. The overestimation of the system reliability deduced based on the reliability of just the physical infrastructure of the converter station is depicted in the blue line in Fig. 2.37. The MTTF of the MTDC grid control is tabulated in Tab. 2.14, which is calculated as per Eq. (2.5).

Test Scenario 2: DT redundancy

In this scenario, a redundant communication link for every DT link between the CS and SCU is considered. With just a single redundant DT link the total time that the communication infrastructure has all the DT links functional between the CSs to the SCU almost doubles as shown in Fig. 2.36 as calculated as per Eq. (2.17). The reliability of the MTDC grid control and its MTTF with redundant DT links is shown in Fig. 2.37 and in Tab. 2.13 respectively. It can be observed that the reliability of the MTDC grid control increases and so the mean time to its failure.

Test Scenario 3: DT & SCU redundancy

In this scenario a redundant SCU is employed for the supervisory control so that if one of the SCU fails the redundant SCU takes over its functions and provides control set points to the CSs. The improvement in the availability of the SCU can be seen by comparing the mean failure time

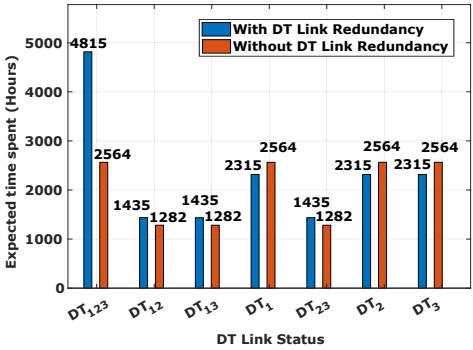


Figure 2.36: DT link reliability with and without redundancy

Table 2.13: MTTF and Availability of MTDC grid control : Impact of DT and SCU Redundancy

Scenario	1	2	3
Availability (in%)	99.62	99.69	99.77
MTTF (Hours)	2645.8	3312.2	4503.1

of SCU with and without redundancy as shown in Tab. 2.14. The availability is calculated considering the mean time to recover to be 10 hours. The service level agreements define the availability in terms of number of '9's in the availability. It can be seen that with redundancy of SCU, its availability was improved by one class higher with three '9's from two '9's availability class. A comparison of the MTDC grid control reliability for all the three cases is shown in Fig. 2.37. It can be noted that the reliability increases with the redundancy of the DT & SCU links. Furthermore, the same trend can be deduced from the comparison of the

Table 2.14: MTTF and Availability of SCU with and without redundancy

Scenario	1	3
Availability (in%)	99.8 hr	99.9 hr
MTTF (Hours)	5000	7500

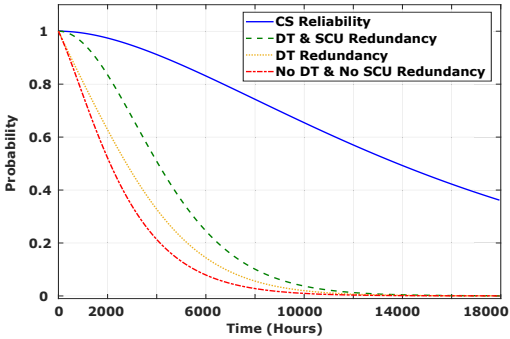


Figure 2.37: MTDC grid control reliability:Impact of DT and SCU redundancy

availability considering a mean time to recovery of 10 hours for the MTDC grid control is tabulated in Tab. 2.13.The percentage ENS as a function of time is shown in Fig. 2.38. The system with the redundancy measures performs better.

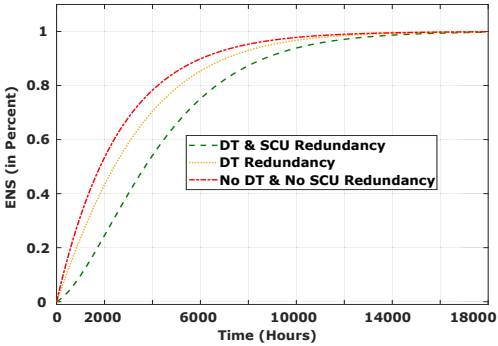


Figure 2.38: Percentage ENS as a function of time :Impact of DT and SCU redundancy

Conclusions

From the results presented, it is shown that the proposed methodology can be used to evaluate the reliability of the CPS MTDC grids and compare the effects of different redundancy measures of the cyber infrastructure. It is seen that, compared to the MTTF of a single physical component (ranging till ≈10 years) the overall mean failure time of the MTDC grid is really low (≈ half a year). This can be attributed to the relatively higher failure rate assumed for the cyber infrastructure (in comparison to the failure rate of the converter components) and the complex interdependence of the failures modelled via the multi-layer CTMCs. Therefore, the proposed methodology helps to avoid the over estimation of the reliability of MTDC grids by also considering the reliability of cyber components and their indirect impacts on the overall system failure. Additionally the ENS and the availability can be easily derived from the standard performance measures of CTMC and MDRM. The proposed methodology is also suitable for systems that have complex failure and recovery processes of the physical, communication and supervisory control infrastructure of the MTDC grid, as they can be modelled by individual complex CTMC models. Thus facilitating the modelling of more complex cyber-physical infrastructure, but still use the same MDRM based procedure for quantifying its reliability. Therefore, the proposed methodology can also be used when Converter Station itself is considered as a cyber-physical system, where the sensors, controllers and gate drivers interact with each other using a high speed Local Area Network(LAN). Thus the proposed method, with multi-layered

CTMC model and the MDRM matrix, is modular and provides a generic framework that can be used to study the reliability of cross domain complex systems, where in the failure of each domain is modelled as a CTMC.

2.7 Conclusion

In this chapter examples have been presented to show the applicability of the proposed methodology using CTMC and the MDRM for evaluating the reliability of the DGA systems. The complete DGA system under study is divided into different functional blocks to combat the state explosion problem of using state space based reliability evaluation methods. With the first test case, it is shown that the ICT infrastructure influences the reliability of the DGA system and the redundancies in it impacts the overall reliability of the DGA system. The calculated reliability is then used to calculate overall cost of unavailability of the system using the Markov Reward Models. In the second test case, a complex heterogeneous DGA system for monitoring distribution grids is presented. Heterogeneous communication infrastructures (Ethernet, PLC and LTE) failure models have been modeled. The monitoring system of the DGA system based on IDE4L automation architecture has been considered for this test case. The division of the DGA system into mutually exclusive and collectively exhaustive Functional Blocks is presented. Using MDRM and the detailed failure models of the individual components within the Functional Block, the reliability of each functional block is evaluated. Finally the overall reliability of the DGA system as a function of reliability of he individual functional blocks is presented. The main purpose of the second test case is to present the applicability of the proposed methodology to model the failure characteristics of a complex heterogeneous automation function realisation.

2.8 Scope of proposed methodology

In the current study, random failures of the components have been considered. The common mode dependant failures of components that are part of the same functional block are also considered within the proposed framework, however common mode failures that impact components of multiple functional block currently have not been considered. Such failures are catastrophic in nature and are generally considered as High Impact with Low Probability (HILP) events (like natural calamities or wide range terrorist attacks). The inclusion of such HILP events in the reliability calculation would enable the system designer a comprehensive idea of the

reliability of the system. The proposed methodology should be extended to study the impact of such HILP events to design appropriate resilience measures. Current study assumes an exponential distribution of the cyber and physical components of the DGA system, however, this assumption is valid only for components that are considered to be in their prescribed operational time, however for cost optimization the DGA infrastructure might be operated beyond their prescribed operational times and thus failure characteristics considering the ageing of the devices must be considered. One of the interesting extensions of this work is to perform a Global Sensitivity Analysis (GSA) to identify the weakest link in the DGA system. With GSA the variation of the overall reliabiliy as a function of the variance of the failure rates of components of each automation device could be evaluated. This enables the system designers to prioritize their investments in improving the system reliability either by introducing redundancies or replacing the devices with more reliable components. Another extension that is really interesting is to use the MDRM and the CTMC models of the cyber and physical components to identify the availability of each combination of the availability the cyber and physical components. If we represent these state as individual CTMC states of the combined system and perform a power flow of the grid considering the impacts of the availability of subset of the components, the avarage powerflow/energy supplied/not supplied could be evaluated in detail. Such a modelling allows the evaluation of the impact of failure of communication infrastructure (discrete time domain) on to the power flow (which is in continuous time domain).

3

Susceptibility of DGA systems

3.1 Introduction

The digitization of technical and business operations of the DSOs is evolving quickly. The EU report lists use cases leveraging on digitization, taken from many current EU large projects and demonstrations. For example, the project IDE4L [Rep+17] has produced a full automation architecture based on digitization, which supports advanced functionalities like local state estimation in MV and LV grids, fault location and service restoration, and cooperation of the DSO with Aggregators, TSOs and third party providers. The architecture, thats is based on IEC 61850 standard series has been successfully demonstrated in the field and is predicted to be deployed for distribution grid automation in the next decade [MP16]. Furthermore, the EU commission on 30^{th} November 2016, had published the winter package, that proposes the establishment of distributed energy markets enabling the entry of new participants like the Prosumers and smaller renewable energy generating entities in the energy exchange [Coma][HW17]. This initiative encourages energy exchange within a neighbourhood and thus requires a complete distributed operation and control of distribution grids, for which heavy integration of ICT infrastructure is needed. In the pursuit of digitizing the distribution grids, much more futuristic schemes for the control and automation of the distribution grids are now being explored, involving the smart meters /controllers and Cloud ([FLE],[NRG]), Edge computing using 4G and 5G communication systems ([SUC],[ESA],[NRG]), the Future Internet and Blockchain based platforms([FIS], [PLA]) [MP16].

The digitization with advance ICT infrastructure provides flexibility in data management and configuration of the automation system. It enables the design of communication intensive grid control schemes and thus optimize the control functions. It also facilitates real time condition monitoring and triggering of associated preventive maintenance measures and failure diagnosis. Though digitization has so many benefits, it in-

troduces additional vulnerabilities in the automation of the distribution grids, as different ICT components would be installed at the end customer, distributed energy producers, network service providers, network operators and market entities. This is because, digitization increases the complexity of the distribution grid automation systems and the cyber-physcal security concerns due to the diversified ownership of the devices, varied access rights and role management, patch management procedures followed, and cyber-security management systems deployed. Such a system is highly susceptible to malicious attacks. These attacks not only compromise the integrity and confidentiality of the devices involved in the automation of the grid but also hamper the availability of the complete automation system. Traditionally, the malicious attacks on grid automation systems can be classified into two categories:

- Physical attacks target the power system components such as transformers, generators and transmission lines to alter the power flow that might create power outages, cascading failures [SWB04], [Che+11] and finally a blackout. An example of a physical attack on the California transmission substation by sniper is provided in [Smi14]. The drones were used to drop bombs on the critical infrastructure and cause physical damages. A large number of drone based attacks have been reported by the critical infrastructure owners in middle east [CD20].

- Cyber attacks target the Supervisory Control And Data Acquisition (SCADA) system to disrupt the power system operation, which can cause direct/indirect economic losses and are relatively difficult to detect if the attack vectors are well structured. An attack vector is a method or pathway used by an intruder (hacker) to access or penetrate the target system. An example of the cyber attack on the Israel Electricity authority by a computer virus infection is presented in [The16].

Recently, a new category of threats to all critical infrastructures named Coordinated Cyber-Physical Attacks (CCPA)s are emerging, in which cyber attacks are used to mask physical attacks [DZL17]. The stealth nature of the cyber attacks and outages caused due the physical attacks makes the CCPAs detrimental attacks compared to the traditional ones. The December 2015 attack on the Ukrainian electrical grid is an example of such a CCPA, which opened several circuit breakers (i.e., the physical attacks) to cause approximately 225,000 customers to lose power [Rob16]. During the attack, telephonic floods and the KillDisk server wiping (i.e., the cyber attacks) were used to cover up the emergency and prolong the outages

[Rob16]. A number of countermeasures have been proposed to minimize the risks of the CCPAs. Several countermeasures have been proposed in the literature as defenses against cyber-physical attacks on power systems [KB21],[Zog+21],[ZLW21],[Hum+17]. The authors in [Liu+18a] propose a method to detect and mitigate insider cyber threats. A review of different cyber security standards that govern the cyber security requirements for a secure smart grid is provided in [Hus+18]. Among the different cyber security standards the IEC 62351 series and the IEC 62443 standards are noteworthy. The former provides measures to improve the cyber security of the traditional communication protocols used for data exchange for protection, control and monitoring of the power grids. A detailed review of the measures prescribed in IEC 62351 for IEC 61850 based grid automation has been presented in [HUK20]. The later provides the complete set of procedures that automation device manufacturer, the system integrator and the infrastructure owner should follow in order to maintain the prescribed level of security against cyber attacks through periodic device checks, standardized patch management, periodic security training for operating personals and so on. A review of the IEC 62443 standard and its application is provided in [Pig13]. In addition to the CCPAs, due to the advancements in the drone technology, new attack vectors that cause physical damage to the critical infrastructure are also on the rise [CD20]. The availability of the critical infrastructure has been found to be hampered due to frequent and devastating drone attacks in the middle east [CD20]. An image analytics based countermeasure against drone attacks has been presented in [Tzo19].

It is crucial to assess cyber and physical security risks, for providing an effective guidance on the design and operation of critical systems. The quantification of the security risks entails the evaluation of the threat propagation. With a proper modelling of the threat propagation, the system availability can be evaluated so that appropriate countermeasures may be chosen to effectively enhance it. Thereby, promoting the response to unexpected security attacks on to the critical infrastructure. However, it should be noted that, based on the skill of the attacker to launch a cyber-physical attack, the physical and cyber vulnerabilities of the devices and the personnel involved in critical infrastructure operation, are exploited differently. This introduces uncertainty in the attack launch and its propagation. Hence while modelling the threat propagation, the uncertainty in the attack propagation need to be considered. Additionally, due to the uncertainty of the threat propagation, no countermeasure can be assumed to provide complete security against all kinds of cyber-physical attacks, but can safely be assumed that they reduce the risk of it.

For this study, the availability of the DGA is quantified considering the countermeasures deployed, all possible vulnerabilities of the components of the automation system, their exposure, and their exploitability. Such quantification of the threat propagation helps in the evaluation of the susceptibility of the DGA infrastructure to cyber-physical attacks. Furthermore, by studying the possible threat propagation, the infrastructure owners could identify the bottlenecks in the DGA system defenses and evaluate the effectiveness of the countermeasures. Such evaluation helps in fortifying the defenses and thus improve the availability of the DGA systems.

Therefore, in this study a probabilistic threat propagation analysis method is proposed that incorporates the following aspects, which have not been comprehensively addressed in the literature before:

- Dependence of the different attacks (e.g sequential, concurrent etc)
- Uncertainty and frequency of occurrence of an attack event
- Uncertainty in launching time of an atomic attack (atomic attack step)
  - Level of vulnerabilities
  - Degree of exploitation of these vulnerabilities
  - Skill of the attacker
- Effectiveness of a countermeasure
- Time/ Rate of countermeasure actuation

The proposed analysis method starts with a definition of the threat scenarios as an attack tree, where, the attacks are the leaf nodes, the goal of the attack is the root node and the sub-goals are the rest of the other nodes in the tree. The attack tree is a graphical illustration of the logic of the propagation of an attack. However it is static and can not be used for analysing sequential and/or concurrent attacks. Therefore, the attack tree is re-modelled as a Petri net. From the Petri net a reachability graph is generated that shows all possible attack paths with appropriate frequency /attack times. The reachability graph of the attack tree is then considered as a state transition graph of a Markov Chain. Where the states represent the attack status (reaching sub-goals, reaching root nodes) and transitions represent the probability of launching a step of the attack. Indices like the probability of reaching a attack sub-goal, time spent in different sub-goals and the mean time to reach the root node can then be calculated using the

CTMC formalism. The indices can then be used by experts to evaluate the risk of the attack and compare the effectiveness of the countermeasures. The major features and indices that the proposed methodology helps in analysing are as given below:

- Considers attack tree as input (easy for non experts to identify vulnerabilities and impacts)
- Converts attack tree to Petri net and generates the reachability graph (To model attack dependencies)
- Analyses the reachability graph as CTMC state transition graph and calculate the indices for quantifying the risk of the attack propagation by incorporating the following parameters in the model:
  - Uncertainties in attack event occurrence and attack launch time
- Incorporates the countermeasures in the Petri net model whose reachability graph is then analysed for evaluating the impact of the countermeasure using the CTMC formalism and incorporating the following parameters :
  - Effectiveness of a countermeasure
  - Time/ Rate of countermeasure actuation

3.2 Procedure for threat analysis

A critical infrastructure, like the DGA, is susceptible to both physical and cyber threats. A set of definitions are provided below that might be useful to follow the upcoming section on the threat propagation analysis.

- **Asset** is a component of an infrastructure, that could be of cyber, physical or cyber-physical in nature. In the context of DGA and electric power systems, an asset could be a hardware, a software or a physical component like transformers, buildings, secure doors etc.
- **System** is a set of assets that form a part of the infrastructure.
- **Threat agent** is an entity or an incident that has the potential or the intent to harm a system.
- **Threat** is the combination of a threat agents and the potential impact it may lead to or the goals that the threat agents might achieve.

- **Vulnerability** is a gap or a weakness of an asset/system that might be exploited. Vulnerabilities provide a path for a threat agent to achieve its goals.
- **Attack vector** is the path taken by the threat agent to reach the attack goal.
- **Atomic attack** is the single step in the attack vector.
- **Threat scenario**: is the combination of a subset of threat agents and their associated attack vectors.
- **Disutility** is the result of a stakeholder's assessment of a given impact.

The flowchart depicting the different steps of threat analysis of a critical infrastructure with different assets, is shown in Fig. 3.1.

The threat analysis is carried out in the design phase of a critical infrastructure. It is also triggered whenever a new asset is added to the infrastructure or new security threats are found during the periodic, mandatory, security risk assessment of the critical infrastructure. These periodic security risk assessments is typically recommended by standards that provide guidelines for vulnerability and threat analysis of a critical infrastructure, to ensure continuous evaluation of the security risks from evolving threats and threat agents [Comc], [Com09],[Com10],[Com15].

It is evident that to define a threat scenario, a thorough investigation has to be made to list out the assets involved in the operation of the infrastructure, their vulnerabilities, degree of exposure, exploitability of the vulnerabilities, possible threat agents and the associated attack vectors . Such a thorough investigation helps in defining the threat scenario accurately, which increases the accuracy of the threat propagation analysis. Different methods have been proposed in the literature to identify and define the threat scenarios (Step 2 - Step 6). Some of the noteworthy methods specifically proposed for identifying cyber threat scenarios are STRIDE [Pra], PASTA [UM15], LINDDUN [Iza21], SPARTA [Iza21], CVSS [IS] and the adaptation of the KillChain methodology (originally used as a military concept related to the structure of an attack) as Cyber KillChain methodology. As the Kill Chain is successful at describing attack vectors and attack agents, its being heavily used for modelling not only physical attack vectors but also cyber attack vectors, thus enabling the modelling of cyber-physical attack vectors [Cho+18],[MA16].

The threat scenarios defined, then form the basis for modelling the threat propagation. Different formalisms have been proposed in the literature for

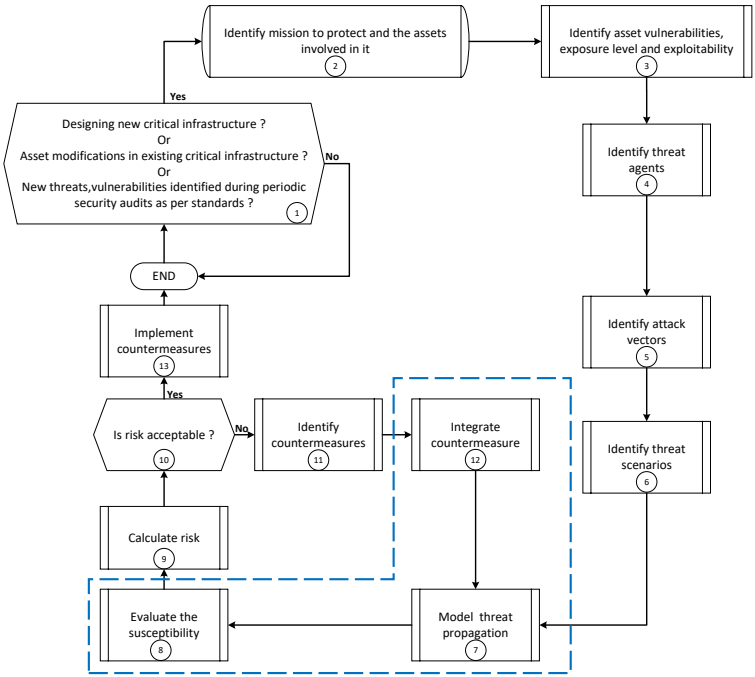


Figure 3.1: Threat analysis flow chart

modelling the threat propagation, that enables quantitatively evaluate the propagation. A detailed overview of the threat modelling methods have been provided in the Sect. 3.3. Using the threat propagation models the susceptibility of the system to the attack agents is evaluated.

The main goal of the suscpetibility analysis is to estimate the likelihood of achieving the attack goals, given that the threat scenario is defined, that maps the threat agents to the attack vectors. The risk of a given threat refers to the "expected disutility". The susceptibility of the system to specific threat agents, is a combination of disutility and the estimated likelihood. It is a measure that is expressed as the likelihood of a disutility being realized. The likelihood may be based on the ability/capacity of a threat agent, exploitability of the existing vulnerabilities and on the effectiveness of the deployed countermeasures (offline and online). A

detailed explanation of the indices used to quantify the susceptibility of the system to the threats is provided in Sect. 3.5.5.

There is always a cost associated to any specific disutility of the system/asset. The estimation of the likelihood of disutility (or the susceptibility) helps in estimating the cost associated to the degrees of disutility and thus evaluate the risk of the susceptibility of the system/asset to threat agents. Once the risk is evaluated and if its found not to be acceptable then appropriate countermeasures are selected. The countermeasures are integrated into the threat propagation model and the suceptibility is re-evaluated and the associated risk is calculated. this process is repeated till the risk calculated is within the acceptable levels. Once the risks calculated are found acceptable then the countermeasures that allow the reduction in the risk are implemented.

A new threat analysis cycle begins only when any new modifications to the infrastructure is made or new threat agents and associated attack vectors have been identified during the periodical security audits of the system, else the threat analysis cycle ends.

the scope of the study is just limited to proposing methodologies for performing the steps 7,8 and 12.

3.3 Threat propagation indices: Susceptibility indices

The evaluation of the threat propagation indices helps in understanding the susceptibility of the infrastructure to the cyber-physical threats. The different threat agents exploit the vulnerabilities and the degree of exposure of the assets to reach specific attack sub-goals and eventually to the main goal. For a given set of information about the threat scenario, namely:

- Threat agents and their respective Attack vectors.
- Identified sub-goals and the root goal of the attack.
- Probability of launch of single atomic attack step based on:
  - The exploitability of the vulnerability.
  - The uncertainty on the time of launch of an attack (reflects the skill of the attack agent)

The susceptibility of any infrastructure can then be evaluated by calculating the different threat propagation indices. The major threat propagation indices are as given below.

- Indices for the perception of threat state

  - Probability to reach a specific threat state (main goal/ sub-goal/Set of sub-goals): helps in devising procedural countermeasures
  - Threat state evolution as a function of time: it is the probability of reaching the different threat states as a function of time. Helps in devising near real time actuation of the emergency countermeasures. Specifically useful for tackling physical threats like the autonomous drone attacks where multiple options of countermeasures are available with varying actuation times and threat reduction capabilities.

- Indices for the perception of temporal aspects of threat evolution.
  - Time to compromise (time to reach the main attack goal): helps to prioritise different countermeasures that have different actuation times.
  - Time spent in sub-goals: helps in the calculation of the risk of the threat. The sub-goals/Set of sub-goals, when reached, represent a partially available system. The cost associated to the different threat states might be different. Therefore, by analysing the time spent in different threat states (before the final goal is achieved), appropriate countermeasures could be chosen in such a way that the time spent in the most costlier threat states are minimised.

3.4 Modelling threat propagation: Review

3.4.1 Modelling formalism: Attack Tree

There are different methods proposed in the literature that help in modelling the threat propagation [Pat+18],[Hu+17],[Gha+],[WTW16],[XDX15]). However, the most basic and widely used methodology, as it is simple and graphically presentable, is the attack tree [TB17]. Effectiveness of threat propagation modelling techniques in terms of attack perception highly depends on its visual aspect [LDB18]. This is true for both experts, such as operators and engineers who are required to make decisions in real time, as well as for non-experts, such as managers who make decisions for long term planning. One of the effective visual methods to show describe the threat propagation is the attack trees. Wherein, the events that lead to an attack goal is represented in a tree structure [Sch99].

The attack tree represents an attack against the system, in a tree structure, where the goal of the attack is the root of the tree and the

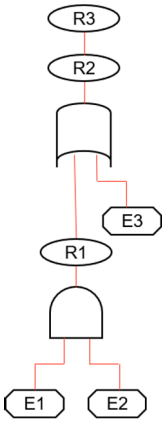


Figure 3.2: Attack Tree Example

different sub-goals are represented as child nodes and the initial launch of the atomic attack events represented as leaf nodes. An exemplary attack tree is shown in Fig. 3.2. E1, E2, E3 depict the atomic attack events which are represented in the figure as leaf nodes. These events could be launched by different attack agent or the same attack agent. R1 is the child node that represents an attack sub-goal. R2 is the root node of the attack tree that represents the main goal of the attacker. The attack trees helps in visualising how different atomic attack steps interact. Additionally, the different attack vectors could be also graphically identified. Furthermore, for a given probability of occurrence of the leaf nodes/child nodes the probability of occurrence of the corresponding parent node ($Pr_{P_{node}}$) that is logically associated with its child nodes/leaf nodes. The probability of occurrence (reaching) of a parent node which is associated with its child nodes/leaf nodes in such a way that all its child nodes/leaf nodes should occur/reached (logical AND) can be calculated as shown in Eq. (3.1). The $P^i_{C_{node/L_{node}}}$ corresponds to the probability of occurrence of the i^{th} child/leaf node that is associated with the k^{th} parent node.

$$Pr^k_{P_{node}} = \prod_{i=1}^{N} (P^i_{C_{node/L_{node}}}) \tag{3.1}$$

The probability of the k^{th} parent node ($Pr^k_{P_{node}}$) that could occur when any of the child/leaf nodes occur (logical OR) can be calculated as shown in Eq. (3.2).

$$Pr^k_{P_{node}} = \sum_{i=1}^{N} (Pr^i_{C_{node/L_{node}}}) \tag{3.2}$$

By using these two equations (Eq. (3.1),Eq. (3.2)) the probability of occurrence of the root node can be recursively calculated from the leaf nodes to the root node. It should be noted that the aforementioned equations are valid when the child nodes are not shared by more than one down stream parent node, in which case the disjoint cut-sets have to be identified and the probability of the parent node can be calculated as a function of occurrence of the cut-sets as shown in Eq. (3.3), Eq. (3.3). Where the P^i_{Cutset} can then be calculated as a function of the probability of occurrence of independent child/leaf nodes as shown in Eq. (3.5) [TB17]. There are different methods proposed to find the cut-sets [TB17].

$$Pr^k_{P_{node}} = \prod_{i=1}^{N} (Pr^i_{Cutset}) \tag{3.3}$$

$$Pr^k_{P_{node}} = \sum_{i=1}^{N} (Pr^i_{Cutset}) \tag{3.4}$$

$$Pr^k_{Cutset} = \prod_{i=1}^{N} (Pr^i_{C_{node/L_{node}}}) \tag{3.5}$$

As explained before, the security assessment of attack trees to determine attributes such as cost and probabilities of reaching the root node is performed based on a bottom-up procedure [PB10]. However, the bottom-up approach is valid only if all transitions are independent. Furthermore, the attack tree based methods mostly focused on the amount or frequency of different and independent system vulnerabilities or atomic attack events. In practice, however different hazardous events may take place in a dependent manner, i.e, the occurrence of one atomic attack step/event impacts the occurrence of another atomic attack step [WBQ18]. Furthermore, the attack trees can not capture the other complex dependence of the atomic attack steps like the concurrence, sequence, priority and inhibition. Additionally, most of the attack modelling paradigms like the attack trees and AIDD [SS14] are static and cannot capture the stochastic nature of the attack. Especially the uncertainty in the launch time of the atomic attack

step.Furthermore, the attack trees are unable to capture more complex dependencies like sequence. Therefore variants of attack tree like the attack defense trees have been proposed [Ji+16] that can capture sequential dependence of attacks. However, the launch of a coordinated cyber-physical attacks involves more complex logical dependencies. Therefore, modelling formalism like the Petri Net (PN) and its variants have been proposed in the literature for modelling complex cyber-physical attack propagation [Dal+06].

3.4.2 Modelling formalism: Petri nets

A PN represent a mathematical modelling language for describing any type of a Discrete Event Dynamic Systems (DEDS) and particularly suitable for describing systems characterized by concurrency and resource sharing [Mur89]. A PN is a directed bipartite graph that consists of three types of objects: places, transitions, and directed arcs connecting transitions and places [Wan12]. The concept of tokens is used for studying dynamic behaviour of the PN model and they determine execution of a PN. Namely, each place can contain a zero or positive number of tokens. During the execution of a PN, the number and positions of tokens change. An assignment of tokens to the places of a PN is referred to as a marking. Formally a PN is defined as a 5-tuple $N = (P, T, I, O, M_0)$ where,

- $P = \{p_1, p_2, ..p_m\}$ is a finite set of m places.
- $T = \{t_1, t_2, ..t_n\}$ is a finite set of n transitions.
- $I : (P \times T) \longrightarrow N$ is an input function that defines directed arcs from places to transitions.
- $O : (P \times T) \longrightarrow N$ is an output function that defines directed arcs from transitions to places.
- $M_0 : P \longrightarrow N$ is the initial marking.

The rules that allow the firing of the transition and thus the movement of the tokens through the places are as follows.

- Enabling rule: A transition t_i is said to be enabled if each input place p_i of t_i contains at least the number of tokens equal to the weight of the directed arc connecting p to t_i.
- Firing rule: A transition t_i is said to be enabled if each input place p_i of t_i contains at least the number of tokens equal to the weight of the directed arc connecting p_i to t_i.

– An enabled transition t_i may or may not fire depending on the additional condition and context, and

– A firing of an enabled transition t_i removes from each input place p_i the number of tokens equal to the weight of the directed arc connecting p_i to t_i. It deposits in each output place p_i the number of tokens equal to the weight of the directed arc connecting t_i to p_i.

A graphical representation of a PN includes two types of nodes, a circle and a bar, representing a place and a transition, respectively. A token is typically represented with a solid dot. The graphical representation is beneficial for illustration and understanding of PN concepts. A simple example of a PN and illustrated with of places $P = \{p_1, p_2, \ldots, p_7\}$, set of transitions $T = \{t_1, t_2, \ldots, t_5\}$, initial marking $M_0 = (2000001)^T$ and input and output functions as given in the Fig. 3.3.

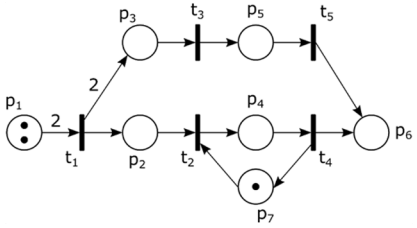


Figure 3.3: Simple Petri net: Initial Marking

In the initial marking, only the transition t_1 is enabled. Fig. 3.4 illustrates the marking of PN after the transition t_1 fires.

The position of tokens after firing of transition t_1 indicates that now transitions t_2 and t_3 are enabled, as illustrated in the Fig. 3.5.

If we assume that the next transition that fires is transition t_2, the new distribution of tokens is as illustrated in the Fig. 3.6.

Similarly all the other transitions are enabled and triggered by the flow of the tokens at the input places of the transitions. The change in tokens in any place marks the change in the marking. The markings then can be considered as the state of the system (whose dynamics is being modelled by the PN and the token flow). The transitions that trigger the change in the markings can then be considered as the state transition. A marking, M_1 is said to be a reachable marking if there exist a sequence of enabled

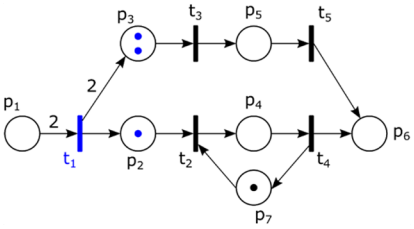


Figure 3.4: Simple Petri net: Marking after transition t_1

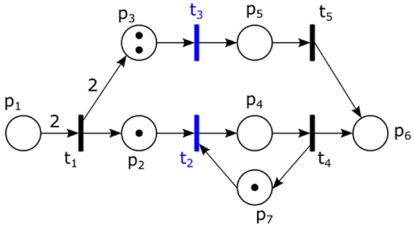


Figure 3.5: Simple Petri net: Transitions enabled after transition t_1

transitions that runs the initial state M_0 into M_1. A rechability tree/graph can be generated, which is a set of markings that are possible from the initial marking. The nodes of the reachability tree represent the markings of the PN, the root representing the initial marking. The directed edge from one marking to another indicates the firing of the corresponding transition. The rechability tree/graph thus generated can be considered as the state transition diagram of the system being modelled, where the marking (nodes) represent the states of the system and the transitions (directed edges) represent the state transitions.

PN Constructs

The different logical constructs that can be modelled by the PN are explaind below. Fig. 3.7 illustrates a construct for sequential execution as transition t_2 can fire only after the firing of t_1. This construct is also suitable to represent the causal relationship between events. Fig. 3.8

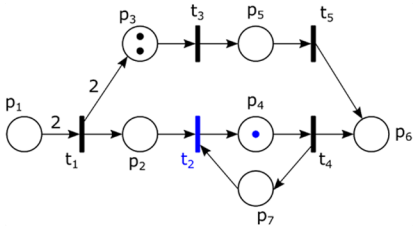


Figure 3.6: Simple Petri net: Marking after transition t_2

Figure 3.7: PN construct for sequential execution

represents a Petri net construct for modeling of conflict between activities. A token at p_1 enables both transition t_1 and transition t_2, but the firing of any disables the other transition.

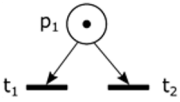


Figure 3.8: PN construct for conflict between activates

In Fig. 3.9 transitions t_1 and t_2 are concurrent. Concurrency is an important characteristic of DEDS and it can be modeled effectively by PN.

A PN construct that can be used to model logical AND is depicted in Fig. 3.10. Namely, transition t_1 is enabled only if there is a token at both p_1 and p_2 places.

The logical OR can be modeled with a PN construct illustrated in Fig. 3.11.

To enable representation of priorities with PN a new type of arc must be introduced. An inhibitor arc is depicted as an arc terminated with a

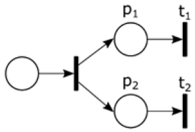


Figure 3.9: PN construct for concurrency

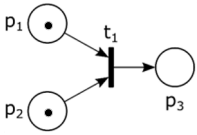


Figure 3.10: PN construct for logical AND

small circle and it changes the transition enabling conditions. Namely, the transition can be enabled only if there are no tokens present on an input place connected to an inhibitor arc. With respect to Fig. 3.12, t_2 is enabled only if p_2 contains a token and p_1 does not have any token. Since t_1 is enabled if p_1 has a token, this PN construct provides priority to t_1 over t_2.

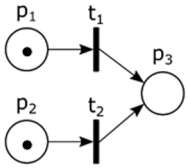


Figure 3.11: PN construct for logical OR

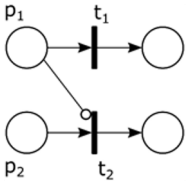


Figure 3.12: PN construct for Priority

PN Classes

Basic PN typically do not provide all required aspects for comprehensive analysis of DEDS. To this end, multiple extension of basic PN have been proposed. The most popular extensions of PN being,

- Timed Petri nets
  - Deterministic Timed Transitions Petri nets: Deterministic Timed Transitions Petri nets refer to a class of Timed PN in which transitions are associated with deterministic firing time.
  - Generalized Stochastic Petri nets: In Generalized Stochastic Petri nets (GSPN), there are two types of transitions that are timed and immediate. Timed transitions are associated with exponentially distributed firing times. Immediate transition fire in with zero delay with specified firing probabilities.
- Colored Petri nets: Colored PN introduced the concept of distinguishing tokens in terms of colors that indicate the token identity. The main motivation for introducing this concept is to allow for a more compact representation of models. Furthermore, the different

colours of the tokens, depending upon what a token represents, could be defining different sources of data, different attacks, different data types,etc. Each place and transition can also have associated colors. For instance, a transition may have a condition attached to its firing rule depending on token colors. This is particularly useful in modelling concurrent attempts of different attacks where each type of an attack attempted is represented with a token of different colour. A specific state of the system (if the attack attempt was a success or a failure), is only reached when a the condition logic pertaining to those specific coloured tokens is met.

Threat propagation modelling with PN

In the context of modelling cyber-physical attacks using the PN, the tokens represent atomic attack event, the colour of the tokens differentiate the atomic attack type, places represent the individual sub-goals/main goal of the attacker, the transition represents individual atomic attack step, the logical constructs model the attack vector, the marking represents set of sub-goals/goal that have been compromised and the reachability tree/graph represents the threat propagation (as a state transition diagram).

The PN provides a wide range of constructs that enable modelling of complex interdependence between different attack propagation steps. Additionally, the authors in [Dal+06] also tackle the problem of stochasticity in the launch of the attacks by modelling the attack tree using GSPN. Though the GSPN covers a lot of limitations of the standard attack tree (and its variants) have, it can only help in evaluating the static stochastic performance measures. This generally boils down to the evaluation of the probability that a specific token has stayed in a specific place, where the token corresponds to the attack and the place represents the goal/sub goal of the attack. But in reality when a coordinated attack is launched, a set of sub-goals/goals are reached and therefore the probability of occurrence of the complete marking, amount of time to reach a marking and dynamic probability (as a function of time) for staying in a marking have to be analysed. Here the Marking represents the threat state and the transitions correspond to threat state transitions. Though GSPN help in visualising and study the propagation of the attacks by analysing the token flow, it unfortunately does not provide enough mathematical tools to analyse the threat propagation indices for the perception of the threat state and also the temporal aspects of the threat state evolution. Furthermore, differentiation in the probability of occurrence of the same atomic step at different stages of attack can not be modelled using a GSPN. A state space based models would enable a better modelling of threat evolution

whose evolution is dependent on its current state. Therefore, in this study a CTMC based threat propagation modelling is proposed that provides the additional mathematical rigour to analyse these indices. Additionally, a methodology based on a MADM approach is proposed to assign parameters to the threat state transitions, that considers the asset's level of vulnerability, their degree of exposure and the skill of the threat agent.

3.5 Proposed Methodology: MADM & CTMC based threat propagation modelling

As mentioned before due to the shortcomings of the methods to model the threat propagation to evaluate the susceptibility indices, a novel method with MADM-CTMC based method is proposed. An overview of the proposed methodology and the different steps involved in the threat propagation modelling and the evaluation of the susceptibility indices are described in this section.

3.5.1 Overview

A flow diagram of the proposed methodology for evaluating the susceptibility of the DGA to the cyber-physical threats is shown in Fig. 3.13. The complete methodology can be grouped into five basic parts. Firstly the threat scenario has to be represented by a modelling formalism that enables all possible constructs of the threat propagation. As it has been presented before, since the GSPNs provide a wide range of logical constructs that could help in representing complex threat scenarios, it has been chosen as the formalism for representing the threat scenario.

In the second part, the state evolution of the threat scenario is modelled. Basically the model is a state transition diagram where the states represent the different threat states an the transitions the individual atomic attack steps. To obtain this state transition diagram, firstly the reachability tree/ graph of the GSPN is generated. Where the nodes of the tree/graph correspond to the marking of the Petri nets and the transitions are the transitions that trigger the change in the marking. Typically the marking represents a single/set of sub-goals/main goal of the attack. As the isomerism of the GSPN and CTMC has been proved [Mol81], the markings in the reachability graph of the GSPN correspond to the states of the CTMC and the reachability graph corresponds to the state transition diagram of a CTMC . The state transition diagram represents the different probabilistic attack paths that are possible to reach all attack goals.

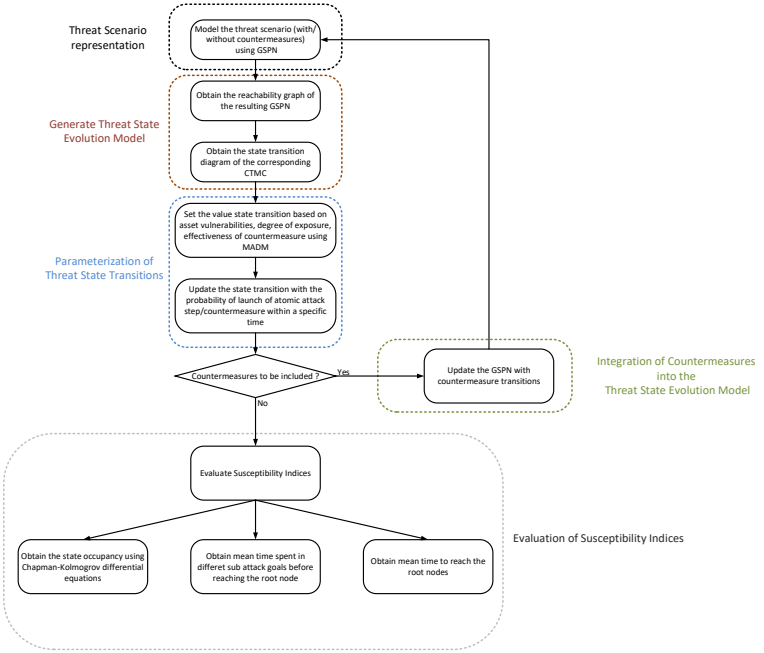


Figure 3.13: Flow chart of the proposed methodology for threat propagation modelling and susceptibility analysis

Once the state transition diagram has been generated, the next steps correspond to the parameterization of the transitions (atomic attack steps). The evolution of the threat state depends heavily on the values attributed to the probability of the launch of the individual atomic attack step. This probability depends on the levels of the vulnerability, degree of exposure of these vulnerability and the skill of the attacker. It should be noted that all the three factors mentioned are abstract, however empirical values can be set based on the expert opinion and analysing the data (typically pertaining to the time taken to launch the atomic attack) of the previous successful attempts in launching the atomic attack. A detailed explanation would be provided in Sect. 3.5.4.

The next step is to evaluate the susceptibility indices as described in Sect. 3.3 using the mathematical tools for evaluating the CTMC. A

detailed description of the calculation of the different indices is provided in Sect. 3.5.5.

Finally when the countermeasures have to be considered the are integrated in the GSPN model of the threat scenario. Once a new GSPN model has been generated representing the threat scenario with the countermeasures, the reachability tree7graph has to be regenerated that includes the transitions corresponding to the countermeasures. After which the transitions have to be re-parameterized based on the effectiveness of the countermeasures in reducing the vulnerabilities or their degree of exposure. A detailed explanation of re-parameterization of the transitions is provided in Sect. 3.5.6. A detailed account of the different steps would follow with an example.

3.5.2 Threat scenario representation

The attack tree representation of an exemplary threat scenario is depicted in Fig. 3.14. Here the leaf nodes E1, E2, E3 denote the three different atomic attack events. The leaf nodes E1 and E2 can be considered as two ways of compromising an asset (Asset-1) by exploiting Vulnerabilities V1 and V2 respectively, that have varied degrees of exposure. The leaf node E3 represents the exploitation of the Asset-2 through its vulnerability V3. The Child node (Sub-Goal1) can be considered as the state where the Asset-1 has been compromised which can be achieved either by exploiting vulnerability V1 or the vulnerability V2. The root node (Main Goal) is achieved when Asset-2 is compromised after the Asset-1 has been compromised.

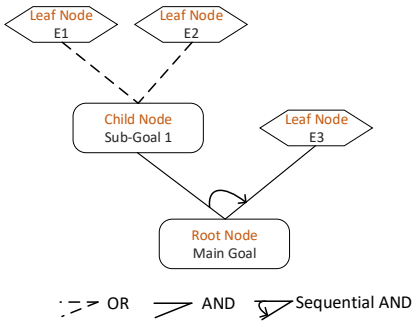


Figure 3.14: Exemplary Threat Scenario Representation: Attack Tree

The GSPN representation of the threat scenario is depicted in Fig. 3.15. The triggering of the individual atomic attack events (E1, E2 and E3) is represented with a sequence construct $\{p_{Ei-S}, t_{Ei}, p_{Ei-T}\}$, where place p_{Ei-S} corresponds to a Safe state where the atomic attack i^{th} atomic attack (Ei) has not yet been launched/triggered. The token in this place represents the atomic attacks whose propagation is to be studied. In this case a threat propagation analysis is to be made for a threat scenario where all the three atomic attack events have been triggered. For analysing the threat evolution of threat scenario where only the atomic attack event E1 is launched, then there would be a token only in the place p_{E1-S}. The transition t_{Ei} corresponds to the rate at which the atomic attack Ei is launched/ triggered. Finally the place p_{Ei-T} corresponds to the unsafe state where a specific atomic attack (Ei) has been launched. The

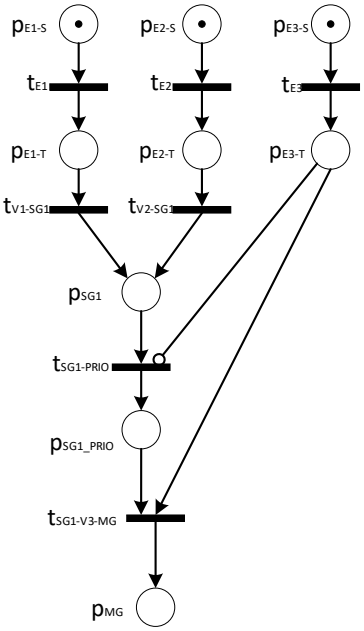


Figure 3.15: Exemplary Threat Scenario Representation: GSPN

Sub-Goal1 is reached either by exploiting the vulnerability V1 or V2

represented by the transition t_{V1-SG1} and t_{V2-SG1} respectively. These transitions correspond to the rate at which the vulnerabilities V1 and V2 is exploited. This rate is dependent on the level of vulnerability, ease of exploitation of the vulnerability and the skill of the threat agent.

A MADM based methodology has been proposed to calculate the rates for these transitions corresponding to the exploitation of the asset vulnerabilities in Sect. 3.5.4. The compromise of Asset-1 is achieved by exploiting its vulnerabilities, represented by a token transitioned either from place p_{E1-S} or p_{E2-S} to place p_{SG1}. The place p_{SG1}corresponds to a state where the Asset-1 has been compromised. So as to reach the Main Goal, it is necessary in this case that the Sub-Goal1 is reached before the atomic attack E3 is launched. Therefore, a transition $t_{SG1-PRIO}$ is modelled that allows the token to transit from place p_{SG1} to $p_{SG1-PRIO}$ only if there is no token in place p_{E3-T}. This functionality is modelled as a priority construct and as an immediate transition. There is no stochastic time associated to this specific transition as it only represents a logical condition. The final Main goal of the attack is then reached only by triggering the transition $t_{SG1-V3-MG}$ that represents the exploitation of the vulnerability of the Asset-2 (V3) given that the Asset-1 has already been compromised. The place p_{MG} represents a state where the final goal of the attack has been compromised if a token is present in this place. It should be noted that all the other transitions except the $t_{SG1-PRIO}$ correspond to a specific atomic attack step and hence represent a probability of successful launch of the atomic attack step within a specific time.

Once the GSPN model has been created, the movement of the tokens can be studied. The movement of the tokens represent change in the marking of the GSPN and thus a change in the state the threat evolution. While representing the threat scenario with GSPN, the multiplicity of the transitions modelled such that, when it is triggered all the tokens in its input place are removed and a single token is transferred to its output place. Such a measure is incorporated to reduce the number of duplicate markings generated that represent the same state of the attack. In the next subsection, a detailed explanation of modelling the threat evolution using the markings of the GSPN is presented.

3.5.3 Model threat state evolution

The modelling of the threat evolution starts with the generation of the reachability graph/tree that denotes the changes in the markings of the GSPN as the tokens move through the GSPN when the logical criteria for triggering the transitions is met. Beginning with the initial marking, for generating the reachability tree/graph, transitions which are enabled

by this marking are identified and the new markings that result from the firing of each of the enabled transitions are generated. Each new marking is added to the tree and the directed edges from the markings are drawn. The algorithm for generating the reachability tree is as given below [Tha12].

m = total number of Markings
$M_i = i^{th}$ Marking
$T_i = i^{th}$ Transition
n = total number of Transitions
Initializing $i = 1$ and $m = 1$
while $i \leq m$ **do**
  for $j = 1$ to T_n **do**
    if j is enabled by Marking M_i, then generate new marking $M_{temp}(k)$ **then**
      for each k **do**
        if $M_{temp}(k)$ is not already in the tree **then**
          $m = m + 1$
          $M_m = M_{temp}(k)$
          $edge(M_i, M_m) = j$
        end if
      end for
    end if
  end for
  $i = i + 1$
end while

The reachability tree/graph generated from the GSPN models of the exemplary threat scenario (shown in Fig. 3.15) is shown in Fig. 3.16. The complete list of the names of the markings and its associated marking values have been tabulated in Tab. 3.1, Tab. 3.2.

As shown in the Fig. 3.16 the total number of markings of the reachability graph is 36. However, since the transition $t_{SG1-PRIO}$ is considered to be a logical condition, the input markings corresponding to the transition $t_{SG1-PRIO}$ would be subsumed by the output markings. In this case the markings M_5,M_9, M_{10}, M_6, and M_{20} would be subsumed by the markings M_{11}, M_{16}, M_{17}, M_{12},and M_{21} respectively. Thus resulting in the reachability graph shown in Fig. 3.17.

Once the simplification of the reachability graph is done for immediate transitions, the next step is to label the markings to specific states of threat evolution. The markings represent a specific threat state, the transition from one marking to another represents a threat state evolution. But it should be noted that different markings may or may not correspond to the

Table 3.1: List of Markings

Marking	Marking Value
M	$\{p_{E1-S}, p_{E2-S}, p_{E3-S}, p_{E1-T}, p_{E2-T}, p_{E3-T}, p_{SG1}, p_{SG1-PRIO}, p_{MG}\}$
M_0	$\{1, 1, 1, 0, 0, 0, 0, 0, 0\}$
M_1	$\{0, 1, 1, 1, 0, 0, 0, 0, 0\}$
M_2	$\{1, 0, 1, 0, 1, 0, 0, 0, 0\}$
M_3	$\{1, 1, 0, 0, 0, 1, 0, 0, 0\}$
M_4	$\{0, 0, 1, 1, 1, 0, 0, 0, 0\}$
M_5	$\{0, 1, 1, 0, 0, 0, 1, 0, 0\}$
M_6	$\{1, 0, 1, 0, 0, 0, 1, 0, 0\}$
M_7	$\{0, 1, 0, 1, 0, 1, 0, 0, 0\}$
M_8	$\{1, 0, 0, 0, 1, 1, 0, 0, 0\}$
M_9	$\{0, 0, 1, 0, 1, 0, 1, 0, 0\}$
M_{10}	$\{0, 0, 1, 1, 0, 0, 1, 0, 0\}$
M_{11}	$\{0, 1, 1, 0, 0, 0, 0, 1, 0\}$
M_{12}	$\{1, 0, 1, 0, 0, 0, 0, 1, 0\}$
M_{13}	$\{0, 1, 0, 0, 0, 1, 1, 0, 0\}$
M_{14}	$\{0, 0, 0, 1, 1, 1, 0, 0, 0\}$
M_{15}	$\{1, 0, 0, 0, 0, 1, 1, 0, 0\}$
M_{16}	$\{0, 0, 1, 0, 1, 0, 0, 1, 0\}$
M_{17}	$\{0, 0, 1, 1, 0, 0, 0, 1, 0\}$
M_{18}	$\{1, 0, 0, 0, 0, 1, 0, 1, 0\}$
M_{19}	$\{1, 0, 0, 0, 0, 0, 0, 0, 1\}$
M_{20}	$\{0, 0, 1, 0, 0, 0, 1, 1, 0\}$

Table 3.2: List of Markings

Marking	Marking Value
M	$\{p_{E1-S}, p_{E2-S}, p_{E3-S}, p_{E1-T}, p_{E2-T}, p_{E3-T}, p_{SG1}, p_{SG1-PRIO}, p_{MG}\}$
M_{21}	$\{0, 0, 1, 0, 0, 0, 0, 2, 0\}$
M_{22}	$\{0, 0, 0, 0, 0, 1, 0, 2, 0\}$
M_{23}	$\{0, 0, 0, 0, 0, 0, 0, 1, 1\}$
M_{24}	$\{0, 0, 0, 0, 1, 1, 0, 1, 0\}$
M_{25}	$\{0, 0, 0, 0, 1, 0, 0, 0, 1\}$
M_{26}	$\{0, 0, 0, 1, 0, 1, 0, 1, 0\}$
M_{27}	$\{0, 0, 0, 1, 0, 0, 0, 0, 1\}$
M_{28}	$\{0, 1, 0, 0, 0, 1, 0, 1, 0\}$
M_{29}	$\{0, 1, 0, 0, 0, 0, 0, 0, 1\}$
M_{30}	$\{0, 0, 1, 0, 1, 0, 0, 1, 0\}$
M_{31}	$\{0, 0, 0, 0, 1, 1, 0, 1, 0\}$
M_{32}	$\{0, 0, 0, 0, 0, 1, 1, 1, 0\}$
M_{33}	$\{0, 0, 0, 0, 0, 0, 1, 0, 1\}$
M_{34}	$\{0, 0, 0, 0, 1, 1, 1, 0, 0\}$
M_{35}	$\{0, 0, 0, 1, 0, 1, 1, 0, 0\}$
M_{36}	$\{0, 0, 0, 0, 0, 1, 2, 0, 0\}$

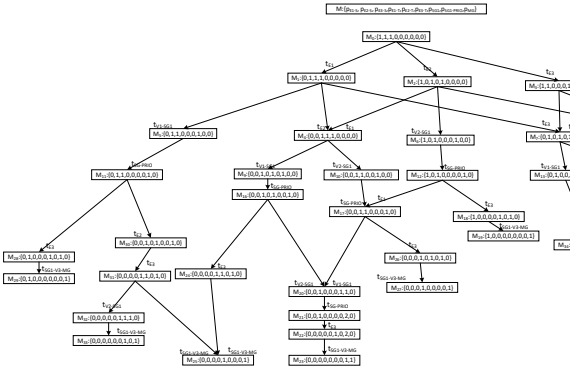


Figure 3.16: Reachability graph of the exemplary threat scenario

Table 3.3: Labelling of Markings

Threat State Class	Marking (Threat State)								
	p_{E1-S}	p_{E2-S}	p_{E3-S}	p_{E1-T}	p_{E2-T}	p_{E3-T}	p_{SG1}	$p_{SG1-PRIO}$	p_{MG}
S_{MG}	*	*	*	*	*	*	*	*	1
$S_{SG1-E3T}$	*	*	*	*	*	1	1 or 2	0	0
S_{SG1}	*	*	*	*	*	0	1	0	0
$S_{V12-SG1}$	*	*	*	*	*	0	2	0	0
$S_{SG1-PRIO}$	*	*	*	*	*	0	1	0	0
S_{E3-T}	*	*	*	0	0	1	0	0	0
S_{E2-T}	*	*	*	0	1	0	0	0	0
S_{E1-T}	*	*	*	1	0	0	0	0	0
S_{E1E2-T}	*	*	*	1	1	0	0	0	0
S_{E1E3-T}	*	*	*	1	0	1	0	0	0
S_{E2E3-T}	*	*	*	0	1	1	0	0	0
$S_{E1E2E3-T}$	*	*	*	1	1	1	0	0	0
S_{SAFE}	*	*	*	0	0	0	0	0	0

the same threat state. A meaningful threat state class is used as a label to classify the different markings. This allows the association of markings to meaningful threat state classes. For example, there are different markings that correspond to reaching of the main goal, which is identified by a token 1 at the place p_{MG}. Therefore, the Markings M_{19}, M_{23}, M_{25}, M_{27}, M_{29}, and M_{33} belong to the same threat state class. Similarly the other markings are also labelled with a specific threat state class according to the presence of a token in the specific places as described in Tab. 3.3. The $*$ in the marking represents that it could take any value from 0 to n, where n is any natural number.

The reachability graph shown in Fig. 3.17 becomes the state transition graph of a CTMC. The different markings become the states of the CTMC

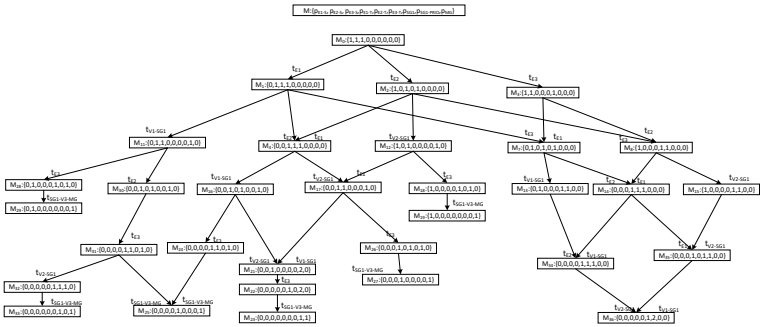


Figure 3.17: Reachability graph of the exemplary threat scenario simplifying for immediate transitions

that represents the threat state evolution. From this point on the threat state represents the marking of the reachability tree and the reachability tree/graph would be called as the state transition diagram.

The labelling of the markings, help in classifying the states of the CTMC into different threat state classes that represent a tangible cyber-physical threat state. A pictorial representation of the state transition graph of the exemplary threat scenario along with the classification of the states into their classes is provided in Fig. 3.18.

The state transition graph can further be simplified considering the fact that the the markings M_{29}, M_{33}, M_{25}, M_{23}, M_{27}, M_{19} all correspond to the reaching of the final goal of the attack. Thus these markings are considered as a single state S_{MG}. Furthermore, the markings M_{34}, M_{35} and M_{36} can be clubbed into a single threat state/class (S_{MG}) as no further transitions arise from these markings that transit to another threat state/class. Additionally, the M_{13} and M_{15} can also be clubbed to the same threat state for the aforementioned reason. Finally the most simplified CTMC state transition graph, as depicted in Fig. 3.19 of the exemplary threat scenario, is derived.

From the Fig. 3.19 it can be seen that there are two absorbing states, S_{MG}, $S_{SG1-E3T}$. The state $S_{SG1-E3T}$ corresponds to a state where, the sub-goal1 is reached after the vulnerability V3 has been exploited. In such case the main goal is not reached as the sequential dependence of the exploitation of vulnerability V1 or V2 before the exploitation of vulnerability V3 is not met. The state S_{MG} is reached only in those case when the aforementioned sequential dependence so the vulnerability

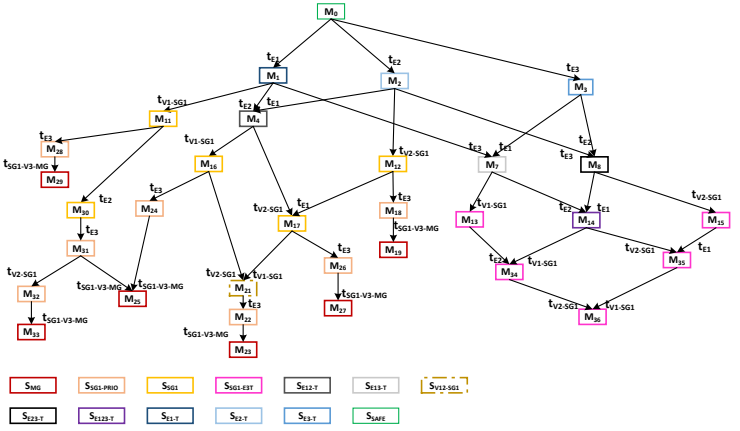


Figure 3.18: CTMC State transition graph with threat state class associations

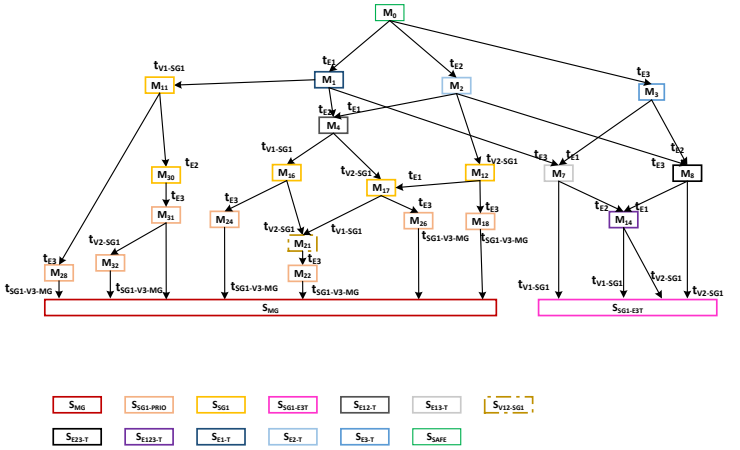


Figure 3.19: Simplified CTMC threat state transition graph

exploitation is met. The CTMC thus depicts the different possible threat

state evolution direction. A detailed explanation of the different CTMC metrics are given in Sect. 3.5.5. But before the susceptibility metrics are calculated, the parameterization of the transitions in the state transition graph of the CTMC has to be made. In the next subsection an explanation is provided on this aspect.

3.5.4 Parameterization of threat state transitions

The most important part in the modelling the threat state evolution is the parameterization of the transitions in the state transition graph. These transitions determine the swiftness of the threat propagation and the direction of the threat propagation. The state transitions are stochastic in nature. These transitions generally represent the asset's level of vulnerability, their degree of exposure and the skill of the threat agent to exploit these vulnerabilities. In this study, an exploitation factor c_{EF} is introduced to capture the easiness in exploiting the vulnerability based on the level of the vulnerability and the degree of exposure. The skill of the threat agent is captured by the stochastic time taken to launch the atomic attack step. Higher the skill shorter is the average time (higher rate) to launch the atomic attack step. In this study, the atomic attack step launch time is considered to be stochastic and follows an exponential distribution. Hence, the transition of the state transition graph of the threat evolution, can be parameterized as a function of the c_{EF} and the rate of atomic attack launch time as shown in Eq. (3.6).

$$\lambda_{ij} = c_{EF}^{ij} * \lambda_{TA-SK}^{ij} \tag{3.6}$$

Where λ_{ij} is the rate of transition from threat state i to threat state j, c_{EF}^{ij} is the exploitability factor and the $1/\lambda_{TA-SK}^{ij}$ represents the mean time to successfully complete the exploitation of the vulnerability. The time to compromise reflects the skill of the attacker (threat agent). In this study, it is assumed that the probability density function of the time to successfully complete the launch of the attack (exploitation of the vulnerability that triggers the threat state transition from state i to state j) is exponentially distributed with a mean time $1/\lambda_{TA-SK}^{ij}$ time units. Therefore, the overall state transition time is also exponentially distributed with a mean time of $1/\lambda_{ij}$. Once the values of the different λ_{ij}s are determined then using the standard metrics of CTMC the susceptibility of the infrastructure could be evaluated as presented in Sect. 3.5.5.

However, to determine the values of the λ_{ij} the values of c_{EF}^{ij} must be determined. The methodology for determining the values of λ_{TA-SK}^{ij} is beyond the scope of this study. However, such the values could be

Table 3.4: Likelyhood of Vulnerability Exploitation

Vulnerability Level	Degree of Exposure		
	Low	Medium	High
Low	Very Unlikely	Unlikely	Possible
Medium	Unlikely	Possible	Likely
High	Possible	Likely	Very Likely

experimentally derived. In case of exploitation of the cyber vulnerability the data on the penetration tests could be used to determine the mean time to successfully exploit the vulnerability. In case of exploiting the physical vulnerability, for e.g attacks by drones, the mean time to compromise can be determined by the maximum speed, maximum area that it could cover and maneuverability of the drone. Furthermore, currently AI based methods have been used to determine these quantities [PJ21],[KL20]. Within the scope if this study, it is assumed that the mean compromise times for every atomic attack step is known.

The c_{EF}^{ij} represents the likelihood of the vulnerability to be exploited. This likelihood is empirically evaluated based on the level of vulnerability and the degree of exposure as shown in Tab. 3.4. This matrix has been developed inspired from the standard risk assessment matrices presented in [Kuz+21],[Def17], [JHT19].

The generic explanations of the what is considered to be low, medium and high for levels of vulnerability and the degree of exposure is provided as given below.

- Vulnerability level
  - Low: Successful attack is possible only with very high skill
  - Medium: Successful attack is possible with average skill
  - High: Successful attack is possible with low skill
- Degree of exposure
  - Low: Highly restricted access (physical/logical)
  - Medium: Restricted access (physical/logical)
  - High: Easy access (physical/logical)

It is evident from the Tab. 3.4 that, the likelihood of the vulnerability exploitation is very qualitative in nature. However, to evaluate the threat propagation, this likelihood has to be quantified and attribute it to the specific c_{EF}^{ij}. To facilitate the quantification of the c_{EF}^{ij} based on the qualitative assessment of the vulnerability exploitation, an Analytical

Hierarchical Process (AHP) based (a specific type of MADM) methodology is proposed.

AHP based quantification of Exploitation Factor & Countermeasure Efficiency

Consider a generic threat state as shown in Fig. 3.20. The state transition from $Threat - State_i$ to $Threat - State_{j,k,l}$ represent the exploitation of two different vulnerabilities and actuation of a countermeasure whose likelihood has been qualitatively evaluated as *Very Likely*, *Possible* and *Very Unlikely*. The likelihood evaluation of the countermeasure is explained in Sect. 3.5.6.

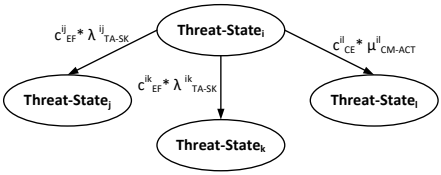


Figure 3.20: Generic threat state and transitions

With the help of AHP a weighting factor (such that $0 \leq$ weighting factor ≤ 1) can be derived considering the relative likelihood of the vulnerability exploitation. The weighting factor thus derived then represents the individual c^{ix}_{EF} (or c^{ix}_{CE} for countermeasure efficiency explained in Sect. 3.5.6) where $x \in j, k, l$. AHP method is a useful and effective technique, developed by [Saa87], for solving complex decision making problems. It breaks down the problem into a hierarchical structure of the goal, attributes (or criteria) and alternatives . In our model, the AHP method is used to compute the weight for each attribute by carrying out pairwise comparisons of the attributes, which is done by the decision makers or experts. The importance of an attribute is directly proportional to its weight. In this case the attributes are the vulnerabilities that can be exploited from the current threat state. The weight is the quantification of its likelihood(c^{ix}_{EF} (or c^{ix}_{CE}) where $x \in j, k, l$).The steps for calculating the weights for the attributes are explained below.

1. Create a pairwise comparison matrix A. The matrix A is a m x m matrix where m is the number of attributes (or vulnerabilities that could be exploited from the current threat state). In matrix A, each item a_{ij} represents the importance of j^{th} attribute in relation to i^{th}

attribute. The numerical value assigned to each item in matrix A is derived from the Tab. 3.5 [Saa87].

$$A = \begin{bmatrix} 1 & a_{12} & a_{13} & a_{14} & \dots & a_{1m} \\ \frac{1}{a_{12}} & 1 & a_{23} & a_{24} & \dots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1m}} & \frac{1}{a_{2m}} & \frac{1}{a_{3m}} & \frac{1}{a_{4m}} & \dots & 1 \end{bmatrix} \tag{3.7}$$

Relative Likelihood	**Interpretation**
1	Equally Likely
3	Moderately more Likely
5	Strongly Likely
7	Very Strongly Likely
9	Extremely Likely
2,4,6,8	Intermediate values between the two adjacent judgments

Table 3.5: Pairwise Comparison Scale

2. Compute the normalized pairwise comparison matrix A_{norm} from matrix A. Each entry $\overline{a_{ij}}$ in matrix A_{norm} is calculates as shown below

$$\overline{a_{ij}} = \frac{a_{jk}}{\sum_{l=1}^{m} a_{lk}} \tag{3.8}$$

3. The weight of each attribute (or quantification of the likelihood of j^{th} vulnerability be exploited) w_j is calculated by taking the average of each row in A_{norm}.

$$w_j = \frac{\sum_{l=1}^{m} \overline{a_{jl}}}{m} \qquad j = 1, ..., m \tag{3.9}$$

4. There could be inconsistencies when pairwise comparisons are performed by the decision maker [Saa87]. The consistency of matrix A can be checked by computing the consistency ratio (CR). If CR is less than 10%, then the matrix is consistent and the calculated weights can be used further but, if not, then the decision makers have to improve the judgment and recreate the comparison matrix A.

$$CR = \frac{CI}{RI} \tag{3.10}$$

$$CI = \frac{\lambda_{max} - m}{m - 1} \tag{3.11}$$

where CI is the consistency index, RI is the random index, m is the dimension of the matrix and λ_{max} is the average of eigenvalues.

RI is calculated from the average CI of 500 randomly filled matrices. The calculated values of RI for (m<=10) are shown in Tab. 3.6

m	2	3	4	5	6	7	8	9	10
RI	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Table 3.6: Values of RI

Similarly the AHP is used iterative at every threat state for determining the c_{EF} of all its outgoing transitions. The outgoing transitions represent the exploitation of the vulnerability from the current threat state. Once the exploitation factors have been quantified for all transitions, then the standard metrics of CTMC can be used to derive all the susceptibility indices as explained in Sect. 3.5.5.

3.5.5 Susceptibility evaluation

As mentioned in the Sect. 3.3, the main objective of the susceptibility analysis is to evaluate the indices for the threat state perception and the indices for the perception of the temporal aspects of threat evolution. Once the threat state evolution is modelled as a CTMC with the transitions properly parameterized as explained in Sect. 3.5.4, then the standard metrics of the CTMC could be used to evaluate the aforementioned susceptibility indices.

Threat state evolution formulation with CTMC

The threat state evolution is considered as stochastic process, $\{X(t), t \geq 0\}$ with continuous time and discrete states $S_{\aleph} = S0, S1, S2, ..., Sn$, where the evolution is state dependant and is only influences by the current state that the threat has evolved to. The stochasticity in the threat evolution comes from the uncertainty of the time of launch of the atomic attack step, which is attributed to the skill of the threat agent, levels of vulnerability and the degree of exposure of the vulnerability.

Assuming that the state of the system at time k is $X(k) = i$, the conditional probability that the system will be in state j at time $t + k$ is:

$$\begin{aligned} &Pr(X(t+k) = j \\ &\quad |X(k) = i, X(u) = x(u), 0 \leq u < k) = \\ &Pr(X(t+k) = j \\ &\quad |X(k) = i, \ for\ all\ possible\ x(u), 0 \leq u < k) \end{aligned} \tag{3.12}$$

where $x(u), 0 \leq u < k$ denotes the history of the system state evolution up till the time k but not including k. The aforementioned stochastic process is said to be a CTMC, which means that, if the present state of the system is known, the future development of the system state is only dependent on the current state and is completely independent of anything that has happened in the past. This is true in modelling the cyber-physical attacks as the propagation of the attack in the future only depends on the current state of the attack. Given a CTMC with all the possible states and the conditional state transition probability matrix P , the probability of being in a specific state could be calculated as shown in Eq. (3.13)

$$\begin{aligned} &\pi_j(t) = \sum_{i=0}^{n} p_{ij}(0,t) * \pi_i(0); \quad such\ that \\ &\sum_{i=0}^{n} p_{ij}(0,t) = 1 \quad and \quad \sum_{j=0}^{n} \pi_j(t) = 1 \end{aligned} \tag{3.13}$$

Where $\pi_j(t)$ is the Probability Mass Function (PMF) of the system to be in state j at time t, p_{ij} is an element of matrix P (as shown in Eq. (3.14)) corresponding to the conditional probability of jumping to state j from state i , $\pi_i(0)$ is the PMF of the system to be in state i initially and n is the total number of threat states possible.

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \tag{3.14}$$

Indices for the perception of threat state

Evaluation of the threat evolution as a function of time helps in calculating the probability of the threat being in a specific threat state. The evaluation of the dynamic state occupancy probability of the CTMC provides the exact information, once the threat evolution has been modelled as a CTMC. The dynamic state occupancy probability of the j^{th} threat state, $p_j(t)$, can be calculated based on the Chapman Kolmogorov's equation [TB17]. The solution for the dynamic state occupancy probabilities is then obtained by solving the Eq. (3.15).

$$\frac{d\left(\pi(t)\right)}{dt} = \boldsymbol{\pi}(t)Q \tag{3.15}$$

Where $\boldsymbol{\pi}(t) = [\pi_1(t), \ldots \pi_j(t) \ldots, \pi_n(t)]$ (a matrix of state occupancy probabilities) and Q is the infinitesimal generator matrix, that is a partial differential of the P matrix over time subject to the total probability constraints [TB17]. The Q is defined as shown in Eq. (3.16).

$$Q = [\lambda_{ij}]\,,\ \textit{such that}\ \lambda_{ii} = -\sum_{\forall j} \lambda_{ij} \tag{3.16}$$

Where λ_{ij} represents the rate at which the system transits from threat state i to threat state j, which includes the vulnerability exploitation factor the stochastic compromise rate of the atomic attack step as per Eq. (3.6). Given the initial state $\boldsymbol{\pi}(0)$, the $\boldsymbol{\pi}(t)$ can then be calculated as shown in Eq. (3.17). Different numerical methods can be used to solve the equation. In this study Runge-Kutta 3^{rd} order method is used as the integrator.

$$\boldsymbol{\pi}(t) = \boldsymbol{\pi}(0)e^{Qt} \tag{3.17}$$

In most cases the different threat states are classified into various classes that have a specific physical significance, for example the threat states that correspond to the reaching of the final attack goal, or a single sub-goal or set of sub-goals. Therefore, in such cases the probability of occurrence of the complete threat class would be interesting evaluate. For example in the threat scenario example presented in Fig. 3.18, all the red threat state correspond to reaching of final goal of the attack and all the yellow

states represent eh compromise of sub-goal1 given that the Vulnerability V3 has not been previously exploited and so on. The complete probability of reaching the final goal, for e.g can only be evaluated by summing the probabilities of all the threat states belonging to the specific threat class. Understanding the threat class evolution has more physical significance, as it is helpful in designing the appropriate counter measures that are specific for the threat class. Hence, finally the the probability of reaching a specific threat class is calculated as per the Eq. (3.18).

$$\begin{aligned} \left[\pi^{i}_{Threat-Class}\right] &= \sum_{\forall j \in Threat-Class} \pi_j; \\ &such\ that\ 0 < i \leq k \\ &where\ k\ = number\ of\ Threat\ State\ Class \end{aligned} \tag{3.18}$$

Both the $\boldsymbol{\pi}(t)$ and the vector of $\left[\pi^{i}_{Threat-Class}\right]$ are the indices for perception of the threat state. Where, the former provides the dynamic probability of each threat state possible, and the later provides the dynamic probability of the threat state classes. Depending upon the granularity of the available countermeasures, higher granular countermeasures reduce the risk of individual threat state and lower granular countermeasures reduce the risk of complete threat class, either the $\boldsymbol{\pi}(t)$ or the $\left[\pi^{i}_{Threat-Class}\right]$ can be considered as the susceptibility index.

Indices for the perception of temporal aspects of threat evolution

The two major indices that helps in understanding the temporal aspects of the threat evolution are the time to compromise and the average time spent in the other threat states (apart from the main attack goal). Typically, when an attack tree is translated into a CTMC, it results in an CTMC with absorbing states. The absorbing states are those state of a CTMC that have only incoming transitions and no out-going transitions. Such a state generally represents the reaching of the main goal of the attack tree. For CTMCs with absorbing states additional temporal measures pertaining to the absorption (compromise time), namely the expected absorption time $E[T_a]$, can be evaluated, as shown in Eq. (3.19). The expected absorption time corresponds to the mean time the attacker takes to reach the root node. Subsequently the time spent in each transient state (other states in the CTMC except the absorbing states) before reaching the main goal ($\tau = [\tau_1, \tau_2, ..., \tau_u]$) can also be calculated as shown in Eq. (3.20).

$$E[T_a] = -\boldsymbol{\pi}_u(0) Q_u^{-1} \varepsilon^T \tag{3.19}$$

$$\boldsymbol{\tau} = -\boldsymbol{\pi}_u(0)Q_u^{-1} \tag{3.20}$$

Where Q_u (as shown in Eq. (3.21) is a partition of Q over the transient states Ω_u, $\boldsymbol{a_N}$ is a set of N column vectors grouping the transition rates from any transient state to the N absorbing states, and the row corresponding to the absorbing state has only zero entries.

$$Q = \begin{bmatrix} Q_u & \boldsymbol{a_1}^T & \cdots & \boldsymbol{a_N}^T \\ 0_1 & \cdots & \cdots & 0_1 \\ \vdots & & & \vdots \\ 0_N & \cdots & \cdots & 0_N \end{bmatrix} \tag{3.21}$$

Where $\boldsymbol{\pi}_u(0)$ is the vector of the initial state of the transient states. ϵ is the row vector of ones with a size equal to the cardinality of the state space Ω, such that $\Omega = \Omega_u \cup \Omega_a$, where, Ω_u is the set of transient states of the CTMC and the Ω_a the set of absorbing states with cardinality N. When an attack tree is represented as a CTMC with an absorbing state, the transient states correspond to reaching sub goals of the attack and the absorbing state corresponds to the reaching of the root node. It should be noted that a CTMC representation of a complex attack tree with defenses could have more than one absorbing state that would either correspond to a root node or to a healthy state or to subgoals. Hence it is important to evaluate the expected time to absorption to the different absorbing states. The expected time for the absorption in to a single absorption state is given by equation (3.19), but when more than one absorption state exist then the time to the i^{th} absorbing state is given by Eq. (3.22), where $1 \leq i \leq N$.

$$E[{T_a}^i] = \frac{-\boldsymbol{\tau} Q_u^{-2} \boldsymbol{a_i}^T}{\boldsymbol{\tau} \boldsymbol{a_i}^T} \tag{3.22}$$

3.5.6 Integration of countermeasures

There are different types of countermeasures that could be deployed for reducing the risk of the attack. These measures vary depending upon the type of attack they protect from. In case of protection against physical attacks, advance sensor based intrusion detection systems are deployed. Additionally, emergency physical security measures could be deployed automatically depending upon the alarms from the intrusion detections and additional alarms from prediction of the physical threat propagation. Special measures have to be taken to reduce the risks of cyber attacks. For instance, taking appropriate measures to ensure proper management of access rights, the integrity of the data exchanged, the

encryption of the communication protocol used for data exchange, denial of unauthorized network access, denial of unauthorized configuration changes of automation device/communication device and other systematic measures against phishing attacks and credential thefts.

Both for evaluating the effectiveness of the countermeasures against physical and cyber attacks, the deployamable countermeasures should be modelled in the threat propagation model. Once the susceptibility is evaluated for a threat scenario, the appropriate set of countermeasures are chosen to be implemented. However, before the implementation it is important to check the risk reduction factor of the countermeasure. Therefore, the transitions corresponding to the countermeasure actions should be included in the threat propagation modelling. This is done by including the countermeasure transitions in the original GSPN model of the threat scenario. as shown in Fig. 3.21 and generating the CTMC associated with it, as shown in Fig. 3.22.

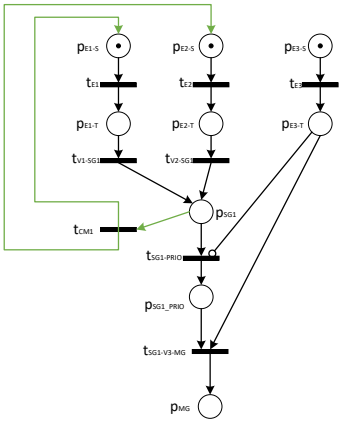


Figure 3.21: GSPN model of the threat scenario with countermeasure

Once the CTMC is generated, the attack transitions and the countermeasure transitions have to be re-parameterized, based on their relative likelihood. The countermeasures have their Countermeasure Efficiency ($c_C^{ij}E$) and their rate of actuation (μ_{CM-ACT}). The countermeasure transition rate can then be calculated as per the equation(3.23).

$$\lambda_{ij} = c_{CE}^{ij} * \mu_{CM-ACT}^{ij} \tag{3.23}$$

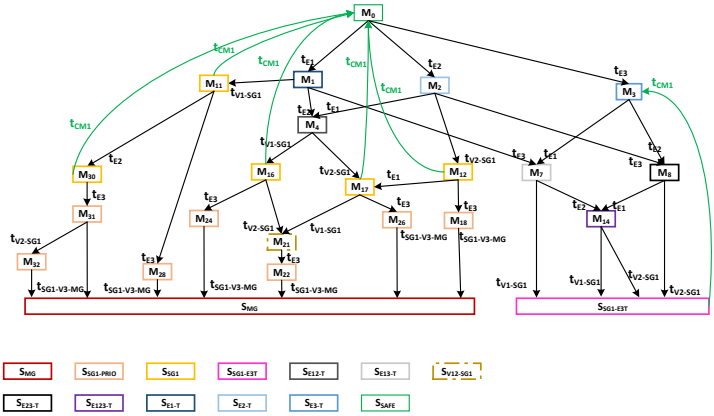


Figure 3.22: CTMC state transition graph of the threat scenario with countermeasure

The likelihood of the actuation of the countermeasure is considered as the efficiency of the countermeasure. The efficiency of the countermeasure is determined qualitatively by assessing its ability to reduce the risk of the threat. If a countermeasure is designed to reduce the risk completely of a *Very Likely* threat then the qualitative assessment of the c_{CE}^{ij} is *Very Likely*. The quantification of the c_{CE}^{ij} is done as explained in Sect. 3.5.4.

3.6 Test Case

3.6.1 Test Case description

A simple example of threat scenario, shown in Fig.3.2, is considered here to illustrate the features of the proposed method. From the set of all the threat classes presented in Tab. 3.3, the S_{SG1}, $S_{SG1-PRIO}$ and $S_{SG1-E3T}$ are considered to be the major sub goals of the attacker and S_{MG} is the final goal of the attack. Two different test cases are presented and the probability of reaching the root node and the time to reach the root node for both the cases are calculated.The Test case 1 covers the analysis of the threat scenario without countermeasures and in test case 2 the analysis of the threat propagation with countermeasures is presented. A comparison

of the threat propagation time and probability of reaching the final goal of the attack are presented.

Finally, a comparison of the time spent in each transient state/state class is also provided. The time spent in each transient state is useful to calculate the cost of an attack on the system depending on the degradation of the system performance when any of the sub attack goals have been reached. For both the test cases irrespective of threat state the likelihood of the outgoing transitions is as tabulated in Table.3.7. However, it should be noted that for modelling more complex threat scenarios, state dependent likelihood levels could be used, wherein for every threat state each of the outgoing transition is given a specific likelihood. Once the likelihood is defined, for each threat state a relative pairwise weights for each of its outgoing transition, is determined based on the Table.3.5. These weights either correspond to the c_{EF}^{ij} or c_{CE}^{ij} based on whether the transition represents an atomic attack step or the actuation of the countermeasure. The mean time to successfully launch an atomic attack step or the mean time to actuate a countermeasure assumed for the test cases are tabulated in Table.3.7. Please note that the values are represented as rates (1/mean-time). It should be noted that these attack times and actuation times are assumed to be exponentially distributed.

Table 3.7: Transitions, their likelihood and compromise rates

Transition	Likelihood	Rate $(time - Unit)^{-1}$
$t_{E1} - \lambda_{TA-SK}$	Possible	.1
$t_{E2} - \lambda_{TA-SK}$	Possible	.1
$t_{E3} - \lambda_{TA-SK}$	Unlikely	.01
$t_{V1-SG1} - \lambda_{TA-SK}$	Likely	1
$t_{V2-SG1} - \lambda_{TA-SK}$	Likely	1
$t_{SG1-V3-MG} - \lambda_{TA-SK}$	Possible	1
$t_{CM1} - \mu_{CM-ACT}$	Very Likely	10

3.6.2 Test Case-1 : Threat scenario without countermeasure

The probability of threat being in any of the threat states calculated as per Eq. (3.17) for the given threat scenario without countermeasures is depicted in Fig. 3.23. Based on these threat state occupancy probabilities, the probabilities for the different threat classes can be calculated as per Eq. (3.18) is depicted in Fig. 3.24.

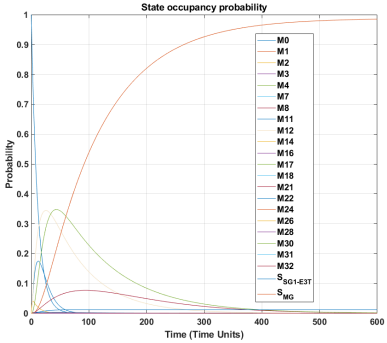


Figure 3.23: Probability of threat state occupancy- Case 1

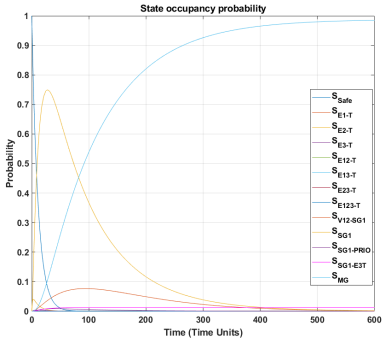


Figure 3.24: Probability of threat state class occupancy- Case 1

As explained in Sect. 3.5.3 the threat evolution of the scenario under study is represented by a CTMC with two absorbing state where each of the absorbing state corresponds to different goals of the attack. The threat propagation ends in these states, and there is no further threat states that it can transit to. Therefore, as depicted in the Fig. 3.24, the probability of the threat to occupy the absorbing threat state classes S_{MG} and $S_{SG1-E3T}$ settles to a value 0.9881 and 0.0119 respectively. As it can be seen, the probability of occupying S_{MG} is higher than the probability of occupying the threat state class $S_{SG1-E3T}$. This can be attributed to the fact that the likelihood of exploiting the Vulnerability V3 with respect to exploiting the vulnerability V1 or V2 is comparatively low. Therefore, the probability of exploitation of vulnerability V1 and V2 first has higher

probability and hence higher probability to reach S_{MG} in comparison to reaching $S_{SG1-E3T}$.

The threat propagates over a set of transient threat states before it reaches the absorbing CTMC states (S_{MG} and $S_{SG1-E3T}$). The mean time spent in the transient states before reaching each of the absorbing states is depicted in Fig. 3.25. The absorption time is calculated based on a pre-condition that a specific threat has reached an absorbing state, then how much time did it take to reach there. It shows how fast the threat propagates in the direction of a specific absorbing state (end state of the threat). Such an analysis helps to understand the rate at which the threat propagates in a direction. It is to be noted that the faster propagation (smaller absorption time) doesn't correspond to most probable threat propagation path. In contrary, for e.g in this exemplary threat scenario, we see that probability of reaching the $S_{SG1-E3T}$ is lower than the probability of reaching S_{MG}, though, the rate of reaching the $S_{SG1-E3T}$ is higher than that of S_{MG}, i.e the mean time to reach S_{MG} is higher than reaching $S_{SG1-E3T}$, as shown in Fig. 3.25.

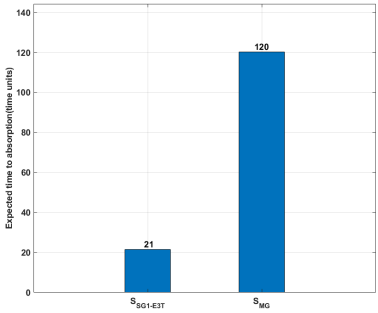


Figure 3.25: Mean time to be absorbed into S_{MG} and $S_{SG1-E3T}$ threat state classes- Case 1

The time to absorption, is also the total time spent in different transient states. Depending on the time spent in different transient states (degraded operation states) the risk of the degraded operation could be calculated. Furthermore, countermeasures with appropriate temporal characteristics could be selected. Therefore, the time spent in the different transient state classes for the exemplary threat scenario calculated as per Eq. (3.20) is depicted in percentage in Fig. 3.26.

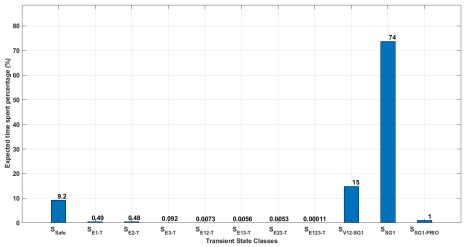


Figure 3.26: Percentage mean time spent in the transient threat state classes- Case 1

3.6.3 Test Case-2 : Threat scenario with countermeasure

In this test case the impact of the countermeasures would be presented. The countermeasure t_{CM} is introduced to thwart the further threat propagation from the threat class S_{SG1}. The probability of threat state occupancy is depicted in Fig. 3.27 and the probability of occupying of the threat state classes is depicted in Fig. 3.28. Due to a strong countermeasure with a faster actuation and high efficiency the most probable state of the threat propagation is the S_{Safe}.

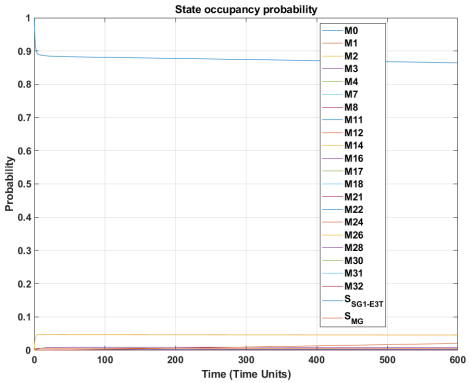


Figure 3.27: Probability of threat state occupancy- Case 2

To understand the threat state/state class where the threat mostly resides before it reaches the absorbing state, the percentage of mean time

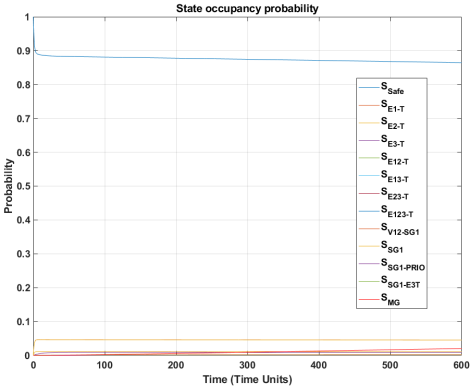


Figure 3.28: Probability of threat state class occupancy- Case 2

spent by the treat in different threat state classes when countermeasure is considered is depicted in Fig. 3.29.

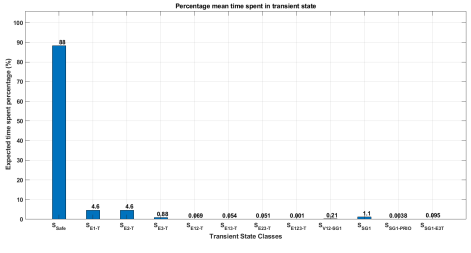


Figure 3.29: Percentage mean time spent in the transient threat state classes- Case 2

To evaluate the effectiveness of the countermeasure a comparison of the probability of reaching the main goal of the threat scenario S_{MG} is compared and depicted in Fig. 3.30.

The mean time to reach the main goal of the attack with and without countermeasure is depicted in Fig. 3.31. From both the aforementioned comparison it is clear that the countermeasure deployed reduces the probability of reaching the threat propagation to the main goal of the attack. Furthermore, the time taken by the threat to propagate to the final goal is drastically increased. Finally a comparison of the percentage

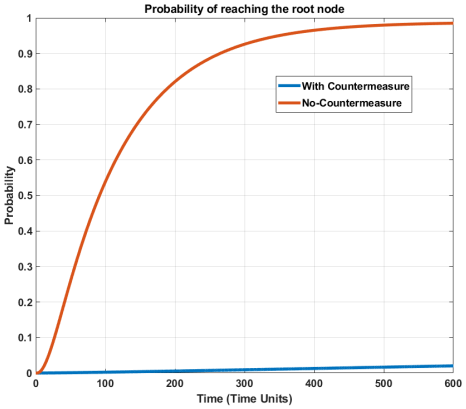


Figure 3.30: Probability of reaching the attack goal: With Countermeasure vs No Countermeasure

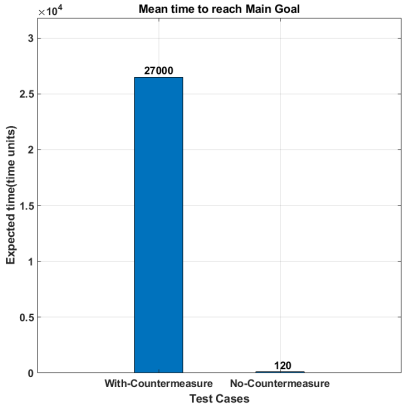


Figure 3.31: Mean time to reach the main attack goal : With Countermeasure vs No Countermeasure

mean time occupied in the transient states that are considered in this example as the major sub goals of the attacker (S_{SG1}, $S_{SG1-PRIO}$ and $S_{SG1-E3T}$) along with the safe state S_{Safe} is depicted in Fig. 3.32.

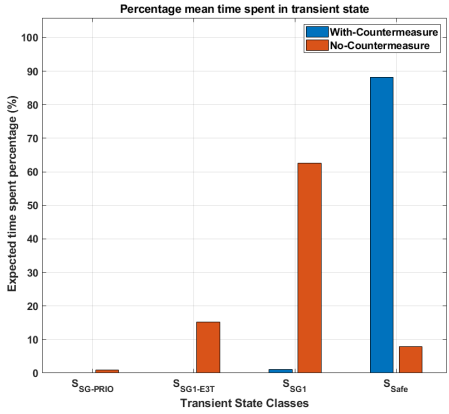


Figure 3.32: Percentage mean time spent in major sub goals of the attack and the safe state : With Countermeasure vs No Countermeasure

It can be seen from Fig. 3.32 that due to the deployment of the countermeasure, the threat does not propagate and majorly stays in the safe state.

3.7 Conclusion

In this study a stochastic methodology based on CTMC and AHPto analyse attack trees and also their extensions with countermeasures has been presented. The steps to be followed to obtain the CTMC from attack trees using PNs have been explained. Specific performance measures using CTMC, namely the state occupancy probability, time spent in the transient states and the estimated absorption time have been mapped to the probability of reaching the sub attack/attack goals, expected time spent in sub attack states and time to reach root node respectively. The proposed methodology provides flexibility to include the uncertainty in the likelihood of vulnerability exploitation based on the levels of the vulnerability and the degree of exposure using AHP. Furthermore, the effectiveness of the countermeasures compared to the likelihood of vulnerability exploitation is also taken into consideration in the threat propagation modelling. This enables the system designers to assess the risk of a specific attack given the efficiency of a countermeasure. The results presented for the test

case 2 show that, with CTMC, effectiveness of the countermeasure can be calculated by evaluating the probability of threat state occupancy, time spent in the transient states and the time to reach the main goal of the attack.

3.8 Scope and future work

The proposed method has been shown to model threat scenarios, include uncertainties of the attack propagation and countermeasure actuation. However, it should be noted that the methodology proposed is based on state space analysis. Therefore, depending upon the complexity of the attack being modelled, number of threat agents, number of vulnerabilities to be considered in the threat scenario, the size of the attack vectors, the state space representation of the threat scenario could easily explode. One of the future work of this presented methodology is to solve the state space explosion problem of the methodology. One method to investigate for this purpose is the applicability of the coverability graph instead of reachability graph for generating he threat state transition graph. Another shortfall of the methodology is that it can only accurately model the threat propagation for all known threat agents and attack vectors. But in the evolving threat space in the cyber-physical domain, the proposed methodology should be extended with a periodic automatic update of the attack vectors and thus enriching the state transition graph of the threat propagation. The proposed methodology provides the initial model of the threat propagation where all the threat states are known, but it can be extended to include unknown states using machine learning methods like Hidden Markov Models to identify the threat states based on data on the detected attacks. The proposed methodology could be used for real time prediction of the threat propagation. This might be especially helpful for evaluating conflicting countermeasures and when to activate them, based on the threat propagation over a span of time. Investigations should be made on methods to reduce the computation complexity/ computational speed to provide the threat propagation prediction within the prescribed amount of time, such that, the actuation of the countermeasure is possible before the threat reaches the main goal. This is particularly interesting feature to be part of an online threat perception system for Critical Infrastructures that can actuate varied sets of countermeasures against different cyber-physical threats that may involve unauthorized physical intrusion.

4

Resilient Design of DGA Systems

4.1 Introduction

Traditionally the distribution grid automation systems have a centralized architecture where the data from the different field devices like the measurement units and the Remote Terminal Units (RTUs) are collected centrally by the Supervisory Control And Data Acquisition System [WMB05]. The collected data is then used for the different monitoring and control applications like the State Estimation (SE), Volt/Var control, network congestion management, Optimal power dispatch, fault location isolation and optimal service restoration and so on by Distribution grid Management System/Energy Management System (DMS/EMS). These applications ensure the safety and reliability of the power grids. However, both the SCADA and the DMS/EMS are generally deployed in dedicated servers in a control centre. Any attack on these servers resulting in their failure would cause the loss of the operational capabilities with possible consequent blackout. For example, the coordinated cyber-attacks performed on the Distribution Grid Automation (DGA) system of the Ukranian DSO exploited this vulnerability [RMT]. Several decentralized distribution grid automation architectures were proposed in literature, in particular the IDE4L project [IDE][Ang+17]. In the proposed architecture, the intelligence for grid operation was allocated to individual HV (High Voltage), MV(Medium Voltage) and LV(Low Voltage) substations for managing their respective downstream grid, using the Substation Automation Unit (SAU). This reduces the computational and communication burden to the SCADA/DMS. Furthermore, each SAU is responsible for operating a specific segment of the grid and interacts with the control center and other SAUs for coordinated control of the whole power grid. The failure of a single SAU results in the failure of a segment of the grid. The SAU is equally vulnerable as the SCADA/DMS , as it is also deployed on dedicated computational hardware. Though several countermeasures have been proposed

to deal with phishing attacks, credential theft, distributed denial-of-service (DDoS) attack, killDisk attack and unauthorized VPN/Remote Terminal access[LGV13][GW13], they don't provide mechanisms that ensures availability of their functions once they have been compromised. In order to improve the availability of the grid operation functions even when the SAU is compromised, solutions were developed and presented in [Sad+18]. The authors propose a method to virtualise the grid operation functions that can be migrated from one hardware to another using Calvin IoT platform. They also investigate the effectiveness of virtualization of the functions and the latency in migration of the functions. The system is so designed that a central entity identifies the failed SAU and coordinates the migration/re-initialization of the operation functions into an another healthy SAU in the network. Similarly, the authors [Ori+20] propose a centralised architecture using Node-Red for improving the availability of a Phasor Data Concentrator (PDC) that processes Phasor Measurement Unit (PMU) measurements collected through a wide area network. However, in all of the previous works presented, the coordination of the migration of the functions was achieved by a central entity. This introduces again a single point of failure of the system. Furthermore, the coordination system is not byzantine tolerant and sensitive to status data manipulation. Additionally, the approaches do not provide a methodology to optimally place the grid operation functions considering the hardware and software capabilities of the computational resources that would host the function. Therefore, in order to mitigate the drawbacks of the previously presented works, a completely distributed coordinated scheme is proposed that uses Blockchain and smart contracts to improve the resilience of the distribution grid automation system, specifically SAU in the context of IDE4L architecture.

4.2 Exemplary DGA system: IDE4L – Its shortcomings

A decentralized automation architecture has been proposed within the IDE4L project [IDE][Ang+17], in order to improve the performance of the traditional centralised ADA system. In the proposed architecture, the individual MV and LV substations manage their respective downstream grid, using the Substation Automation Unit (SAU). The SAU enables the distribution of the grid operation intelligence to individual MV and LV substations. A SAU is a cyber-physical unit that has specific hardware and software components. From the hardware perspective a SAU is computational resource that has processing capabilities, data storage capabilities and has appropriate communication interfaces required to

communicate with other SAUs, IEDs (Intelligent Electronic Device), RTUs (Remote Terminal Units) and DMS (Distribution Management System). The different software components of the SAU form the three major layers as depicted in Fig. 4.1. The interfacing layer contains all the communication protocol translators that enable SAU to interact with different IEDs, RTUs and SAUs. The software components of the interfacing layer retrieve the data from the storage layer (mostly a database) and encapsulate in the specific communication protocol and send it (actuation command, control set point etc) to the appropriate receiver (IED-Actuator and RTUs). Furthermore, the raw data (measurements, status set points etc) received from the IEDs, RTUs and SAUs, after de-encapsulating the messages from them is stored in the instances of storage layer. Typically, the instance of a storage layer is a database. The third layer, application layer, of SAU hosts all the monitoring, control protection algorithms that are necessary for grid operation, namely, state estimation, Volt VAR control, FLISR etc.

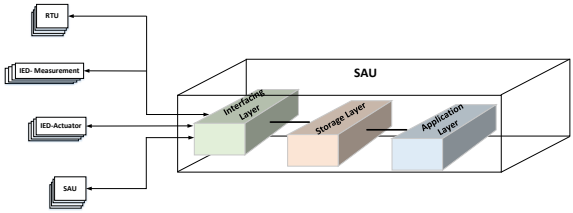


Figure 4.1: Components of SAU

The de-centralized automation architecture with SAUs for an exemplary MV grid is depicted in Fig. 4.2. The IP based secure wide area communication and standardized data modelling schemes help in realizing such a decentralized automation architecture proposed in IDE4L project. In this architecture each SAU is responsible for operating a specific segment of the grid. This reduces the computational and communication burden to the SCADA/DMS. It interacts with the IEDs configured as measurement devices (IED-Measurement), IEDs configured to control actuators and protection devices (IED-Actuator), the DMS and other SAUs (in the MV and LV grid) for coordinated control of the whole distribution grid. Depending upon the application (monitoring(control/protection) the type of data, the rate of data exchange, levels of security encryption and the communication protocol used varies. The SAU is so designed that all the software components of the SAU could be deployed in heterogenous com-

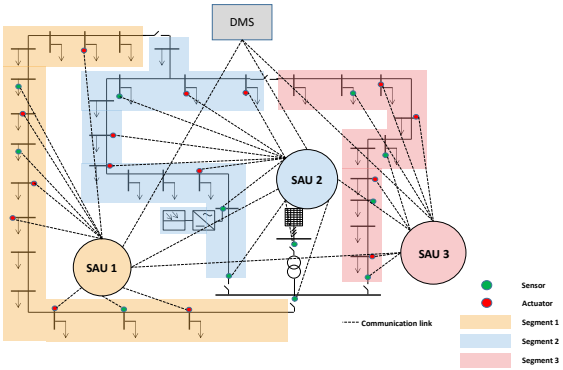


Figure 4.2: IDE4L based Distribution grid automation with SAUs: An Overview

putational hardware ranging from a single board computational devices like Raspberry PI to high performance computational servers [Ang+17].

The SAU enables the decentralization of the grid operation and thus reduces the risk of the complete blackout as each SAU is responsible for its segment. However, it should be noted that each SAU is also deployed in a dedicated hardware that is susceptible to targeted cyber-physical attacks. Loss of a SAU (hardware /Software component) means loss of grid segment operability. In the future with active distribution grids, the SAU would be the most critical component coordinating the distributed generation and load demand connected to the distribution grid. Therefore, additional resilience measures have to be deployed that ensures high availability of the SAU, specifically the algorithms that form the application layer.

The proposed methodology ensures that the algorithms hosted by the SAU that are responsible for the operation of its grid segment is made available, even when the specific SAU is compromised and thus improving the resiliency of the DGA.

4.3 Proposed methodology for improved resiliency of DGA

In this section the necessary pre-requisites, an overview of the proposed solution, and a detailed explanation of how Blockchain and smart contract are used for implementing the solution is presented. In this study, the proposed methodology is explained in the context of increasing the resilience

of the IDE4L automation architecture. Particularly, the improvement in the availability of the grid operation functions hosted by the SAUs is presented.

4.3.1 Necessary pre-requisites and assumptions

For successfully implementing the proposed solution, the following pre-requisites must be fulfilled.

- The communication network between the SAUs and the IEDs (Measurement and Control) deployed, should be so configured that every SAU is able to receive measurements and send control commands to all IEDs irrespective to the grid segment that they are deployed in.
- The Monitoring, Control and Protection Functions should be designed as executables that are platform and OS independent. This enables seamless initialisation of the functions after the migration/re-initialization in a healthy SAU. The [Sad+18] proposes a method that enables seamless virtualization of grid operation functions and initialization using CALVIN
- It is assumed that each SAU hosts services that enables identification of available communication peripheries and monitoring of available computational resources (% CPU availability, number of cores, clock rate) in real time, bandwidth utilization and available RAM in real time.
- Each SAU hosts a heartbeat service that enables the other SAUs in the network to recognise if a specific SAU is alive or is not anymore reachable within a network.

4.3.2 Overview proposed solution

In this study, the main objective of the proposed solution is to design a resilience measure that ensures higher availability of the grid operation functions (Monitoring, Control and Protection algorithms) hosted by SAU even when the specific SAU is compromised by a cyber-physical attack. A cyber-physical attack can be a targeted attack (e.g terrorist attacks) or caused by natural calamities. These attacks can result in a hardware failure or software failure that compromise the functioning of a SAU, thus hampering the operability of a distribution grid segment. The proposed solution provides higher availability of the grid operation functions by migrating/re-initialising all the grid operation functions of

the compromised SAU to a healthy SAU in the network of SAUs. An example to show the benefits of the proposed solution is depicted from Fig. 4.3-Fig. 4.5. The Fig. 4.3 shows the normal operation of distribution grid operated by three different SAUs. Each SAU hosts a set of monitoring function depicted as green square, Control function depicted as yellow square and the Protection function depicted as grey square. As depicted in Fig. 4.4 Segment 3 of the distribution grid fails due to the failure of the SAU 3. However, when the proposed solution is adopted, the algorithms are migrated to the healthy SAU.

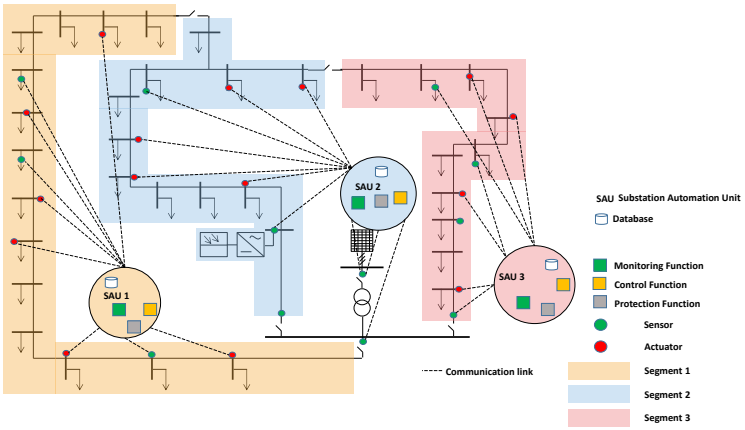


Figure 4.3: Normal operation mode with 3 SAUs

However, with the proposed solution, the monitoring, control and protection functions of the failed SAU are migrated to the other healthy SAUs. Additionally, from the Fig. 4.5 it can be seen that, the functions of the healthy SAUs are also redistributed among them. This migration/re-initialization is done by selecting a target SAU considering the hardware and software capabilities like the available computational and communication resources that are required for successfully hosting a specific grid operation function.

For a successful migration/re-initialization of the grid operation functions the following components are of absolute importance:

- An immutable ledger of the real time status of all SAUs
  - Hardware and software capabilities.

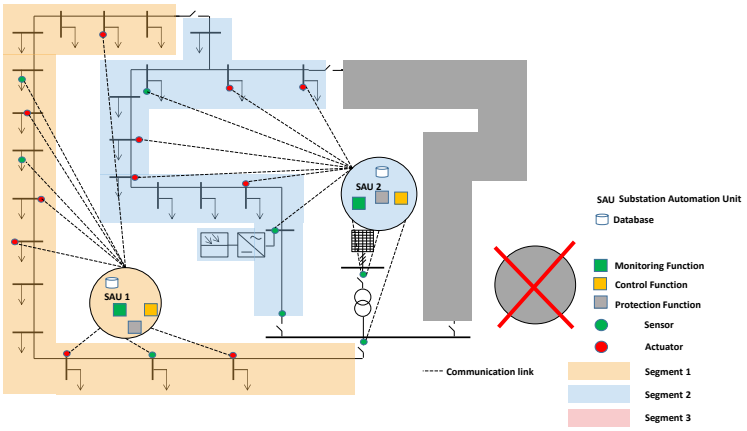


Figure 4.4: Failure of operation of Segment 3 when SAU 3 fails

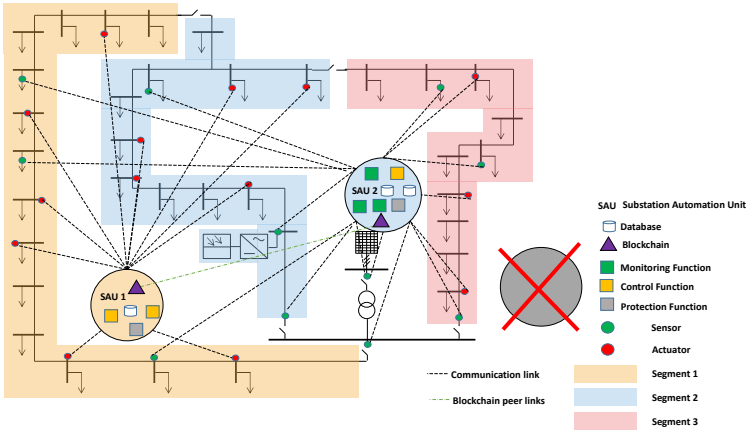


Figure 4.5: Improved availability of SAU 3 with proposed solution

– Grid operation functions currently hosted by them.

– The grid segment they currently operate

- An immutable ledger of the requirements of each grid operation function
  - Required computational and communication resource.
- An automatic triggering of an immutable logic to migrate/re-initialize the grid operation functions when a SAU fails considering the capabilities of the different SAUs (hardware and software) and the requirements of the grid operation functions.

In this study a Blockchain is used for pre-requisite (1) and (2). Whereas, a smart contract is used to implement a logic for optimally choosing the healthy SAU to which the grid operation functions hosted by the failed SAU would be migrated. A detailed explanation of the configuration of the Blockchain and the Smart contract would be presented in the subsequent sections. Furthermore, the necessary pre-requisites for implementing the proposed solution would also be presented.

4.4 Blockchain & Smart Contract: Overview

4.4.1 Blockchain Overview

Blockchain was first introduced as a underlying technology of a P2P electronic cash system i.e. Bitcoin [Nak]. Blockchain is a digital distributed ledger which is replicated and shared among all the nodes in the network [Fan+20]. It is controlled in a decentralized manner by multiple nodes running a consensus protocol [Fan+20]. It is a sequence of blocks, where each block is identified by its cryptographic hash. First block is called genesis block, which contains initial set of transactions and then the hash of this block is calculated by taking its transactions and a timestamp, as input. Furthermore, for every new block that is generated afterward, the hash is determined by taking previous block's hash together with its transactions and timestamp, as input [Rab]. As shown in Fig. 4.6, each block hash is pointing towards previous block's hash which results into chain of blocks [AM17].

Hashing [Gal17] is a process which takes data of arbitrary length as an input and then it applies a mathematical algorithm to give an output of fixed length. For example, Bitcoin uses SHA-256 as its hashing algorithm and output length is fixed to 256 bits. The main characteristics of hashing are given below [LIS]:

- If there are two different inputs (even with a minute difference), then their hash values would be different.

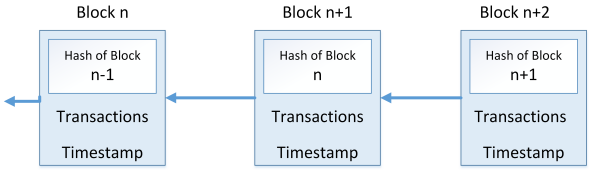


Figure 4.6: Blockchain Structure

- It is impossible to get the input back from its hash value.
- The same input always produces the same hash value
- It quickly converts data (of any size) to its hash value.

Blockchain is an append-only database which means that once the information/- data is recorded on the block then it cannot be altered afterwards. If an attacker would attempt to modify any transaction (or anything inside the block), the hash of the respective block would change and this would subsequently change the hash of all the blocks added after this block. Therefore, the attacker would need to recalculate the hashes of all the blocks that joined after the modified block. This attack is impossible to achieve without being noticed by the Blockchain members. Thus, Blockchain is a temper-proof or immutable data storage and this feature can be used to determine the provenance of information because members can trust the ledger data. Every member on the Blockchain network holds a pair of keys (i.e. public key and private key) and use the private key to produce a digital signature whenever a transaction is executed. This enables the authentication of the member and verification of the transaction's data integrity. Blockchain is a trustless environment as it is operated by unknown or untrusted participants, therefore whenever new information is submitted by the participants, it needs to be validated by all the nodes before being added to the ledger and since Blockchain is a decentralized system, there is no central authority which is responsible for management of the data on the nodes. Therefore, a consensus is the only means by which the nodes validate the new transactions and agree on the same world state. A few known consensus algorithms are the practical byzantine fault tolerance (PBFT), the proof-of-work (PoW) and the proof-of-stake (PoS).

Fig. 4.7, [SM], presents the general idea of how the Blockchain technology works. A Blockchain participant requests a transaction which is sent to all the nodes on the network. A transaction can initiate an exchange

(or transfer) of anything valuable such as cypto currency, records or data, between participants registered on the Blockchain network. Nodes validate the transaction and once it is verified, it is batched with the other transactions into a block. The nodes then append the block to their ledger. Thus, the transaction gets completed and an exchange between participants occurs.

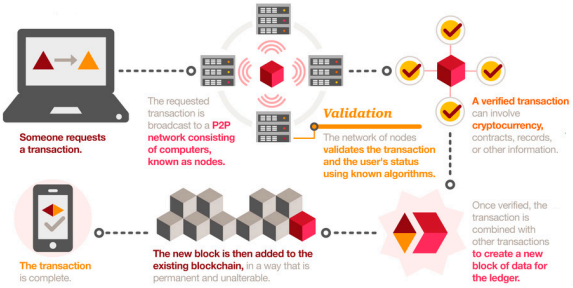


Figure 4.7: General Working of Blockchain

There are three different types of Blockchains namely the public, consortium and private Blockchain [Tah+20]. In a public Blockchain any node can join a Blockchain network and perform transactions. A private Blockchain is restricted and only authorized nodes can participate in the network. A private Blockchain is recommended when specific scalability, privacy, and other regulatory norms have to be met. A private Blockchain is also preferred when all the Blockchain operations are performed internally within an organization and the read permissions have to be restricted to a specific set of nodes. A consortium Blockchain is a kind of private Blockchain but managed by more than one organization where a selected set of nodes from different organization have read permissions and determine the consensus. In this study a private Blockchain, to be more precise a permissioned Blockchain as defined in [BG20] is used for the migration of the grid operation functions from one SAU to another. This is because the ICT infrastructure owned to operate the grid is owned by specific organisation. Each SAU is a participant and the asset exchanged is the grid operation function. Furthermore, no unauthorized SAUs are to be allowed as participants for operating the critical distribution grid infrastructure.

4.4.2 Blockchain configuration for DGA resilence

In this study, the Blockchain is configured for automatic migration of grid operation function, in that respect the Blockchain is configured for the following purposes:

- Store the attributes and operational capabilties of the different SAUs in a Blockchain.
  - Hardware resources
    - Available computational resources
    - Available storage resources
    - Communication interfaces
  - Software resources
    - Available communication protocol translators
    - Firmware compatibility (with the compromised SAU)
  - Grid operation function specific
    - Reachability to specific IEDs (sensors and actuators)
    - Average communication latency between the SAU and specific IEDs that communicated with the compromised SAU
  - Administrative attributes
    - Unique ID
    - Location
    - Current grid operation functions hosted
    - Operation jurisdiction (Grid segment it operates)
    - Priority index for migration coordination: This index helps in determining the Master SAU that takes over the initialization of the migration/re-initialization. The SAU with the highest index updates Blockchain with the ID of the lost SAU and initiates the transaction to trigger the smart contract.
- Requirements of the grid operation functions to be migrated/re-initialized
  - Required minimum computational resource
  - Necessary communication protocols
  - List of thresholds that has to be obeyed

    - Maximum communication latency between the SAU and IED allowed
  - Weights reflecting the importance of SAU resources (computational, storage and communication resources) used for optimal selection of SAU for migrating the grid operation function.
  - List of IEDs (Sensors, actuators)
  - Communication parameters of the IEDs
  - Administrative attributes
    - Unique ID
    - Location

4.4.3 Smart Contracts

Smart contract concept was first introduced by Nick Szabo [Sza] in 1994 but this idea became prominent with the emergence of Blockchain technology. Smart contracts are computer codes or programs that live on a Blockchain and encodes pre-defined rules or agreements which facilitate the exchange of assets between participants such as money, bonds, registry or anything valuable, in a decentralized, transparent and conflict-free manner. Smart contracts are present on each node in the network and are encrypted, therefore they are distributed and secure. Hence, any alteration to embedded logic cannot be done without being observed or without authorization. Figure 2.5 presents a schematic of smart contract[Del+16]. Smart contract gets executed whenever a transaction is invoked by the participant. It enforces the implemented logic with the transaction input and current state of the Blockchain. Then all the nodes verify the output in the consensus protocol and agree on the next state of the Blockchain. In order to reach a consensus, all the nodes should generate the same output for the same input, hence smart contract should be deterministic.

4.4.4 Hyperledger Fabric and Composer for Blockchain and smart contract implementation

Hyperledger Fabric [And+18] is a platform for implementing permissioned Blockchain applications, written in general purpose languages such as Java, Go or Node.js. Permissioned Blockchain means that all the members that participate in the network are associated with an identity provided by the membership service provider (MSP). In the Fabric, there is no in-built cryptocurrency, and it has an append-only ledger which is replicated on all the peers and can track the history of executed transactions. Furthermore,

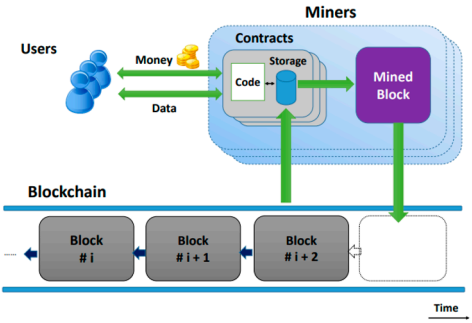


Figure 4.8: Simplified diagram of Smart Contract

the chaincode (or smart contract) implements the business or application logic which is installed on each peer. It allows interaction with the ledger and facilitates the exchange of assets between the transacting members. In the Fabric, a single Blockchain network is a channel. There could be multiple Blockchain networks possible which means different channels, among the network participants. Each channel involves certain transacting members/participants and peers, who are authorized to access that channel. Every channel has its own shared ledger and is isolated from the other channels. A chaincode is installed on the peers and instantiated on the channel and it is possible that the same chaincode is deployed on multiple channels, but each instance is isolated. Whenever a transaction occurs within a channel, a consensus takes place by the peers on the channel. Transactions occurring in one channel are not visible to members of the other channels. Thus, the Fabric provides confidentiality (or data partition mechanism) among members or participants on the same Fabric network. In the Hyperledger Fabric, there are three types of nodes [And+18]:

- `Client`: An application that submits the transaction proposal to the endorsing peers, and later broadcasts the endorsed transactions to the ordering service.

- `Peer`: A node that manages the ledger as well as the chaincode. There are two types of roles that a peer can take up:
  - `Endorser`: A peer which executes the chaincode for the submitted transactions, endorses (cryptographically signed) the results and also has the properties of `Committer` peer.

  - `Committer`: A peer which verifies the endorsements and validates the transactions.

- `Ordering Service`: A node that arranges the transactions into blocks and then delivers the blocks to all the peers for validation. The Fabric offers different implementations of ordering service:
  - `Solo`: Centralized, mainly used for prototype development.
  - `Kafka`: Offers crash fault tolerance(CFT).
  - `BFT-SMarT`[SBV18]: Offers byzantine fault tolerance(BFT).

In the Hyperledger Fabric [Sch17]the general flow of transaction starts when two or more participants join the network (or a channel). They agree upon the details of the chaincode, which is then deployed on all the peers in the channel. In addition, in Endorsement Policy, the condition of endorsement (cryptographically signing the data) is specified, for example, a condition like A and B or C and D means either Peer A and Peer B should endorse the transaction, or Peer C and Peer D should endorse the transaction. These peers become endorsers.

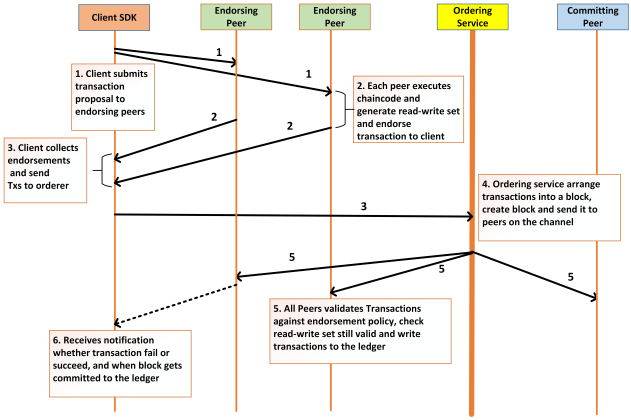


Figure 4.9: Transaction Flow in Fabric

As depicted in Fig. 4.9[And+18], Client sends the transaction proposal to the peers mentioned in the endorsement policy. The transaction proposal includes Chaincode ID, Client ID, Timestamp and Transaction payload. Each endorsing peer executes the specified chaincode (or smart contract) and generates a read-write set based on their current Blockchain state.

Then each peer signs the results (contain read-write set, endorser ID, transaction ID) and returns them to the client. At this stage, peers do not perform any update to the ledger. Client sends the transaction (results), satisfying the endorsement condition, to the ordering service. The ordering service collects multiple transactions and groups them into blocks depending upon configuration parameters (such as Batch Timeout and Batch Size). The Ordering service just arranges the transactions but does not see the details of transactions. It delivers the blocks to all the peers for validation and commitment to the ledger. All peers (Committers as well as Endorsers) receive the blocks and for each transaction in a block, they verify the endorsements (signatures) and validate if read set is still valid based on current ledger state. Then they accept or reject the transaction and, in the end, the block is appended to ledger. Furthermore, Client is also informed by peers when the transaction is accepted or rejected, and when block gets committed to the ledger.

The Hyperledger Composer [Hyp] is an open-source framework which simplifies and accelerates the development of the Blockchain applications. Using the Composer, a Blockchain business network can be designed rapidly, built and deployed on top of the Blockchain platform i.e. Hyperledger Fabric. A Composer business network definition consists of the following components:

1. `Model File`: In the Composer Blockchain network, there are mainly four entities or resources such as *Assets*, *Participants*, *Transactions* and *Events*. Participants submit the transactions in order to exchange assets between each other and also the participants can subscribe to events which can be emitted from the transaction logic. All of these entities are defined in this file using the Composer modeling language.

2. `Script File`; The logic (or transaction processing function) for each transaction is defined in this file and it is coded in JavaScript. Basically, it's a smart contract of the Blockchain application.

3. `Query File`: Queries can be defined to fetch filtered data of resources (assets, participants and even transactions) from the ledger. Queries can be executed by transaction processing functions or the Composer REST server.

4. `ACL`: Rules defined for participant roles (present in the Composer model) which describe the permissions to perform operations (i.e. create, read, update and delete) on the network resources (assets, participants or transactions).

In Fig. 4.10, a basic architecture of Composer network deployed on the Fabric Blockchain is shown.

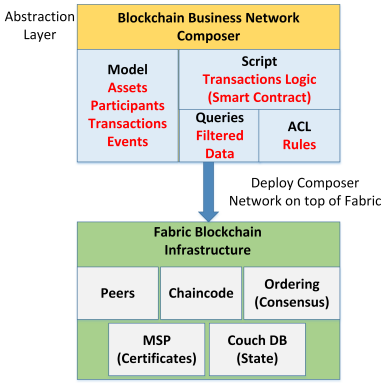


Figure 4.10: Composer Network runs on Fabric

4.5 DGA system configuration for resilience improvement

The Smart Contract is used for implementing the logic of optimal migration/re-initialization of the grid operation function. However, before that the grid operation functions have to be virtualized for easy migration/re-initialization. For this purpose CALVIN IoT platform is used in this study. A short description of the CALVIN framework is provided below. Subsequently the Blockchain & Smart Contract configuration of the complete DGA system is also presented.

4.5.1 CALVIN IoT platform

Calvin is an open-source framework, written in Python, for developing and deploying distributed IoT applications. It combines the concept of actor model and flow based programming. Figure Fig. 4.11 shows the layer stack of the Calvin platform[PA15]. `Calvin Runtime` is the abstraction layer of underlying platform (operating system and hardware) and it is divided into two parts i.e. platform dependent and platform independent. The platform dependent part manages data transfer between actors, communication between Runtimes, and also provides an abstraction of services, such as I/O and sensing capabilities, to actors. On the other hand, the platform

independent part handles scheduling, coordination between Runtimes, migration and provides an interface to the actors.

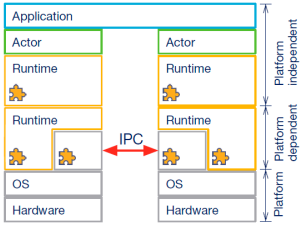


Figure 4.11: Layer Stack of Calvin

Furthermore, each Runtime has a REST API to control it and the related actors. It includes the creation of new actor(s), retrieval of the current state of the Runtime or actor and migration of the actor between Runtimes[Sad+18]. An application is formed by a combination of actors; whereas, an actor is a reusable software component which executes a coded function that takes values from the inports and writes results to the outports. Thus, actors are linked to each other using these ports. A unique feature of Calvin is that it enables migration of actors between Runtimes. During migration, an actor state has to be sent from the old Runtime to the new Runtime so that the same actor instance can be created on the new Runtime. Migration can be triggered by sending a request to host Runtime REST API, including the new Runtime's ID and actor's ID as request inputs. The speed of migration depends on the actor's state size, the involved hardware's processing power and speed of the data transfer.

The CALVIN IoT platform helps in implementing individual grid automation functions (state estimation algorithm, volt-var oprimization algorithm, FLISR algorithm, congestion management algorithms etc) as individual actors (or set of actors). These actors can then be freely activated/initialized /migrated from one Runtime to another. In the context of IDE4L based DGA system, the SAU could be considered as a single CALVIN Runtime. Thus CALVIN helps in virtualizing the SAU and power grid automation functions. Each grid operation function (monitoring, control and protection algorithms) could be programmed as single or multiple actors. The actors can either be snippets or complete grid operation function which could be distributed in various Runtimes. Thus enabling a complete virtualization of the grid operation functions and achieve fully distributed operation of the DGA. In this study a single grid operation function is configured as an actor.

A detailed analysis of how CALVIN could be used for distributed grid automation is presented in [Sad+18]. In this study, a state estimation algorithm is considered as an actor and a set of SAUs as the Runtimes. The availability of the state estimation when it was configured as a single actor and divided into a set of actors is presented in [Sad+18]. The current study utilizes the virtualization functions offered by the CALVIN IoT platform, its API to freely allocate the actors in the Runtimes, get the current configuration of the Runtimes (software, hardware capabailities and availability), The actor configuration in each Runtime, identification of available Runtimes using a heartbeat function, and utilize the proprietary protocol to interact with actors and exchange data.

CALVIN is just one part of the DGA system configuration that enables grid operation function virtualization and facilitates API for migration of the actors. But the actor configurations and the Runtime configurations have to be properly stored in a Blockchain so that the smart contracts could be designed that optimally choose which actor should be allocated to which Runtime. Therefore, in this study, the IDE4L DGA system SAUs have to be configured not only to support the CALVIN IoT platform but also the Blockchain framework , which in this case is the Hyperledger Fabric. A detailed explanation of the DGA system configuration with the different steps involved in reaching a consensues on the ownership of the asset (Grid operation function) by the different participants (SAUs) is provided.

4.5.2 DGA system configuration: Blockchain perspective

The Hyperledger Fabric uses the Blockchain framework to improve the resilience of the IDE4L based DGA system. The Fabric network consists of different entities, namely, the peer nodes, ordering service nodes and client nodes from different organizations. To implement the proposed solution the SAUs are considered to act as both client and a peer in the Fabric network. Each SAU is installed in a Primary substation (Medium Voltage Substation) (from Now on called as PSAU) and Secondary Substation (LV substation) (From now on called as SSAU). According to the IDE4L architecture, several SSAUs report data from their secondary substation to a set of PSAUs for coordination of the automation of a section of the distribution grid. Furthermore, PSAUs interact with each other to coordinate the complete distribution grid automation. Since the PSAUs play a major role in coordination, the computational resources, memory storage resources and network connectivity of the PSAUs are generally higher than that of the SSAUs. Furthermore, the number of PSAUs in a distribution grid is lower than the number of SSAUs. This is due to the

inherent radial design of distribution grids. Taking these aspects of the PSAUs into consideration, the peer hosted by the PSAUs are configured as an endorsing peer and that of the SSAUs are configured as committing peer. To separate the critical ordering functions from the endorsers, separate ordering service nodes need to be deployed. A detailed explanation on the deployment specifics of the ordering nodes is out of scope , however, it is assumed that appropriate configuration of OSNs (Ordering Service Nodes) and the Kafka/Zookeeper clusters, as suggested in [TNV18], is done to enable efficient management of the broadcasted transactions from the PSAUs and SSAUs.

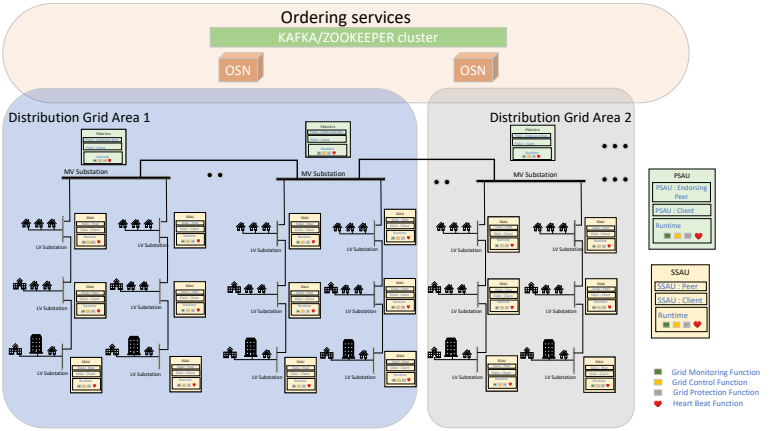


Figure 4.12: DGA System Configuration with CALVIN and Hyperledger Fabric

An overview of the entities involved in the Fabric network is as given Fig. 4.12. The transaction flow in Hyperledger has four major phases [TNV18].

- Endorsement phase: The clients in SSAUs and the PSAUs generate transaction proposals signed with their credentials to all PSAUs in the same distribution grid area. The endorsing peer of the PSAU checks if the client is authorized to invoke such a transaction and signs the transaction response and replies it to the respective clients. The client checks if the transaction response bears the signature of the endorsing peer.

- Ordering phase: After the check, the client generates a well-formed transaction and broadcasts it to the ordering service. An Ordering Service Node (OSN) participates in the consensus protocol and cuts block of transactions which is delivered to the peers by a gossip communication protocol.

- Validation phase: All peers (endorsing and committing) check for the identity of the orderer from the blocks of transaction that were received from the ordering service and perform validation as mentioned in [TNV18]

- Ledger update phase: Once the validation is done the transaction is updated in the local ledger.

Once the DGA system is configured as mentioned above, where the assets are the CALVIN actors, participants are the SAU's Hyperledger Clients, then the Smart Contracts can be configured that enables automatic exchange of assets (actors) between the participants (SAUs) in such a way that the assets are always owned by the most optimal participant that has enough resources to host the asset. In this study, a MADM approach based optimal selection of the SAUs is proposed. The logic of the MADM approach is coded as a smart contract. A detailed explanation is provided in Sect. 4.6.

4.6 Smart Contract Configuration: MADM based optimal allocation of DGA functions

Smart contracts are self-executing codes that automate the workflows or processes. They reside on Blockchain nodes and hence are decentralized and cryptographically secured. Therefore, alteration or changes in the smart contract code is impossible without being noticed.

A smart contract is triggered by a transaction. It then executes automatically in a specified way on each node on the network, based on the data inserted in the submitted transaction and smart contract's world state i.e. the data stored on the Blockchain node. Smart contracts eliminate the need of a third-party to facilitate the exchanges between transacting parties (or devices) as all network nodes execute the contract and reach a consensus on the produced output [MG17]. In case, a node is malicious or altered, then it will produce disparate results and prevent the network from reaching a consensus. So, due to its non-deterministic nature, the transaction will be rejected. Additionally, all transactions are digitally signed and stored in an immutable ledger which preserves data integrity,

and enables historical tracking or data verifiability. Hence, because of all these characteristics, Blockchain based smart contracts give us an opportunity to improve the grid automation resiliency [MG17].

The integration of Calvin with a Blockchain application will create a peer-to-peer marketplace [CD16] where all Runtimes can trigger transactions automatically and migrate/allocate actors among themselves. This idea is very similar to exchanging assets, such as bitcoin or land registry, via Blockchain. As shown in 4.13, the SAU (*Runtime 1*), which is hosting applications *App 1* and *App 2*, submits a migration transaction to the Blockchain network automatically, which then executes the pre-defined logic of a smart contract leading to the migration of *App 1* to *Runtime 2*. Once the actual migration is complete, the smart contract also updates the Blockchain state to maintain synchronization. Thus, the application of Blockchain in power grid automation can be of significant importance. In the following sections, the different modes of allocation and the design of the allocation algorithm, implemented using smart contract, for the selection of the optimal target Runtime is explained.

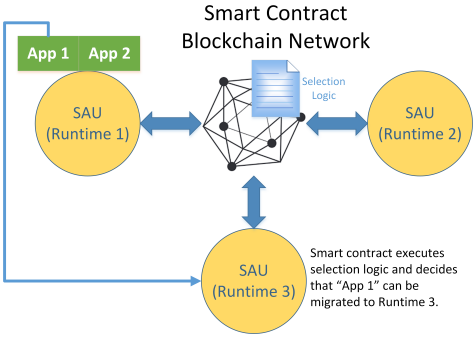


Figure 4.13: Smart Contract based Migration

4.6.1 Modes of migration

In this section, two different approaches, i.e. periodic migration and Runtime failure migration, to trigger the migration of actors are presented.

Periodic migration

Using this technique, the system can reduce the risk of cyber-physical attack by providing a security by obscurity measure as the location of the

actors is not fixed and it would be difficult for any attacker to predict the location of the actor's future deployment. As shown in figure Fig. 4.14, the application (grid operation function) (*App 1*) is running on *Runtime 1* can be attacked or is currently under attack and is still active. Suppose if a recurring migration gets triggered on *Runtime 1* before the Runtime fails, then the actor will be migrated to a new Runtime and the attack will be mitigated. Also, the attacker will not be able to immediately predict the new location of the actor as the destination Runtime will be chosen randomly by the smart contract. Therefore, periodic migration can make the system more robust and reliable.

Steps for performing the migration are mentioned as follows,

1. Each Runtime is in operation and triggers migration automatically at fixed time intervals

2. Runtime submits a Blockchain transaction which executes a smart contract logic

3. Smart contract produces an output which includes the destination Runtime ID, the migration actor's ID and the actor's state

4. Current Runtime performs actual migration using the smart contract's output. This task is independently performed by the Calvin platform. Therefore, details of how Calvin performs migration can be referred to in [Eri]

5. If migration is successful, then the current Runtime submits another transaction to update the Blockchain state, i.e. update the ownership of the migrated actor

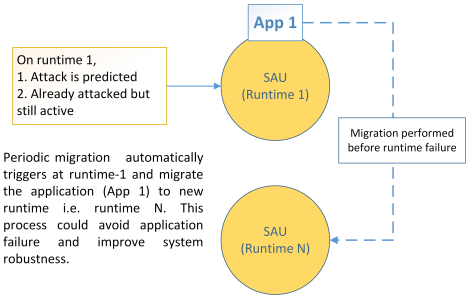


Figure 4.14: Automatic Migration Periodically

Runtime failure migration

In case of Runtime failure, all the actors running on this Runtime need to be re-deployed or migrated to a new execution environment so that service downtime can be minimized. In Blockchain, the state of each actor is securely saved at regular intervals and the last saved state can be used to handle the failure. An actor's state contains connection information such as inports and outports, and this could be useful in re-deployment. This method looks similar to the checkpoint/restart technique [Tre05]. In this section, a method for the re-deployment of actors of a failed Runtime is proposed as follows,

1. A heartbeat actor, running on each Runtime, checks periodically if other Runtimes are working or not. When a Runtime fails, all other Runtimes on the same network will discover its failure because they will not receive a heartbeat signal from the failed Runtime [SBL17]

2. All other Runtimes on the same network will stop their periodic migration

3. A new operational Runtime needs to be selected which will be responsible for re-deploying the actors of the failed Runtime

4. Selected Runtime will submit a Blockchain transaction which contains the failed Runtime's ID

5. Smart contract will process the transaction and choose the new optimal Runtime for the placement of an actor of the failed Runtime. It will generate results which include the destination Runtime ID, actor ID (actor to be re-deployed) and the actor's state (last saved state before the failure)

6. Selected node will analyze the actor's state, re-configure the actor ports and then initiate the deployment of the actor on the chosen destination Runtime

7. If deployment is successful, the selected node will submit another Blockchain transaction to update the ownership of the re-deployed actor

8. The selected node will repeat steps from 3 to 5 until all the actors of failed Runtime have been re-deployed

9. After finishing re-deployment, the selected Runtime will submit a Blockchain transaction to update the status of the failed Runtime

so that the smart contract's logic does not consider this Runtime in its Runtime selection process

10. The selected Runtime will inform other Runtimes to re-start their periodic migration

In this section, only interactions with the Blockchain network, as shown in Fig. 4.15, are presented. The tasks involved in step 1,2,3,6 and 10, is implemented in Calvin platform and is presented in [Sad+18].

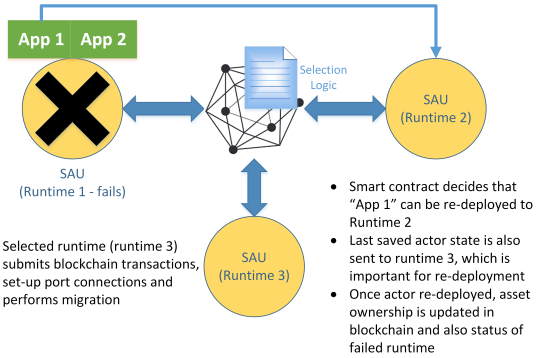


Figure 4.15: Runtime Failure Migration

4.6.2 MADM based optimal selection of deastination Runtime

Selecting an optimal destination Runtime for actor migration is a two-step mechanism, i.e. selection of capable Runtimes and application of Multi Attribute Decision Making (MADM), which are explained as follows.

Selecting capable Runtimes

In this study, it is assumed that all the Runtimes (or SAUs) are on the same network, with an established connection between them as shown in Fig. 4.16. The goal of the first step is to select Runtimes that satisfy the list of requirements as described below. These selected Runtimes are capable of hosting an actor but the most optimal one will be chosen using the MADM approach, presented in Sect. 4.6.2.

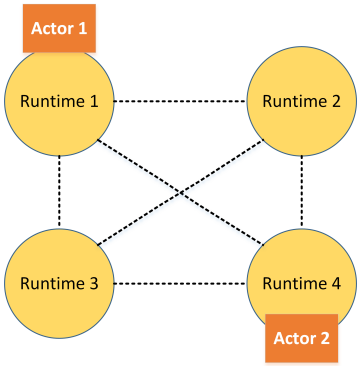


Figure 4.16: Computational Network

List of requirements

1. Runtime status should be operational
2. Actor deployment requirements should match with Runtime attributes [Gil16]
   - As shown in Fig. 4.17, an actor's requirements could be its execution location (or address) and should match with the Runtime's location (or address). When an actor needs to be migrated, the smart contract logic will consider only those Runtimes, for placement, which will be on the same connected network (or same static location). This enables geolocation based resource optimization of DGA systems.

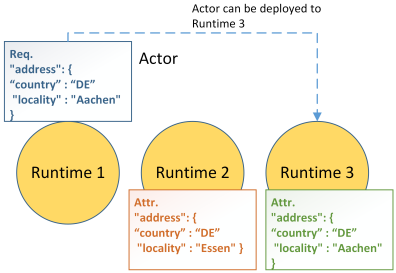


Figure 4.17: Requirement Matching with Attributes and Migration

3. Runtime capabilities should contain all the functionalities needed by an actor for its execution.
    - For example, an actor `io.print()` prints data to the Runtime's console (or outport) [Eri]. It requires `calvinsys.io.stdout` CalvinSys module for its execution. For the actor's deployment, a new Runtime should contain `calvinsys.io.stdout` in its capability list.

4. A Runtime should have enough computational resources as assumed and shown in Tab. 4.1

Resource	Value
Available CPU (%)	$> 20\%$
Available RAM (GB)	> 2GB
N/W BW Utilization (%)	$< 80\%$

Table 4.1: Computational Resources

5. An actor can be connected to a remote intelligent electronic device (IED) as shown in figure 4.18. Every Runtime should have a heartbeat actor running and measuring the Round Trip Time (RTT) to the remote IED. Using the RTT, link latency can be estimated and it is an important parameter for applications that require low-latency connections, especially for high critical FLISR applications. Each capable destination Runtime's RTT value should be below a certain threshold.

Whenever a Runtime triggers migration, the smart contract retrieves the parameter's values, mentioned in the requirements list (Sect. 4.6.2), from the Blockchain ledger. Therefore, these values should be updated periodically by other Blockchain transactions, which facilitates the smart contract's decision making on the latest timestamped data.

Overview Smart Contract logic with MADM

Multi Attribute Decision Making methods (MADM) are extensively used in solving problems when there exits a set of feasible alternatives which need to be analyzed and evaluated with respect to a set of, usually conflicting, attributes. The aim of MADM is to determine the best alternative or rank the alternatives [Yue11]. MADM has been used in various sectors such as finance, manufacturing, economics or cloud computing.

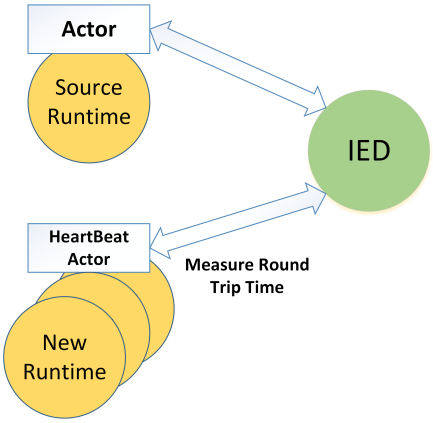


Figure 4.18: Measuring Round Trip Time

The information required to make a decision in MADM problems, comprises of attributes' values and attribute's weights. The weights define the importance of the attributes and the values provide details on the capability or characteristics of the alternatives [Din+16]. Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), a well known MADM approach, is applied in our problem, i.e. the decision to select the most appropriate destination Runtime for actor migration. The alternatives are the capable destination Runtimes as obtained from Sect. 4.6.2 and the attributes include the Runtime's computational resources such as CPU, memory, network bandwidth, cores, clock rate and round trip time. Another MADM method, Analytical Hierarchy Process (AHP), is used to calculate weights of the attributes [JM17]. The general flow of MADM approach is shown in figure 4.19.

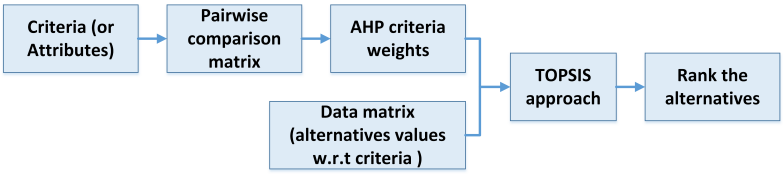


Figure 4.19: General Flow of MADM method

Analytical Hierarchy Process (AHP)

AHP method is a useful and effective technique, developed by [Saa87], for solving complex decision making problems. It breaks down the problem into a hierarchical structure of the goal, attributes (or criteria) and alternatives as shown in Fig. 4.20. In our model, the AHP method is used to compute the weight for each attribute by carrying out pairwise comparisons of the attributes, which is done by the decision makers or experts. The importance of an attribute is directly proportional to its weight.

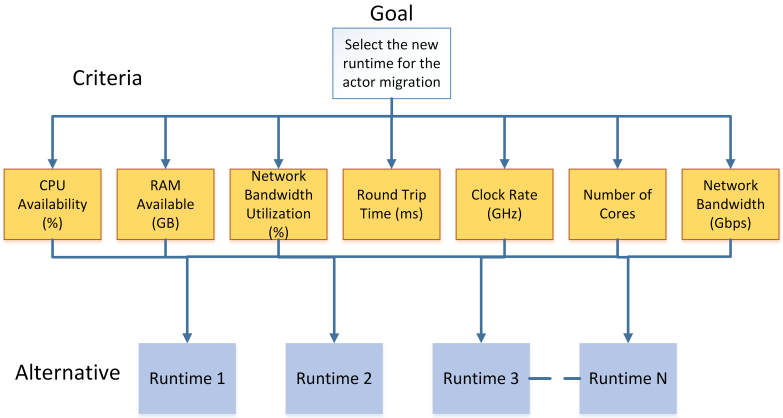


Figure 4.20: Decision Problem

The steps for calculating the weights for the attributes are explained below.

1. Create a pairwise comparison matrix A. The matrix A is a m x m matrix where m is the number of attributes (or criteria). In matrix A, each item a_{ij} represents the importance of j^{th} attribute in relation to i^{th} attribute. The numerical value assigned to each item in matrix A is derived from the Tab. 4.2, [Saa87].

$$A = \begin{bmatrix} 1 & a_{12} & a_{13} & a_{14} & \dots & a_{1m} \\ \frac{1}{a_{12}} & 1 & a_{23} & a_{24} & \dots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1m}} & \frac{1}{a_{2m}} & \frac{1}{a_{3m}} & \frac{1}{a_{4m}} & \dots & 1 \end{bmatrix} \tag{4.1}$$

Intensity of Importance	Interpretation
1	Equal Importance
3	Moderate Importance
5	Strong Importance
7	Very Strong Importance
9	Extreme Importance
2,4,6,8	Intermediate values between the two adjacent judgments

Table 4.2: Pairwise Comparison Scale

2. Compute the normalized pairwise comparison matrix A_{norm} from matrix A. Each entry $\overline{a_{ij}}$ in matrix A_{norm} is calculates as shown below

$$\overline{a_{ij}} = \frac{a_{jk}}{\sum_{l=1}^{m} a_{lk}} \tag{4.2}$$

3. The weight of each attribute (or criteria) w_j is calculated by taking the average of each row in A_{norm}

$$w_j = \frac{\sum_{l=1}^{m} \overline{a_{jl}}}{m} \qquad j = 1, ..., m \tag{4.3}$$

4. There could be inconsistencies when pairwise comparisons are performed by the decision maker [Saa87]. The consistency of matrix A can be checked by computing the consistency ratio (CR). If CR is less than 10%, then the matrix is consistent and the calculated weights can be used further but, if not, then the decision makers have to improve the judgment and recreate the comparison matrix A.

$$CR = \frac{CI}{RI} \tag{4.4}$$

$$CI = \frac{\lambda_{max} - m}{m - 1} \tag{4.5}$$

where CI is the consistency index, RI is the random index, m is the dimension of the matrix and λ_{max} is the average of eigenvalues.

RI is calculated from the average CI of 500 randomly filled matrices. The calculated values of RI for (m<=10) are shown in Tab. 4.3

m	2	3	4	5	6	7	8	9	10
RI	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Table 4.3: Values of RI

TOPSIS

TOPSIS technique, developed by [HY81], is a MADM approach that ranks the alternatives by calculating their distances from the positive ideal solution and the negative ideal solution at the same time. The best or optimal alternative is closest to the positive solution and furthest from the negative solution[Yue11]. Each attribute is either a benefit attribute or cost attribute. The positive ideal solution is a set that contains the maximum values of the benefit attributes and minimum values of the cost attributes, whereas the negative ideal solution contains the minimum values of the benefit attributes and maximum values of the cost attributes.

The procedure for the implementation of TOPSIS is mentioned below.

1. Create a Decision Matrix (D) with m rows and n columns, where $(A_1, A_2, ...A_m)$ are m alternatives and $(C_1, C_2, ...C_n)$ are n attributes (or criteria). In the decision matrix, each entry x_{ij} is the monitored value of i^{th} alternative with respect to j^{th} attribute [MLL12][DBA15].

$$D = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \tag{4.6}$$

2. Calculate the normalized decision matrix (r_{ij}) using the following formula:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{l=1}^{m} x_{ij}^2}} \tag{4.7}$$
$$i = 1, ..., m, j = 1, ..., n$$

3. Calculate the attribute(or criteria) weight matrix W. The weight of each attribute w_i is calculated using AHP method as shown in Sect. 4.6.2.

$$W = \begin{bmatrix} w_1 & \dots & \dots & 0 \\ \vdots & w_2 & \dots & \vdots \\ \vdots & \dots & w_i & \vdots \\ 0 & \dots & \dots & w_n \end{bmatrix} \tag{4.8}$$

4. Calculate the weighted normalized decision matrix (v_{ij}) by multiplying each attribute weight (w_j) with its corresponding column in normalized decision matrix (r_{ij})

$$v_{ij} = w_j * r_{ij}, j = 1, 2, ..., n, i = 1, 2, ..., m \tag{4.9}$$

where w_j is the weight of j^{th} criterion and $\sum_{j=1}^{n} w_j = 1$

5. Determine the positive ideal solution (A^+) and the negative ideal solution (A^-) using the weighted normalized decision matrix (v_{ij})

$$\begin{aligned} A^+ &= \{(max_i v_{ij} | j \in B), (min_i v_{ij} | j \in C)\} \\ &= \{v_1^+, v_2^+, ..., v_n^+\} \\ A^- &= \{(min_i v_{ij} | j \in B), (max_i v_{ij} | j \in C)\} \\ &= \{v_1^-, v_2^-, ..., v_n^-\} \end{aligned} \tag{4.10}$$

Where B is the benefit attribute and C is the cost attribute.

6. For each alternative, calculate the separation (S_i^+) from the positive ideal solution and the separation (S_i^-) from the negative ideal solution

$$\begin{aligned} S_i^+ &= \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^+)^2} \\ S_i^- &= \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^-)^2} \\ i &= 1, ..., m \end{aligned} \tag{4.11}$$

7. Compute the relative closeness coefficient (RC) for each alternative using its separations

$$RC_i = \frac{S_i^-}{S_i^+ + S_i^-} | i = 1, ..., m \tag{4.12}$$

8. Rank the alternatives according to their relative closeness (RC_i). The higher the value of RC_i, the better is the alternative A_i.

Smart contract selects the Runtime (or alternative) with the highest relative closeness and then the selected actor is migrated to this Runtime. Therefore, whenever there is a actor which needs to be migrated, smart contract performs logic as described in Sect. 4.6.2 and Sect. 4.6.2 to determine the best or optimal Runtime for actor placement.

4.7 Proof of Concept implementation: Resilient DGA

In this section, the implementation details of Blockchain proof-of-concept (PoC) for the proposed concept i.e. grid operation function migration, is presented. The goal is to utilize the key features of Blockchain technology. The developed solution demonstrates:

1. The integration of the architecture presented in [Sad+18] with Blockchain technology
2. The data storage into the Blockchain ledger
3. The execution of migration process using Blockchain.

This solution can be used by future researchers as a basic opertaional platform for creating new applications or to gain educational understanding about blockhain, smart contracts and its application in DGA resiliency. At first, the scenario along with the architecture and the development environment are described. Afterwards, the details regarding the Blockchain prototype implementation are presented.

4.7.1 Scenario

The assumed scenario is as follows: some substation automation units (SAUs) are interconnected and running grid applications (grid operation functions) such as State Estimation or Volt VAR Control, as shown in Fig. 4.21. These applications would be receiving data from remote intelligent electronic devices (IEDs). Each SAU submits Blockchain transactions in order to insert or update its configuration data as well as application

data into the Blockchain ledger. Based on pre-defined logic in smart contract, SAUs perform automatic application migration among themselves.

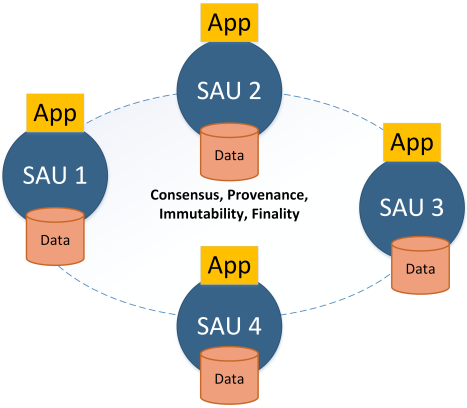


Figure 4.21: SAUs Network

4.7.2 Prototype architecture

The architecture of the implemented prototype is shown in Fig. 4.22. Calvin IoT[Eri18] platform is used for developing and deploying SAUs functionalities and its applications. Implementation in Calvin is out of scope of this thesis. Hyperledger Composer[Hyp18] is used for building Blockchain business network whereas Node-RED[Nod18a] tool is used to integrate Blockchain with Calvin platform.

The internal mapping is shown in Fig. 4.23. For each Calvin Runtime, a participant is created in the Blockchain and for each Calvin application or actor, an asset is created. In Node-RED, in-built nodes are used to receive data from Calvin Runtimes or vice-versa, and to submit transactions to Composer Blockchain network. Node-RED is a flow-based programming tool for rapidly building Internet of Things applications i.e. to wire together hardware devices, APIs or existing online services[Nod18a]. It provides browser-based graphical tool for integrating predefined nodes (written in JavaScript). These nodes can receive data, process data and output data.

In this study, Node-RED is specifically used to integrate Calvin REST API with Hyperledger Composer Blockchain network. For example, in Node-RED, `Http` node is used to send `GET` or `POST` request to external

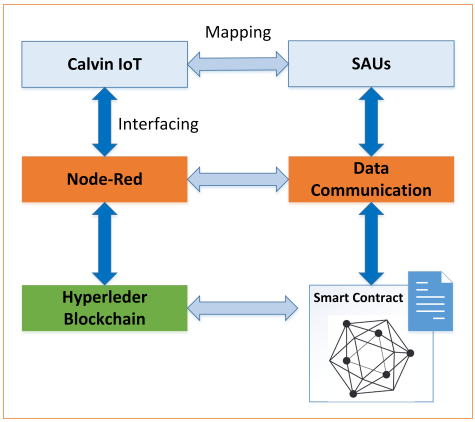


Figure 4.22: System Design

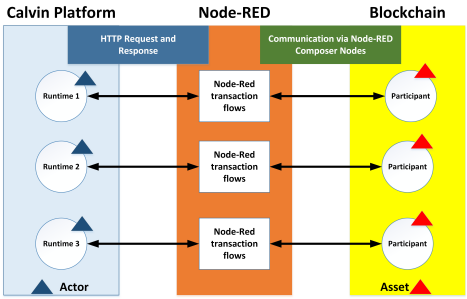


Figure 4.23: Mapping between Calvin and Blockchain via Node-RED

REST API and `function` node is used to process data. Moreover, external package i.e. `node-red-contrib-composer` is used which provides nodes required to interact with Composer network in order to perform activities as follows[Nod18b]:

- Submit Blockchain transaction
- Read, update and delete assets and participants
- Subscribe to events

4.7.3 Environment setup

The machine (or computer), used for application development, needs to be equipped with the right configuration. At first, all the prerequisites, given in Tab. 4.4, are installed and then the Hyperledger Composer (v0.19.1) development environment tools are installed as given at [Hyp18]. In this process, the default Fabric network (v1.1.0) dependencies are also downloaded. The default Fabric can be started to create a single peer Blockchain network. However, the Fabric network binaries and configuration files can also be downloaded separately from [Fab17] and configured to setup two or more peer Blockchain networks. After completing the installation, the business network is defined using the Composer which is explained in the next section.

Operating System	Ubuntu Linux 14.04/16.04 LTS (both 64-bit)
Memory	minimum 4GB
Docker Engine	Version 17.03 or higher
Docker-Compose	Version 1.8 or higher
Node	8.9 or higher (version 9 is not supported)
npm	v5.x
git	2.9.x or higher
Python	2.7.x
Code Editor	VSCode

Table 4.4: Development Tools Prerequisites

4.7.4 Composer Business Network

A Composer business network is defined for the selected scenario as shown in Fig. 4.24. In further subsections, this model is discussed in detail.

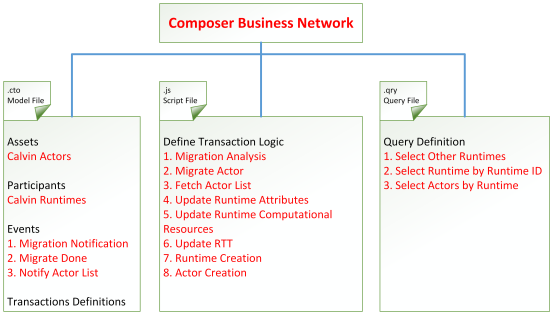


Figure 4.24: Composer Business Network

Data Model

In this section, the model definitions of assets, participants and events are presented. Runtime is a participant which is uniquely identified with `uuidNode`. Each Runtime contains the list of actors, `actorList`, running on it. An actor is an asset which is uniquely identified with `uuidActor` and each actor is linked with one Runtime, represented by `Runtime` field, which means that the actor is being executed on that particular Runtime at that moment. In addition, there are many other variables in the actor and Runtime structure which are used in the transaction processing logic. Furthermore, the list of all the member variables and their types, in actor and Runtime definition are shown in Fig. 4.25.

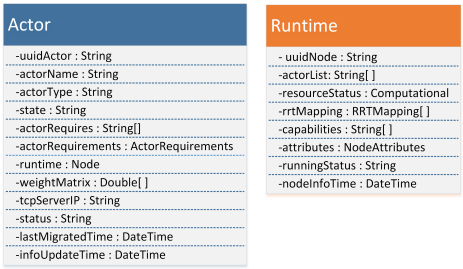


Figure 4.25: Actor and Runtime Definition

In the Composer network, events are defined in the model file and are emitted by the specified transactions in their respective transaction processing function[Hyp18]. In our model, external application, i.e. Node-RED, is subscribed to defined events in order to get some important information when a specified transaction is committed to the ledger and utilizes the emitted data to process another transaction. Three different events i.e. `Migration Notification`, `Notify Actor List` and `Migrate Done`, are defined as shown in Fig. 4.26.

Migration analysis and execution

Migration of an actor from an old Runtime to a new Runtime is a two step process. The overall transaction execution flow is shown in Fig. 4.27.

1. At first, *MigrationAnalysis* transaction is submitted by the Runtime. The logic of this transaction is responsible for selecting the actor for migration and deciding the best new Runtime for actor placement, as shown in figures Fig. 4.28,Fig. 4.29,Fig. 4.30. When a transaction

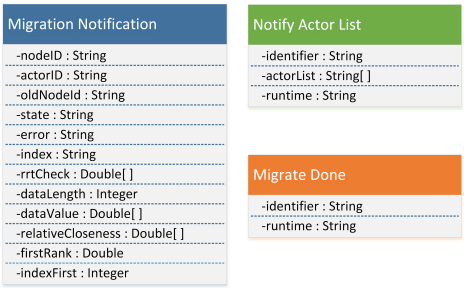


Figure 4.26: Events Definition

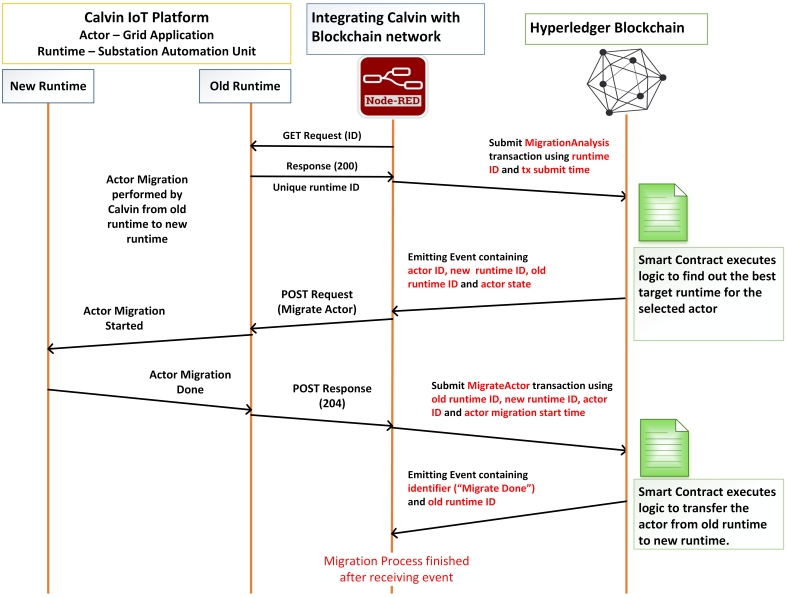


Figure 4.27: Migration Analysis Tx Flow

gets committed to the ledger, an event *MigrationNotification* is emitted which contains results of migration analysis such as actor ID (i.e. actor to be migrated), old Runtime ID (i.e. current Runtime which is already hosting the actor), new Runtime ID (i.e. new target

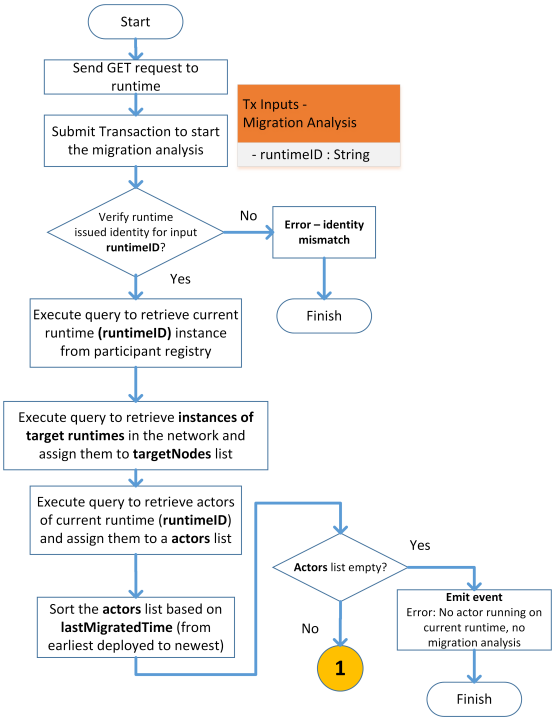


Figure 4.28: Migration Analysis Tx Processing Logic(Part-1)

host chosen after migration process) and the actor's state. The error handling for this transaction is shown in Fig. 4.32.

2. The second step involves the submission of POST request to the old Runtime with migration analysis details followed by the migration of the selected actor to new Runtime. After successful migration, a POST Response is received which is used to submit *MigrateActor* transaction. The submitted transaction invokes the logic as explained in Fig. 4.31. This transaction transfers the ownership of the actor from the old Runtime to the new Runtime. This is equivalent to updating the actor list of both the Runtimes along with changing the link (pointer) connecting the actor and the Runtime. The error handling for this transaction by Node-RED is shown in Fig. 4.33.

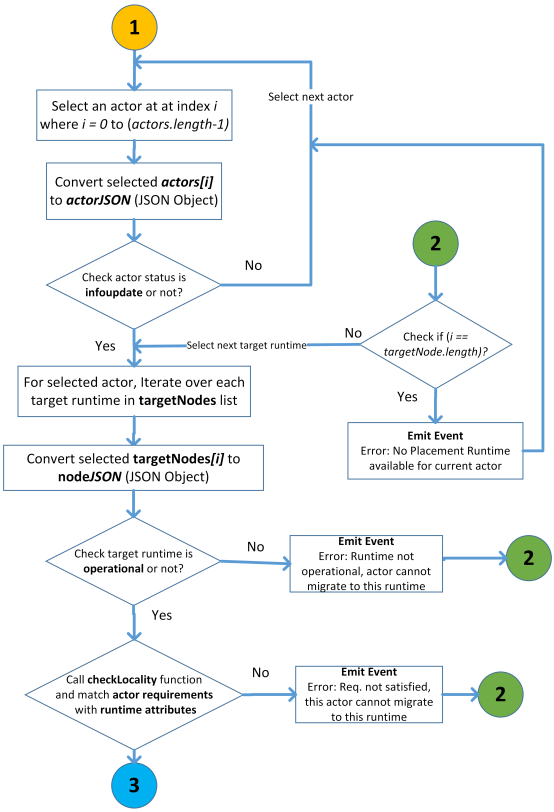


Figure 4.29: Migration Analysis Tx Processing Logic(Part-2)

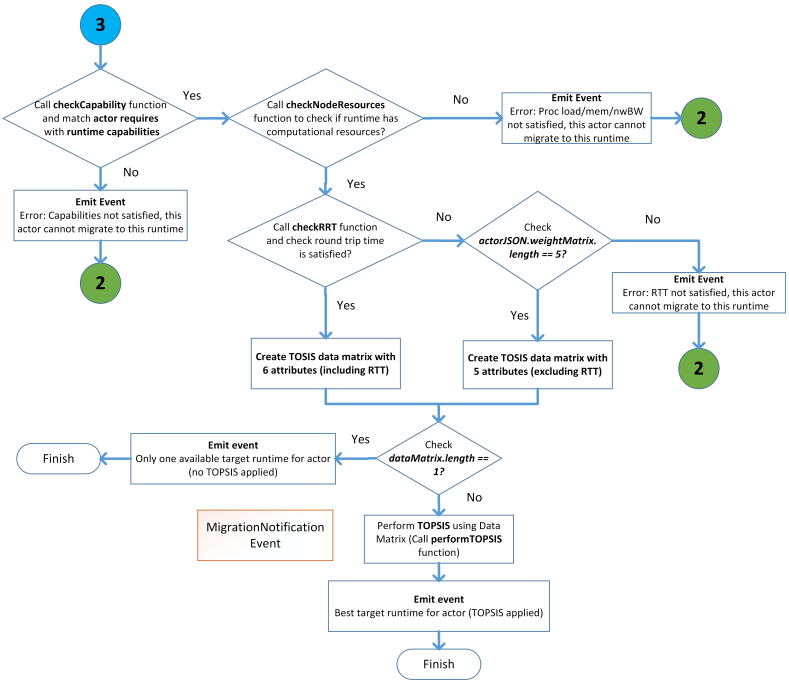


Figure 4.30: Migration Analysis Tx Processing Logic(Part-3)

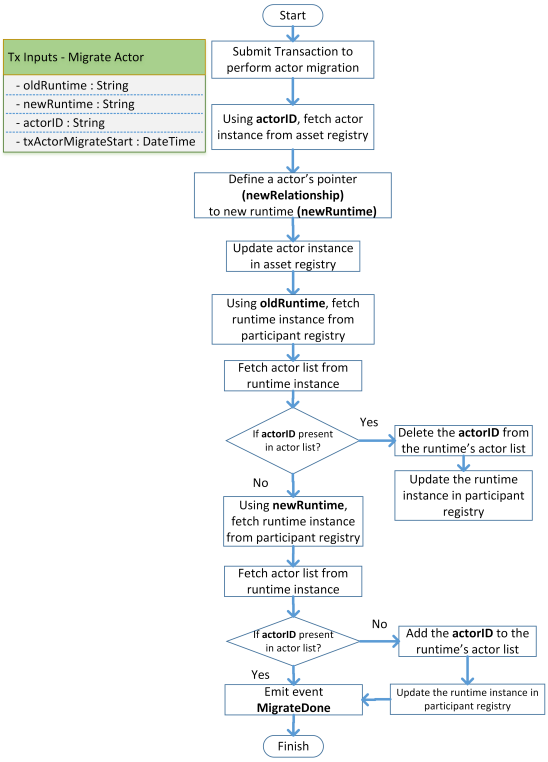


Figure 4.31: Migrate Actor Tx Processing Logic

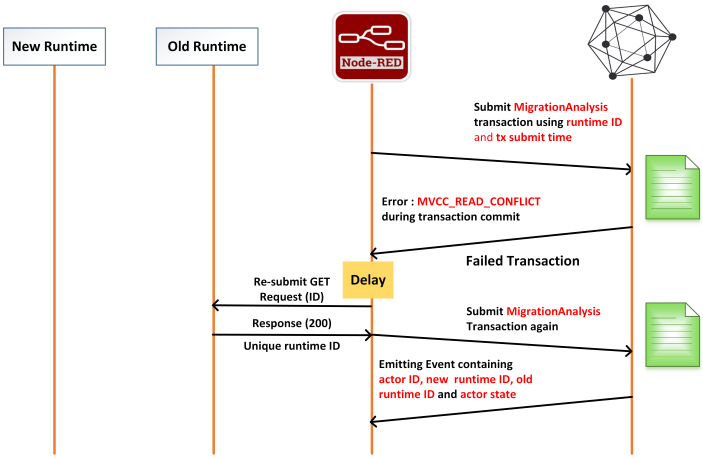


Figure 4.32: Migration Analysis Tx Flow during Error

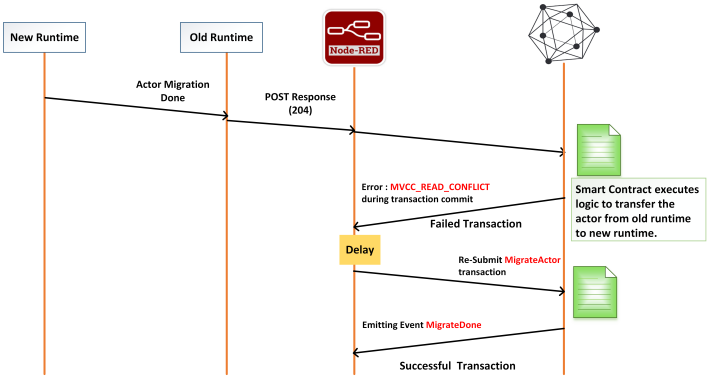


Figure 4.33: Migrate Actor Tx Flow during Error

4.8 Evaluation and test results

In this section, the functionality of the implemented proof-of-concept(PoC) has been evaluated and a performance analysis has been carried out. Within the functionality testing, the working of the actor migration process is evaluated. Subsequently, in the performance analysis, the timing calculations of Blockchain transactions for multi-peer networks are performed for the some scenarios. This thesis evaluation has been carried out on a single machine, which has the configuration as shown in Tab. 4.5. All Blockchain peers run locally as docker containers and other integrated applications such as Calvin and Node-RED also run locally as a process. Therefore, due to the local network set-up, the network delays are not considered during the performance analysis. In real scenarios there could not only be network delays, but also more advanced hardware for executing applications. Hence, the performance would be different from the current set-up. With this PoC, the aim is to give a sense of applicability of Blockchain in grid application migration and in the future, this implementation can be improved and extended further.

Resource Parameters	**Attribute Values**
Operating System	Ubuntu Linux 16.04 LTS (64-bit)
Memory	8 GB
Processor	Intel Core i3-2330M
Clock Rate	2.20 GHz

Table 4.5: Execution Environment

For evaluating the actor migration process, a four peer Blockchain network is created using the Hyperledger Fabric and then the Composer application is deployed to the Blockchain network. Using Node-RED flows, four Runtimes (i.e. participants) are created in the ledger and then four actors (i.e. assets) are created for each Runtime. Furthermore, data is updated for all the Runtimes and actors by submitting the transactions via Node-RED flows.

For an actor to be migrated, the AHP pairwise comparison matrix is created by the decision maker and then the criteria weights are computed in MATLAB as shown in the Tab. 4.6 and Tab. 4.7 respectively. Along with the actor's state information, these weights were also added in the ledger (or asset registry) and considered to be fixed for the tested scenario. In addition, for testing purposes, the values of computation resources are assumed constant for each Runtime as presented in the Tab. 4.8.

Comparison Matrix	CPU Availability (%) ∗ Clock Rate (GHz)	RAM Available(GB)	N\W BW Utilization(%)	RTT (ms)	Cores	N\BW(Gbps)
CPU Availability (%) ∗ Clock Rate (GHz)	1	1/3	1	1/3	3	3
RAM Available(GB)	3	1	3	1/2	4	4
N\W BW Utilization(%)	1	1/3	1	1/3	3	3
RTT (ms)	3	2	3	1	5	5
Cores	1/3	1/4	1/3	1/5	1	1
N\BW(Gbps)	1/3	1/4	1/3	1/5	1	1

Table 4.6: AHP Pairwise Comparison Matrix

Runtime Attribute\Weight	Weight
CPU Availability (%) ∗ Clock Rate (GHz)	0.1323
RAM Available(GB)	0.2663
N\W BW Utilization(%)	0.1323
RTT (ms)	0.3584
Cores	0.0554
N\BW(Gbps)	0.0554

Table 4.7: Relative Closeness

4.8.1 Migration Process

A subset of the actor's state as fetched from the ledger is shown in Tab. 4.9 and based on the actor's current Runtime, a scenario is created as shown in Fig. 4.34, for evaluating the migration process.

The `Migration Analysis` transaction is triggered via Node-RED flow created for a `Runtime 3` which then executes the smart contract on all four peers. From the smart contract's output (i.e. emitted event), it can be seen that `Runtime 1`, `Runtime 2` and `Runtime 4` were qualified as the target Runtimes for actor migration. Smart contract applied TOPSIS

Table 4.8: TOPSIS Data Matrix - Migration Analysis

Data Matrix Class	Runtime Attributes					
	CPU Availability (%) ∗ Clock Rate (GHz)	RAM Available(GB)	N\W BW Utilization(%)	**RTT (ms)**	**Cores**	**N\BW(Gbps)**
Runtime 1	72∗2.2	13	70	13	4	1
Runtime 2	85∗1.4	7	55	4	2	10
Runtime 3	67∗2.6	10	28	9	2	10
Runtime 4	50∗2.1	8	51	6	4	10

Actor Attribute	Value
Actor ID	`a97a8001-5322-4fa1-9ebc-6b9f83de0f09`
Actor Name	*test_Blockchain : client*
Current Runtime ID	`4d687d0d-8ff2-4dff-a552-6b6baf9528c6`
Runtime Name	`Runtime 3`

Table 4.9: Actor's State Before Migration

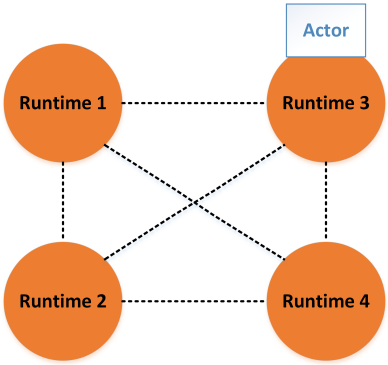


Figure 4.34: Evaluation Scenario

technique on the data matrix as shown in figure Tab. 4.10, created from selected Runtime's data and then chose the Runtime with highest relative closeness. Therefore, from Tab. 4.11, it can be seen that `Runtime 2` has the highest relative closeness and is chosen as the new destination Runtime for actor placement.

Since the `Migration Analysis` transaction got committed to the block in the ledger, this means that all four peers (i.e. endorsing peers in Fabric) have generated the same output, otherwise the transaction would have failed. Moreover, the smart contract results are similar to the TOPSIS

Table 4.10: TOPSIS Data Matrix - Migration Analysis

Data Matrix Class	Runtime Attributes					
	CPU Availability (%) ∗ Clock Rate (GHz)	RAM Available(GB)	N\W BW Utilization(%)	RTT (ms)	Cores	N\BW(Gbps)
Runtime 1	72∗2.2	13	70	13	4	1
Runtime 2	85∗1.4	7	55	4	2	10
Runtime 3	50∗2.1	8	51	6	4	10

Relative Closeness	Value
Runtime 1	0.3275699050131547
Runtime 2	0.6400157745842961
Runtime 4	0.6007424157478733

Table 4.11: Relative Closeness

simulation in MATLAB for the same data matrix and AHP weights. Therefore, it can be concluded that the smart contract implementation should be deterministic which means that for the same transaction proposal, all peers should return the same results, if not, a difference in results could lead to consensus failure. This could impose a limitation on the deployment of grid applications as a smart contract if they contain functions which may be random or non-deterministic in nature.

4.8.2 Performance Evaluation

As mentioned in [PST17], the latency and throughput are considered as the main performance tests that need to be evaluated for every Blockchain application. In this thesis, the performance evaluation of the Blockchain platform is conducted in terms of average latency.

In order to evaluate the performance, two peers and four peers Blockchain network are setup using Fabric and also parameters such as batch timeout and batch size are modified to change the Fabric network configuration. The **Batch Timeout** is the waiting time after the arrival of first transaction for further transactions before creating a block and the **Batch Size** parameter contains *max_message_count* which sets the maximum number of transactions per block and *absolute_max_bytes* which limits the size of the block. In Composer business network running over Fabric, four Runtimes are created and then four actors for each Runtime are created. For the latency calculations, the data is collected for each transaction as follows:

- The transaction deployment time is the time (ISO 8601 format) when transaction is triggered via Runtime's Node-RED flow.

- The transaction completion time is the time (ISO 8601 format) when block containing respective transaction gets committed to the ledger.

Latency is defined as the time difference between transaction completion time and transaction deployment time. The average latency is defined as the mean of latency of transactions present in a data set created for a

specific type of transaction. In the further sections, the variation in the average latency is explored by changing the number of Blockchain peers, batch timeout and the number of transactions per block.

Network Scaling Effect

This test is performed with only one Runtime invoking the transactions via Node-RED, therefore, there is only one transaction per block and there are no parallel transactions from other Runtimes. By configuring a two peer and a four peer Blockchain network with configuration i.e batch timeout (`2 sec`), a data set containing 25 records (or blocks) for each transaction is created for both networks. Then the average latency is calculated individually for each data set. Thereafter, the comparison between the average latency calculated for both networks for each transaction is shown in Fig. 4.35. It is observed that the latency increases with respect to the number of Blockchain peers. The reason could be that more time is required by the four peer network in reaching a consensus. Since the evaluation is performed locally, the machine resources are now shared by four peers, therefore, this could slow down the processing of transactions at each peer. All Blockchain peers process the transaction and generate an output and only if the results from all the peers are identical, will the transaction be committed to the ledger. Consequently, the time to receive confirmations from all peers in a four peer network is more than a two peer network. When peers are located separately, resource allocation may not be a problem, but network delays could affect the transaction latency. Therefore, keeping in mind the above analysis, the effect of scaling the Blockchain network should be taken into account while designing the Blockchain platform for grid applications.

Batch Timeout Effect

A four peer Fabric network with two different configurations i.e. batch timeout set to `1 sec` and `2 sec`, are setup for this evaluation and only one Runtime is invoking the transactions via Node-RED in this test. For both configured networks, a data set containing 25 records (or blocks) for each transaction is created and then average latency is calculated individually for each data set. Thereafter, the comparison between the average latency calculated for both networks for each transaction is shown in Fig. 4.36. It is observed that decreasing the batch timeout would improve the latency. For example, in the implemented model, the migration transactions (i.e. `Migration Analysis` and `Migrate Actor`) are always processed as a single transaction per block therefore there is no need to wait

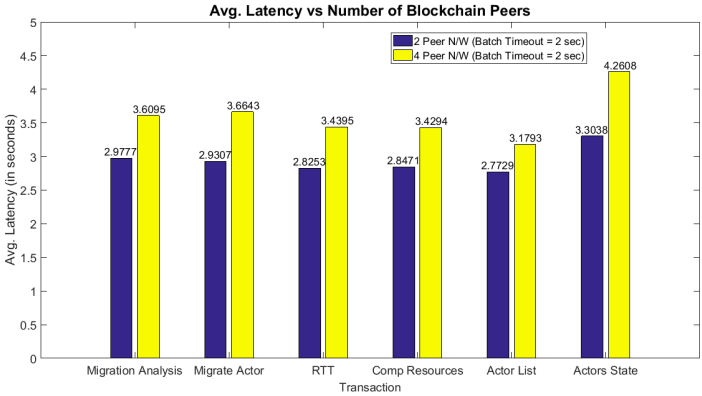


Figure 4.35: Average Latency vs Number of peers

for further transactions to be added to the block. Hence, batch timeout value equal to `1 sec` would be good if there is a need to minimize actor migration time. However, this also reduces the throughput of the network. Thus, while developing a Blockchain platform for grid applications, it needs to be taken into consideration that batch timeout value would affect the latency as well as throughput.

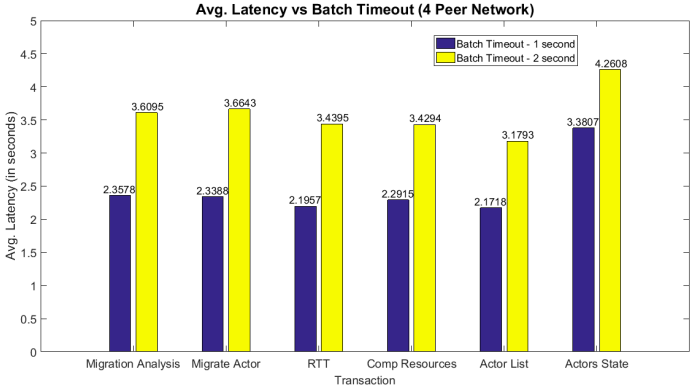


Figure 4.36: Average Latency vs Batch Timeout

Batch Timeout Effect

In the previous sections, only one Runtime is considered for performance evaluation in order to understand the influence of scaling and batch timeout. However, in production ready systems, there could be multiple users submitting the transaction at the same time, therefore this would also impact the transaction latency. In this section, the influence on the transaction latency when one Runtime is invoking the transaction and other Runtimes are also triggering the same transaction almost at the same time, is observed. The Fig. 4.37 and Fig. 4.38 shows the variation in the average latency with respect to number of transactions per block, for `RTT` and `Update Actor State` transactions respectively. Since the batch timeout value is `1 sec` and batch size (*max_message_count*) is 25, all the transactions arrived within timeout are added and processed in the same block, and committed to the ledger. It is observed that the latency increases when the number of transactions added to a block increases. Thus, the impact of transactions from other users should be taken into consideration while developing the Blockchain platform for grid applications.

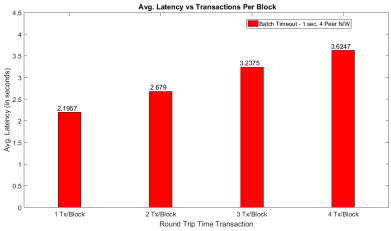


Figure 4.37: Average Latency vs Tx per Block(RTT)

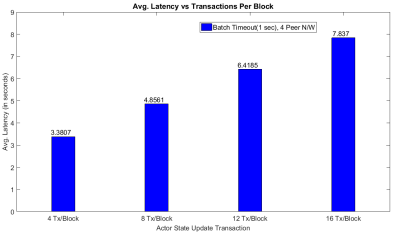


Figure 4.38: Average Latency vs Tx per Block(Actor State)

4.9 Conclusion

In this thesis, a novel approach for improving the resiliency of the grid automation system by utilizing a Blockchain based smart contract was introduced and a PoC implementation was demonstrated. First and foremost, the potential drawbacks of the current architecture, i.e. the Calvin remote manager based migration, were pointed out followed by the explanation of how Blockchain based smart contracts can enhance the grid automation resiliency by performing secure, automated and distributed migration of grid operation functions (or Calvin actors) between SAUs (or Runtimes).

Then, two types of migration techniques were discussed which can dynamically relocate the grid functions to different physical systems (or Runtimes), as follows:

- Periodic Migration – This technique could mitigate the attack by periodically changing the application's execution location (i.e. host Runtime) which improves the system robustness.

- Node Failure Migration – This technique could reduce the service downtime by migrating applications of attacked or failed nodes, to new destinations.

As a part of this study, an algorithm (or migration logic) was developed for selecting the best Runtime for actor placement based on a multi-criteria optimization method, which was programmed in JavaScript and implemented via Smart Contract. A Blockchain development framework i.e. Hyperledger Composer (along with Hyperledger Fabric) integrated with the distributed IoT environment i.e. Calvin, was utilized to realize the concept, validate the functioning of the prototype and investigate the performance.

The implemented application was validated by performing application (or actor) migration for a predicted test scenario. Moreover, the permissioned Blockchain characteristics such as identity verification and historical tracking were also validated. It was observed that the transaction latency increases with an increase in the number of Blockchain peers due to the fact that peers took more time in reaching a consensus. Secondly, the transaction latency was evaluated with respect to batch timeout. It was observed that decreasing the batch timeout improves the transaction latency. Lastly, it was observed that the transaction latency increases with increase in number of transactions per block. This is due to the fact that as the number of transactions per block increases, the block committing time also increases.

It can be concluded that it is possible to migrate the grid operation functions to different physical systems by utilizing the Blockchain based smart contract solution. However, the performance of this solution would depend upon the configuration and Runtime parameters. Therefore, while designing real world applications, the impact of these evaluated parameters as well as other possible parameters, such as network delays, should be taken into consideration.

4.10 Scope and future work

The scope of the proposed methodology could be extended to any critical infrastructure automation systems like the controlling gas grids, railway systems, process industries etc. In the current study, only a PoC implementation was done for a specific set of grid operation functions using open source IoT platform, CALVIN, which is not properly maintained. Furthermore, alternatives to Hyperledger Fabric like the IOTA which is computationally inexpensive can improve the overall perfomance of the migration/re-initialisation of the grid operation functions. The proposed solution has been tested for the grid operation functions that act on real time measurements and not on historical data. Whenever the grid operation function is migrated, it will re-initialize the connection with the sensors/actuators and obtain the real time data from them and start operating based on the real time measurements that it receives. Any historic data is not used for the current action. Hence, in this study the storing of the real-time measurements is not considered. However, for grid operation functions like load forecasting, generation forecasting functions, might need historical data. Measures have to be taken to ensure the data redundancies. Furthermore, the real time measurement and status data exchanged with the field devices might be lost during the migration. Therefore, proper data management procedures have to be integrated with the proposed solution to ensure complete resiliency of the DGA systems.

5

Conclusion

As mentioned earlier, in the process of making a system resilient it is important to understand the reliability and the susceptability of the system to random and intended failures. To study the impact of random failures and thus design appropriate measures to improve the system availability the reliability of the cyber-physical DGA system has to be evaluated. Therefore, in this thesis a methodology of evaluating the reliability of cyber-physical DGA system using CTMC and Markov chains is proposed. Two examples have been presented to show the applicability of the proposed methodology using CTMC and the MDRM for evaluating the reliability of the DGA systems. The complete DGA system under study is divided into different functional blocks to combatt eh state explosion problem of using state space based reliability evaluation methods. With the first test case, it is shown that the ICT infrastructure influences the reliability of the DGA system and the redundancies in it impacts the overall reliability of the DGA system. The calculated reliability is then used to calculate overall cost of unavailability of the system using the Markov Reward Models. In the second test case, a complex heterogeneous DGA system for monitoring distribution grids is presented. Heterogeneous communication infrastructures (Ethernet, PLC and LTE) failure models have been modeled. The monitoring system of the DGA system based on IDE4L automation architecture has been considered for this test case. The division of the DGA system into mutually exclusive and collectively exhaustive Functional Blocks is presented. Using MDRM and the detailed failure models of the individual components within the Functional Block, the reliability of each functional block is evaluated. Finally the overall reliability of the DGA system as a function of reliability of he individual functional blocks is presented. The main purpose of the second test case is to present the applicability of the proposed methodology to model the failure characteristics of a complex heterogeneous automation function realisation.

To capture the impact of the intended attack the concept of susceptibility is introduced. A generic flow of steps to evaluatet eh risk of the intended attack is presented. One of the major part of the risk assessment is the threat propagation analysis, with which the appropriate countermeasures are chosen to be implemented. The proposed methodology helps in modelling the threat propagation and evaluate the different susceptibility indices. The threat scenario is initially represented graphically as a variant of an attack tree. In this study a stochastic methodology based on CTMC and AHPto analyse attack trees and also their extensions with countermeasures has been presented. The steps to be followed to obtain the CTMC from attack trees using PNs have been explained. Specific performance measures using CTMC, namely the state occupancy probability, time spent in the transient states and the estimated absorption time have been mapped to the probability of reaching the sub attack/attack goals, expected time spent in sub attack states and time to reach root node respectively. The proposed methodology provides flexibility to include the uncertainty in the likelihood of vulnerability exploitation based on the levels of the vulnerability and the degree of exposure using AHP. Furthermore, the effectiveness of the countermeasures compared to the likelihood of vulnerability exploitation is also taken into consideration in the threat propagation modelling. This enables the system designers to assess the risk of a specific attack given the efficiency of a countermeasure. The results presented for the test case 2 show that, with CTMC, effectiveness of the countermeasure can be calculated by evaluating the probability of threat state occupancy, time spent in the transient states and the time to reach the main goal of the attack.

Finally since no measure of redundancies and countermeasure against intended failures is fool proof thus the DGA system should be resilient enough to be available as soon as possible even after an unavoidable failure .

In this thesis, a novel approach for improving the resiliency of the grid automation system by utilizing a Blockchain based smart contract was introduced and a PoC implementation was demonstrated. First and foremost, the potential drawbacks of the current architecture, i.e. the Calvin remote manager based migration, were pointed out followed by the explanation of how Blockchain based smart contracts can enhance the grid automation resiliency by performing secure, automated and distributed migration of grid operation functions (or Calvin actors) between SAUs (or Runtimes).

Then, two types of migration techniques were discussed which can dynamically relocate the grid functions to different physical systems (or Runtimes), as follows:

- Periodic Migration – This technique could mitigate the attack by periodically changing the application's execution location (i.e. host Runtime) which improves the system robustness.

- Node Failure Migration – This technique could reduce the service downtime by migrating applications of attacked or failed nodes, to new destinations.

As a part of this study, an algorithm (or migration logic) was developed for selecting the best Runtime for actor placement based on a multi-criteria optimization method, which was programmed in JavaScript and implemented via Smart Contract. A Blockchain development framework i.e. Hyperledger Composer (along with Hyperledger Fabric) integrated with the distributed IoT environment i.e. Calvin, was utilized to realize the concept, validate the functioning of the prototype and investigate the performance.

The implemented application was validated by performing application (or actor) migration for a predicted test scenario. Moreover, the permissioned Blockchain characteristics such as identity verification and historical tracking were also validated. It was observed that the transaction latency increases with an increase in the number of Blockchain peers due to the fact that peers took more time in reaching a consensus. Secondly, the transaction latency was evaluated with respect to batch timeout. It was observed that decreasing the batch timeout improves the transaction latency. Lastly, it was observed that the transaction latency increases with increase in number of transactions per block. This is due to the fact that as the number of transactions per block increases, the block committing time also increases.

It can be concluded that it is possible to migrate the grid operation functions to different physical systems by utilizing the Blockchain based smart contract solution. However, the performance of this solution would depend upon the configuration and Runtime parameters. Therefore, while designing real world applications, the impact of these evaluated parameters as well as other possible parameters, such as network delays, should be taken into consideration.

6

Future Work

In the current study,for modelling the reliability, random failures of the components have been considered. The common mode dependant failures of components that are part of the same functional block are also considered within the proposed framework, however common mode failures that impact components of multiple functional block currently have not been considered. Such failures are catastrophic in nature and are generally considered as High Impact with Low Probability (HILP) events (like natural calamities or wide range terrorist attacks). The inclusion of such HILP events in the reliability calculation would cenable the system designer a comprehensive idea of the reliability of the system. The proposed methodology should be extended to study the impact of such HILP events to design appropriate resilience measures. Current study assumes an exponential distribution of the cyber and physical components of the DGA system, however, this assumption is valid only for components that are considered to be in their prescribed operational time, however for cost optimization the DGA infrastructure might be operated beyond their prescribed operational times and thus failure characteristics considering the ageing of the devices must be considered. One of the interesting extensions of this work is to perform a Global Sensitivity Analysis (GSA) to identify the weakest link in the DGA system. With GSA the variation of the overall reliabiliy as a function of the variance of the failure rates of components of each automation device could be evaluated. This enables the system designers to prioritize their investments in improving the system reliability either by introducing redundancies or replacing the devices with more reliable components. Another extension that is really interesting is to use the MDRM and the CTMC models of the cyber and physical components to identify the availability of each combination of the availability the cyber and physical components. If we represent these state as individual CTMC states of the combined system and perform a power flow of the grid considering the impacts of the availability of subset of the components,

the avarage powerflow/energy supplied/not supplied could be evaluated in detail. Such a modelling allows the evaluation of the impact of failure of communication infrastructure (discrete time domain) on to the power flow (which is in continuous time domain).

The proposed method for evaluating the DGA system susceptibility, has been shown to model threat scenarios, include uncertainties of the attack propagation and countermeasure actuation. However, it should be noted that the methodology proposed is based on state space analysis. Therefore, depending upon the complexity of the attack being modelled, number of threat agents, number of vulnerabilities to be considered in the threat scenario, the size of the attack vectors, the state space representation of the threat scenario could easily explode. One of the future work of this presented methodology is to solve the state space explosion problem of the methodology. One method to investigate for this purpose is the applicability of the coverability graph instead of reachability graph for generating he threat state transition graph. Another shortfall of the methodology is that it can only accurately model the threat propagation for all known threat agents and attack vectors. But in the evolving threat space in the cyber-physical domain, the proposed methodology should be extended with a periodic automatic update of the attack vectors and thus enriching the state transition graph of the threat propagation. The proposed methodology provides the initial model of the threat propagation where all the threat states are known, but it can be extended to include unknown states using machine learning methods like Hidden Markov Models to identify the threat states based on data on the detected attacks. The proposed methodology could be used for real time prediction of the threat propagation. This might be especially helpful for evaluating conflicting countermeasures and when to activate them, based on the threat propagation over a span of time. Investigations should be made on methods to reduce the computation complexity/ computational speed to provide the threat propagation prediction within the prescribed amount of time, such that, the actuation of the countermeasure is possible before the threat reaches the main goal. This is particularly interesting feature to be part of an online threat perception system for Critical Infrastructures that can actuate varied sets of countermeasures against different cyber-physical threats that may involve unauthorized physical intrusion.

The scope of the proposed methodology could be extended to any critical infrastructure automation systems like the controlling gas grids, railway systems, process industries etc. In the current study, only a PoC implementation was done for a specific set of grid operation functions using open source IoT platform, CALVIN, which is not properly maintained. Furthermore, alternatives to Hyperledger Fabric like the IOTA which is

computationally inexpensive can improve the overall perfomance of the migration/re-initialisation of the grid operation functions. The proposed solution has been tested for the grid operation functions that act on real time measurements and not on historical data. Whenever the grid operation function is migrated, it will re-initialize the connection with the sensors/actuators and obtain the real time data from them and start operating based on the real time measurements that it receives. Any historic data is not used for the current action. Hence, in this study the storing of the real-time measurements is not considered. However, for grid operation functions like load forecasting, generation forecasting functions, might need historical data. Measures have to be taken to ensure the data redundancies. Furthermore, the real time measurement and status data exchanged with the field devices might be lost during the migration. Therefore, proper data management procedures have to be integrated with the proposed solution to ensure complete resiliency of the DGA systems.

Acronyms

OLTC	On Load Tap Changer
PDC	Phasor Data Concentrator
PDF	Probability Density Function
PLC	Power Line Communication
PMF	Probability Mass Function
PMU	Phasor Measurement Unit
PN	Petri Net
PRM	Probabilistic Relational Models
PTP	Precision Time Protocol
PV	Photovoltaic
RBD	Reliability Block Diagram
RF	Radio Frequency
RTU	Remote Terminal Unit
SAU	Substation Automation Unit
SCADA	Supervisory Control And Data Acquisition
SCU	Supervisory Control Unit
SE	State Estimation
SM	Smart Meter
SMDC	Smart Meter Data Concentrator
SPMD	Single Programm Multiple Data
SPN	Stochstic Petri Nets
TSO	Transmission System Operators
VSC	Voltage Source Converters
WAMPAC	Wide Area Monitoring, Protection And Control
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access

List of Figures

List of Tables

Bibliography

[AFB07] F. Aminifar, M. Fotuhi-Firuzabad, and R. Billinton. "Extended reliability model of a unified power flow controller". In: *IET Generation, Transmission Distribution* 1.6 (2007), pp. 896–903.

[AG05] S. AG. *SN29500 Series: Reliability prediction of electronic equipment*. Tech. rep. 2005.

[AM17] M. Alharby and A. v. Moorsel. "Blockchain Based Smart Contracts : A Systematic Mapping Study". In: *Computer Science and Information Technology (CS and IT)* (Aug. 2017). DOI: 10.5121/csit.2017.71011. URL: http://dx.doi.org/10.5121/csit.2017.71011.

[And+18] E. Androulaki et al. "Hyperledger fabric". In: *Proceedings of the Thirteenth EuroSys Conference* (Apr. 2018). DOI: 10.1145/3190508.3190538. URL: http://dx.doi.org/10.1145/3190508.3190538.

[Ang+15] A. Angioni et al. "Coordinated voltage control in distribution grids with LTE based communication infrastructure". In: *2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC)*. 2015, pp. 2090–2095. DOI: 10.1109/EEEIC.2015.7165498.

[Ang+16] A. Angioni et al. "Real-Time Monitoring of Distribution System Based on State Estimation". In: *IEEE Transactions on Instrumentation and Measurement* 65.10 (2016), pp. 2234–2243. DOI: 10.1109/TIM.2016.2583239.

[Ang+17] A. Angioni et al. "Design and Implementation of a Substation Automation Unit". In: *IEEE Transactions on Power Delivery* 32.2 (Apr. 2017), pp. 1133–1142. ISSN: 0885-8977. DOI: 10.1109/TPWRD.2016.2614493.

[Avi+04] A. Avizienis et al. "Basic concepts and taxonomy of dependable and secure computing". In: *IEEE Transactions on Dependable and Secure Computing* 1.1 (Jan. 2004), pp. 11–33. ISSN: 2160-9209. DOI: 10.1109/TDSC.2004.2.

[BA92] R. Billinton and R. Allan. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. Springer US, 1992. ISBN: 9780306440632. URL: https://books.google.pl/books?id=nqm9N6Yfk9sC.

[BG20] A. Baggio and F. Grimaccia. "Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision". In: *IEEE Access* 8 (2020), pp. 205250–205271. DOI: 10.1109/ACCESS.2020.3036994.

[Bra+12] A. Bracale et al. "A hybrid AC/DC Smart Grid to improve power quality and reliability". In: *2012 IEEE International Energy Conference and Exhibition (ENERGYCON)*. Sept. 2012, pp. 507–514.

[Buc95] P. Buchholz. "Hierarchical Markovian models: symmetries and reduction". In: *Performance Evaluation* 22.1 (1995). 6th International Conference on Modelling Techniques and Tools for Computer Performance Evalution, pp. 93–110. ISSN: 0166-5316. DOI: https://doi.org/10.1016/0166-5316(93)E0040-C. URL: http://www.sciencedirect.com/science/article/pii/0166531693E0040C.

[BVB11] J. Beerten, D. Van Hertem, and R. Belmans. "VSC MTDC systems with a distributed DC voltage control - A power flow approach". In: *2011 IEEE Trondheim PowerTech*. June 2011, pp. 1–6. DOI: 10.1109/PTC.2011.6019434.

[CD16] K. Christidis and M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things". In: *IEEE Access* 4 (2016), pp. 2292–2303. DOI: 10.1109/ACCESS.2016.2566339.

[CD20] S. CRINO and C. ". DREBY. *Drone Attacks Against Critical Infrastructure: A Real and Present Threat*. Tech. rep. Atlantic Council, 2020. URL: http://www.jstor.org/stable/resrep24632.

[Cha+14] N. Chaudhuri et al. *Multi-terminal Direct-Current Grids: Modeling, Analysis, and Control (Wiley - IEEE)*. Wiley-IEEE Press, 2014. ISBN: 9781118729106.

[Che+11] G. Chen et al. "Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks". In: *IEEE Transactions on Power Systems* 26.3 (2011), pp. 1000–1009. DOI: 10.1109/TPWRS.2010.2078524.

[Che+19] D. Chen et al. “Unbalanced power flow algorithm for AC DC hybrid distribution network with diverse-controlled VSC-MTDC converts”. In: *The Journal of Engineering* 2019.16 (2019), pp. 1918–1925.

[Cho+18] S. Cho et al. “Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture”. In: *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. 2018, pp. 1–8. DOI: 10.1109/CyberSA.2018.8551383.

[Coma] E. Commission. *Clean Energy for All*. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:fa6ea15b-b7b0-11e6-9e3c-01aa75ed71a1.0001.02/DOC_1&format=PDF. (accessed: 23.06.2020).

[Comb] I. E. Commission. *SMART GRID STANDARDS MAP*. URL: http://smartgridstandardsmap.com/. (accessed: 01.10.2021).

[Comc] I. S. Committee. *The Risk Management Process For Federal Facilities: An Interagency Security Committee Standard*. Standard. USA: Cyber Security and Infrastructure Security Agency.

[Com09] I. 6. Committee. *IEC TS 62443-1-1:2009: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*. Standard. International Electrotechnical Commission, 2009.

[Com10] I. 6. Committee. *IEC 62443-2-1:2010: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program*. Standard. International Electrotechnical Commission, 2010.

[Com15] I. 6. Committee. *IEC 62443-2-4:2015: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*. Standard. International Electrotechnical Commission, 2015.

[Cos+17] F. B. Costa et al. “Two-Terminal Traveling-Wave-Based Transmission-Line Protection”. In: *IEEE Transactions on Power Delivery* 32.3 (2017), pp. 1382–1393.

[Dal+06] Dalton et al. “Analyzing Attack Trees using Generalized Stochastic Petri Nets”. In: *2006 IEEE Information Assurance Workshop*. June 2006, pp. 116–123. DOI: 10.1109/IAW.2006.1652085.

[DBA15] F. Dammak, L. Baccour, and A. M. Alimi. "The impact of criterion weights techniques in TOPSIS method of multi-criteria decision making in crisp and intuitionistic fuzzy domains". In: *2015 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. Aug. 2015, pp. 1–8. DOI: 10.1109/FUZZ-IEEE.2015.7338116.

[Def17] S. of Defense for Systems Engineering. *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Tech. rep. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017.

[Def91] D. of Defense USA. *MIL-HDBK-217F: Military Handbook: Reliability prediction of electronic equipment*. Tech. rep. 1991.

[Del+16] K. Delmolino et al. "Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab". In: *Financial Cryptography and Data Security*. Ed. by J. Clark et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 79–94.

[DHS03] S. Derisavi, H. Hermanns, and W. H. Sanders. "Optimal state-space lumping in Markov chains". In: *Information Processing Letters* 87.6 (2003), pp. 309–315. ISSN: 0020-0190. DOI: https://doi.org/10.1016/S0020-0190(03)00343-0. URL: http://www.sciencedirect.com/science/article/pii/S0020019003003430.

[Din+16] T. Ding et al. *Multiple Attribute Decision Making Based on Cross-Evaluation with Uncertain Decision Parameters*. 2016. DOI: 10.1155/2016/4313247. URL: http://dx.doi.org/10.1155/2016/4313247.

[DMS18] M. Diekerhof, A. Monti, and S. Schwarz. "Chapter 12 - Demand-Side Management—Recent Aspects and Challenges of Optimization for an Efficient and Robust Demand-Side Management". In: *Classical and Recent Aspects of Power System Optimization*. Ed. by A. F. Zobaa, S. H. Abdel Aleem, and A. Y. Abdelaziz. Academic Press, 2018, pp. 331–360. ISBN: 978-0-12-812441-3. DOI: https://doi.org/10.1016/B978-0-12-812441-3.00012-4. URL: https://www.sciencedirect.com/science/article/pii/B9780128124413000124.

[Dog+20a] A. Dognini et al. “14. Securing CEI by-design”. In: *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Now Publishers, 2020. DOI: 10.1561/9781680836875.ch14. URL: https://doi.org/10.1561/9781680836875.ch14.

[Dog+20b] A. Dognini et al. “Service Restoration Algorithm for Distribution Grids under High Impact Low Probability Events”. In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. 2020, pp. 237–241. DOI: 10.1109/ISGT-Europe47291.2020.9248823.

[Dom12] A. D. Domínguez-García. “Reliability modeling of cyber-physical electric power systems: A system-theoretic framework”. In: *2012 IEEE Power and Energy Society General Meeting*. July 2012, pp. 1–5. DOI: 10.1109/PESGM.2012.6345518.

[DWD12] D.-L. Duan, X.-Y. Wu, and H.-Z. Deng. “Reliability Evaluation in Substations Considering Operating Conditions and Failure Modes”. In: *IEEE Transactions on Power Delivery* 27.1 (2012), pp. 309–316. DOI: 10.1109/TPWRD.2011.2173807.

[DZL17] R. Deng, P. Zhuang, and H. Liang. “CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid”. In: *IEEE Transactions on Smart Grid* 8.5 (2017), pp. 2420–2430. DOI: 10.1109/TSG.2017.2702125.

[Eri] Ericsson. *Calvin Base*. URL: https://github.com/EricssonResearch/calvin-base. (accessed: 21.04.2018).

[Eri18] Ericsson. *Calvin Base*. https://github.com/EricssonResearch/calvin-base. Ericsson, [Online; accessed 21-April-2018]. 2018.

[ESA] ESAFENET. *eSAFENET : Kommunikationsnetz im Internet der Energie*. URL: https://e-safe-net.de/. (accessed: 01.01.2021).

[Fab17] H. Fabric. *Fabric Docs v1.1*. https://hyperledger-fabric.readthedocs.io/en/release-1.1/. Hyperledger, [Online; accessed 30-May-2018]. 2017.

[Fan+20] C. Fan et al. “Performance Evaluation of Blockchain Systems: A Systematic Survey”. In: *IEEE Access* 8 (2020), pp. 126927–126950. DOI: 10.1109/ACCESS.2020.3006078.

[FIS] FISMEP. *FISMEP : FIWARE For Smart Energy platform*. URL: http://fismep.de/. (accessed: 01.01.2021).

[FLE] FLEXMETER. *FLEXMETER : FLEXible smart METERing architecture*. URL: https://flexmeter.polito.it/. (accessed: 01.01.2021).

[Gal17] U. S. S. Gallersdörfers. "Analysis of Use Cases of Blockchain Technology in Legal Transactions". MA thesis. Technical University of Munich, Department of Informatics, 2017, p. 46.

[Gar15] J. Garcia-Hernandez. "Recent Progress in the Implementation of AMI Projects: Standards and Communications Technologies". In: *2015 International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE)*. 2015, pp. 251–256.

[Geo17] A. D. George. *Microprocessor-Based Parallel Architecture for Reliable Digital Signal Processing Systems*. CRC Press, 2017. ISBN: 131589551X.

[Gha+] H. Ghaeini et al. "State-aware anomaly detection for industrial control systems". en. In: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing; 2018*. Pau, France.

[Gil16] J. M. R. Gil. "Secure Domain Transition of Calvin Actors". MA thesis. Department of Electrical and Information Technology, Lund University, 2016.

[Gmb] D. D. E.-A. GmbH. *Einführung von Smart Meter in Deutschland : Analyse von Rolloutszenarien und ihrer regulatorischen Implikationen*. URL: https://www.dena.de/fileadmin/dena/Dokumente/Pdf/9092_dena-Smart-Meter-Studie.pdf. (accessed: 01.07.2020).

[GR15] D. D. Giustina and S. Rinaldi. "Hybrid Communication Network for the Smart Grid: Validation of a Field Test Experience". In: *IEEE Transactions on Power Delivery* 30.6 (2015), pp. 2492–2500.

[Gup+16] S. Gupta et al. "Blackout risk analysis in Smart grid WAMPAC system using KL divergence approach". In: *2016 IEEE 6th International Conference on Power Systems (ICPS)*. 2016, pp. 1–6. DOI: 10.1109/ICPES.2016.7584069.

[GW13] E. Gelenbe and F.-J. Wu. "Future Research on Cyber-Physical Emergency Management Systems". In: *Future Internet* 5.3 (2013), pp. 336–354. ISSN: 1999-5903. DOI: 10.3390/fi5030336. URL: https://www.mdpi.com/1999-5903/5/3/336.

[Hae+19] H. Haes Alhelou et al. “A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges”. In: *Energies* 12.4 (2019). ISSN: 1996-1073. DOI: 10.3390/en12040682. URL: https://www.mdpi.com/1996-1073/12/4/682.

[Haj11] H. Hajian-Hoseinabadi. “Impacts of Automated Control Systems on Substation Reliability”. In: *IEEE Transactions on Power Delivery* 26.3 (July 2011), pp. 1681–1691. ISSN: 1937-4208. DOI: 10.1109/TPWRD.2011.2119404.

[Han+17] S. Hanif et al. “Distributed Congestion Management of Distribution Grids Under Robust Flexible Buildings Operations”. In: *IEEE Transactions on Power Systems* 32.6 (2017), pp. 4600–4613. DOI: 10.1109/TPWRS.2017.2660065.

[HG12] H. Hajian-Hoseinabadi and M. E. H. Golshan. “Availability, Reliability, and Component Importance Evaluation of Various Repairable Substation Automation Systems”. In: *IEEE Transactions on Power Delivery* 27.3 (2012), pp. 1358–1367. DOI: 10.1109/TPWRD.2012.2187935.

[HHG12] H. Hajian-Hoseinabadi, M. Hasanianfar, and M. E. H. Golshan. “Quantitative Reliability Assessment of Various Automated Industrial Substations and Their Impacts on Distribution Reliability”. In: *IEEE Transactions on Power Delivery* 27.3 (2012), pp. 1223–1233. DOI: 10.1109/TPWRD.2012.2188142.

[Hu+17] X. Hu et al. “Multiple cyber attacks against a target with observation errors and dependent outcomes: characterization and optimization”. en. In: *Reliab Eng Syst Saf* 159 (2017), pp. 119–133.

[HU12] T. M. Haileselassie and K. Uhlen. “Precise control of power flow in multiterminal VSC-HVDCs using DC voltage droop control”. In: *2012 IEEE Power and Energy Society General Meeting*. July 2012, pp. 1–9.

[HUK20] S. M. S. Hussain, T. S. Ustun, and A. Kalam. “A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges”. In: *IEEE Transactions on Industrial Informatics* 16.9 (2020), pp. 5643–5654. DOI: 10.1109/TII.2019.2956734.

[Hum+17] A. Humayed et al. “Cyber-Physical Systems Security—A Survey”. In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.

[Hus+18] S. Hussain et al. “Smart Grid Cybersecurity: Standards and Technical Countermeasures”. In: *2018 International Conference on Computer and Applications (ICCA)*. 2018, pp. 136–140. DOI: 10.1109/COMAPP.2018.8460390.

[HW17] L. Hancher and B. Winters. “The EU Winter Package : Briefing Paper”. In: (2017).

[HY81] C.-L. Hwang and K. Yoon. “Methods for multiple attribute decision making”. In: *Multiple attribute decision making*. Springer, 1981, pp. 58–191.

[Hyp] Hyperledger. *Hyperledger Composer*. URL: https://hyperledger.github.io/composer/latest/%20introduction/introduction.html. (accessed: 21.04.2018).

[Hyp18] Hyperledger. *Hyperledger Composer*. https://hyperledger.github.io/composer/latest/introduction/introduction.html. [Online; accessed 21-April-2018]. 2018.

[IDE] IDE4L. *Architecture design and implementation*. URL: http://ide4l.eu/results/. (accessed: 01.09.2016).

[IEC90] IEC. *Telecontrol equipment and systems Part 4: Performance requirements*. en. Standard IEC TR 60870-4:1990. Geneva, CH: IEC, 1990.

[IS] ". of Incident Response and I. Security Teams. *Common Vulnerability Scoring System*. URL: https://www.first.org/cvss/specification-document. (accessed: 27.06.2021).

[Iza21] ". J. C. "Izar Tarandach". *Threat Modeling: A Practical Guide for Development Teams*. O’Reilly Media,Inc, 2021. ISBN: 9781492056553.

[Jam+15] P. Jamborsalamati et al. “Design, implementation and real-time testing of an IEC 61850 based FLISR algorithm for smart distribution grids”. In: *2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. 2015, pp. 114–119. DOI: 10.1109/AMPS.2015.7312748.

[Jam+16] P. Jamborsalamati et al. “A flexible HiL testing platform for performance evaluation of IEC 61850-based protection schemes”. In: *2016 IEEE Power and Energy Society General Meeting (PESGM)*. 2016, pp. 1–5.

[Jam+17] P. Jamborsalamati et al. “Improvement of supply restoration in multi-spare-feeder active distribution grids using IEC 61850”. In: *2017 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia)*. 2017, pp. 1–5. DOI: 10.1109/ISGT-Asia.2017.8378326.

[JHT19] B.-C. Jhong, J. Huang, and C.-P. Tung. “Spatial Assessment of Climate Risk for Investigating Climate Adaptation Strategies by Evaluating Spatial-Temporal Variability of Extreme Precipitation”. In: *Water Resources Management* 33.10 (June 2019), pp. 3377–3400. DOI: 10.1007/s11269-019-02306-8. URL: https://doi.org/10.1007/s11269-019-02306-8.

[Ji+16] X. Ji et al. “Attack-defense trees based cyber security analysis for CPSs”. In: *2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. 2016, pp. 693–698. DOI: 10.1109/SNPD.2016.7515980.

[JM17] A. Jaiswal and R. B. Mishra. “Cloud Service Selection Using TOPSIS and Fuzzy TOPSIS with AHP and ANP”. In: *Proceedings of the 2017 International Conference on Machine Learning and Soft Computing*. ICMLSC ’17. Ho Chi Minh City, Vietnam: ACM, 2017, pp. 136–142. ISBN: 978-1-4503-4828-7. DOI: 10.1145/3036290.3036312. URL: http://doi.acm.org/10.1145/3036290.3036312.

[Joh89] B. W. Johnson. “Design and Analysis of Fault-Tolerant Systems for Industrial Applications”. In: *Fehlertolerierende Rechensysteme / Fault-tolerant Computing Systems*. Ed. by W. Görke and H. Sörensen. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 57–73.

[Kam] R. Kamphuis. *DREAM-Deliverable D5.2 DREAM Framework for active distribution grids: Common capabilities.* URL: http://www.dreamsmartgrid.eu/downloads/#deliverables. (accessed: 05.09.2021).

[KB21] V. Kayalvizhy and A. Banumathi. “A Survey on Cyber Security Attacks and Countermeasures in Smart Grid Metering Network”. In: *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*. 2021, pp. 160–165. DOI: 10.1109/ICCMC51019.2021.9418303.

[KL20] N. Kaloudi and J. Li. “The AI-Based Cyber Threat Landscape: A Survey”. In: *ACM Computing Surveys (CSUR)* 53 (Feb. 2020), pp. 1–34. DOI: 10.1145/3372823.

[KM17] A. Korompili and A. Monti. “Adaptive droop-based voltage control in multi-terminal dc systems”. In: *2017 IEEE Manchester PowerTech*. June 2017, pp. 1–6. DOI: 10.1109/PTC.2017.7980930.

[KNO13] J. Konig, L. Nordstrom, and M. Osterlind. “Reliability Analysis of Substation Automation System Functions Using PRMs”. In: *IEEE Transactions on Smart Grid* 4.1 (2013), pp. 206–213. DOI: 10.1109/TSG.2012.2225452.

[Kor+15] A. Korompili et al. “Flexible Electric Networks of the Future: Project on Control and Automation in MVDC grids”. In: *International ETG Congress 2015; Die Energiewende - Blueprints for the new energy age*. Nov. 2015, pp. 1–8.

[Kum+19] G. Kumar Roy et al. “Data modelling of converters for the automation and monitoring of MTDC grids”. English. In: *IET Smart Grid* 2 (3 Sept. 2019), 456–463(7).

[Kuz+21] I. Kuzminykh et al. “Information Security Risk Assessment”. In: *Encyclopedia* 1.3 (2021), pp. 602–617. ISSN: 2673-8392. DOI: 10.3390/encyclopedia1030050. URL: https://www.mdpi.com/2673-8392/1/3/50.

[LB13] W. Li and R. Billinton. *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. Language of science. Springer US, 2013. ISBN: 9781489913463. URL: https://books.google.de/books?id=qakACAAAQBAJ.

[LC87] J.-C. Laprie and A. Costes. “Dependable Computing and Fault Tolerance at LAAS: a Summary”. In: *The Evolution of Fault-Tolerant Computing*. Ed. by A. Avižienis, H. Kopetz, and J.-C. Laprie. Vienna: Springer Vienna, 1987, pp. 193–213. ISBN: 978-3-7091-8871-2.

[LDB18] H. S. Lallie, K. Debattista, and J. Bal. “An Empirical Evaluation of the Effectiveness of Attack Graphs and Fault Trees in Cyber-Attack Perception”. In: *IEEE Transactions on Information Forensics and Security* 13.5 (May 2018), pp. 1110–1122. ISSN: 1556-6013. DOI: 10.1109/TIFS.2017.2771238.

[LGV13] G. Loukas, D. Gan, and T. Vuong. “A Review of Cyber Threats and Defence Approaches in Emergency Management”. In: *Future Internet* 5.2 (2013), pp. 205–236. ISSN: 1999-5903. DOI: 10.3390/fi5020205. URL: https://www.mdpi.com/1999-5903/5/2/205.

[Li14] W. Li. *Risk Assessment of Power Systems: Models, Methods, and Applications*. IEEE Press Series on Power Engineering. Wiley, 2014. ISBN: 9781118843222. URL: https://books.google.de/books?id=UiTnAgAAQBAJ.

[LIS] LISK. *How Does Blockchain Work*. URL: https%20:%20/%20/%20lisk%20.%20io%20/%20academy%20/%20blockchain%20-%20basics/how-%20does-%20blockchain-%20work. (accessed: 30.05.2018).

[Liu+18a] L. Liu et al. "Detecting and Preventing Cyber Insider Threats: A Survey". In: *IEEE Communications Surveys Tutorials* 20.2 (2018), pp. 1397–1417. DOI: 10.1109/COMST.2018.2800740.

[Liu+18b] W. Liu et al. "Reliability Modeling and Evaluation of Active Cyber Physical Distribution System". In: *IEEE Transactions on Power Systems* 33.6 (2018), pp. 7096–7108. DOI: 10.1109/TPWRS.2018.2854642.

[LSS14] H. Lei, C. Singh, and A. Sprintson. "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems". In: *IEEE Transactions on Smart Grid* 5.5 (Sept. 2014), pp. 2194–2202. ISSN: 1949-3061. DOI: 10.1109/TSG.2014.2314616.

[MA16] M. Mohsin and Z. Anwar. "Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics". In: *2016 International Conference on Frontiers of Information Technology (FIT)*. 2016, pp. 23–28. DOI: 10.1109/FIT.2016.013.

[Man+15a] M. Manbachi et al. "Real-time co-simulated platform for novel Volt-VAR Optimization of smart distribution network using AMI data". In: *2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. 2015, pp. 1–7.

[Man+15b] M. Manbachi et al. "Real-time communication platform for Smart Grid adaptive Volt-VAR Optimization of distribution networks". In: *2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. 2015, pp. 1–7. DOI: 10.1109/SEGE.2015.7324592.

[Man+16a] M. Manbachi et al. "Impact of EV penetration on Volt–VAR Optimization of distribution networks using real-time co-simulation monitoring platform". In: *Applied Energy* 169 (2016), pp. 28–39. ISSN: 0306-2619. DOI: https://doi.org/10.

1016/j.apenergy.2016.01.084. URL: https://www.sciencedirect.com/science/article/pii/S030626191630071X.

[Man+16b] M. Manbachi et al. "Real-Time Co-Simulation Platform for Smart Grid Volt-VAR Optimization Using IEC 61850". In: *IEEE Transactions on Industrial Informatics* 12.4 (2016), pp. 1392–1402.

[Mar+14] A. K. Marvasti et al. "Optimal Operation of Active Distribution Grids: A System of Systems Framework". In: *IEEE Transactions on Smart Grid* 5.3 (2014), pp. 1228–1237.

[McK+17] P. McKeever et al. "MAS for automated black start of multi-microgrids". In: *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 2017, pp. 32–37.

[McK+20] P. McKeever et al. "Ensuring Uninterrupted MTC Service Availability during Emergencies Using LTE/5G Public Mobile Land Networks". In: *Telecom* 1.3 (2020), pp. 181–195. URL: https://www.mdpi.com/2673-4001/1/3/13.

[MG17] M. Mylrea and S. N. G. Gourisetti. "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security". In: *2017 Resilience Week (RWS)*. 2017, pp. 18–23. DOI: 10.1109/RWEEK.2017.8088642.

[MIS19] K. M. Muttaqi, M. R. Islam, and D. Sutanto. "Future Power Distribution Grids: Integration of Renewable Energy, Energy Storage, Electric Vehicles, Superconductor, and Magnetic Bus". In: *IEEE Transactions on Applied Superconductivity* 29.2 (2019), pp. 1–5. DOI: 10.1109/TASC.2019.2895528.

[MLL12] F. Ma, F. Liu, and Z. Liu. "Distributed load balancing allocation of virtual machine in cloud data center". In: *2012 IEEE International Conference on Computer Science and Automation Engineering*. June 2012, pp. 20–23. DOI: 10.1109/ICSESS.2012.6269396.

[Mol81] M. Molloy. *On the integration of delay and throughput measures in distributed processing models*. University of California, Los Angeles, 1981. URL: https://books.google.de/books?id=TrOZAQAAIAAJ.

[Mon+15] A. Monti et al. *Dual Demand Side Management : E.ON gGmbH Project : Project No. 30; First edition*. Tech. rep. Zweitveröffentlicht auf dem Publikationsserver der RWTH Aachen University 2016. - Weiterer DOI 10.18154/RWTH-2015-07284. Aachen, 2015, II, 139 Seiten : grafische Darstellungen. DOI: 10.18154/RWTH-2016-05485. URL: https://publications.rwth-aachen.de/record/660613.

[MP16] A. Monti and F. Ponci. "The Digitalization of Distribution Systems". In: *IEEE Smart Grid: A Special Issue on the Smart Grid in the European Region* (2016).

[MRS16] A. Monti, A. Roscoe, and A. Sadu. "Chapter 6 - International Standards for PMU and Tests for Compliance". In: *Phasor Measurement Units and Wide Area Monitoring Systems*. Ed. by A. Monti, C. Muscas, and F. Ponci. Academic Press, 2016, pp. 87–121. ISBN: 978-0-12-804569-5. DOI: https://doi.org/10.1016/B978-0-12-804569-5.00006-9. URL: https://www.sciencedirect.com/science/article/pii/B9780128045695000069.

[MST16] A. Monti, A. Sadu, and J. Tang. "Chapter 8 - Wide Area Measurement Systems: Applications". In: *Phasor Measurement Units and Wide Area Monitoring Systems*. Ed. by A. Monti, C. Muscas, and F. Ponci. Academic Press, 2016, pp. 177–234. ISBN: 978-0-12-804569-5. DOI: https://doi.org/10.1016/B978-0-12-804569-5.00008-2. URL: https://www.sciencedirect.com/science/article/pii/B9780128045695000082.

[Mur89] T. Murata. "Petri nets: Properties, analysis and applications". In: *Proceedings of the IEEE* 77.4 (1989), pp. 541–580. DOI: 10.1109/5.24143.

[Nak] S. Nakamoto. *Bitcoin*. URL: https://bitcoin.org/bitcoin.pdf. (accessed: 11.05.2018).

[NI99] T. Nakajima and S. Irokawa. "A control system for HVDC transmission by voltage sourced converters". In: *1999 IEEE Power Engineering Society Summer Meeting. Conference Proceedings (Cat. No.99CH36364)*. Vol. 2. July 1999, 1113–1119 vol.2.

[Nod] Node-Red. *Node-Red*. URL: https://nodered.org/. (accessed: 21.04.2018).

[Nod18a] Node-Red. *Node-Red*. https://nodered.org/. [Online; accessed 21-April-2018]. 2018.

[Nod18b] Node-Red. *Node-Red-Contrib-Composer*. https://www.npmjs.com/package/node-red-contrib-composer. [Online; accessed 01-May-2018]. 2018.

[NRG] NRG5. *NRG5 : Energy as a service using 5G Technologies*. URL: http://www.nrg5.eu/. (accessed: 01.01.2021).

[Ori+20] G. D. Orio et al. "A Cyber-Physical Approach to Resilience and Robustness by Design". In: *International Journal of Advanced Computer Science and Applications* 11.7 (2020). DOI: 10.14569/IJACSA.2020.0110710. URL: http://dx.doi.org/10.14569/IJACSA.2020.0110710.

[PA15] P. Persson and O. Angelsmark. "Calvin – Merging Cloud and IoT". In: *Procedia Computer Science* 52 (2015). The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015), pp. 210–217. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2015.05.059. URL: http://www.sciencedirect.com/science/article/pii/S1877050915008595.

[Pat+16] D. Patel et al. "Investigating the performance of QoS enabled LTE networks for IEC 61850 based smart grid applications". In: *2016 IEEE International Energy Conference (ENERGYCON)*. 2016, pp. 1–6. DOI: 10.1109/ENERGYCON.2016.7513965.

[Pat+18] M.-E. Paté-Cornell et al. "Cyber risk management for critical infrastructure: a risk analysis model and three case studies". en. In: *Risk Analysis* 38.2 (2018), pp. 226–241.

[Pau+16a] M. Pau et al. "A state estimation algorithm for hybrid AC/DC networks with multi-terminal DC grid". In: *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. 2016, pp. 1–6. DOI: 10.1109/ISGTEurope.2016.7856278.

[Pau+16b] M. Pau et al. "Low voltage system state estimation based on smart metering infrastructure". In: *2016 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. 2016, pp. 1–6. DOI: 10.1109/AMPS.2016.7602804.

[Pau+18] M. Pau et al. “A cloud-based smart metering infrastructure for distribution grid services and automation”. In: *Sustainable Energy, Grids and Networks* 15 (2018). Technologies and Methodologies in Modern Distribution Grid Automation, pp. 14–25. ISSN: 2352-4677. DOI: https://doi.org/10.1016/j.segan.2017.08.001. URL: https://www.sciencedirect.com/science/article/pii/S2352467716301783.

[Pau+19a] M. Pau et al. “Design and Accuracy Analysis of Multilevel State Estimation Based on Smart Metering Infrastructure”. In: *IEEE Transactions on Instrumentation and Measurement* 68.11 (2019), pp. 4300–4312.

[Pau+19b] M. Pau et al. “Impact of Current and Power Measurements on Distribution System State Estimation Uncertainty”. In: *IEEE Transactions on Instrumentation and Measurement* 68.10 (2019), pp. 3992–4002.

[PB10] L. Piètre-Cambacédès and M. Bouissou. “Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP)”. In: *2010 European Dependable Computing Conference*. IEEE. 2010, pp. 199–208.

[Pig13] R. Piggin. “Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security”. In: *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*. 2013, pp. 1–6. DOI: 10.1049/cp.2013.0001.

[PJ21] D. Preuveneers and W. Joosen. “Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence”. In: *Journal of Cybersecurity and Privacy* 1.1 (2021), pp. 140–163. ISSN: 2624-800X. DOI: 10.3390/jcp1010008. URL: https://www.mdpi.com/2624-800X/1/1/8.

[PLA] PLATONE. *Platone : PLATform for Operatig distribution NEtworks*. URL: https://platone-h2020.eu/. (accessed: 01.01.2021).

[Pon+18] F. Ponci et al. “Instrumentation and measurement testing in the real-time lab for automation of complex power systems”. In: *IEEE Instrumentation Measurement Magazine* 21.1 (2018), pp. 17–24.

[Pra] ". K. "Praerit Garg". *The STRIDE Threat Model*. URL: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN. (accessed: 27.06.2021).

[PST17] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong. "Performance Analysis of Private Blockchain Platforms in Varying Workloads". In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. July 2017, pp. 1–6. DOI: 10.1109/ICCCN.2017.8038517.

[Rab] H. Rabbani. *What is Hashing and Digital Signature in The Blockchain?* URL: https://blockgeeks.com/what-%20is-%20hashing-%20digital-%20signature-%20in%20the-%20blockchain/. (accessed: 11.05.2018).

[Rep+17] S. Repo et al. "The IDE4L Project: Defining, Designing, and Demonstrating the Ideal Grid for All". In: *IEEE Power and Energy Magazine* 15.3 (2017), pp. 41–51.

[RJL18] H. Ruiwen, D. Jianhua, and L. L. Lai. "Reliability Evaluation of Communication-Constrained Protection Systems Using Stochastic-Flow Network Models". In: *IEEE Transactions on Smart Grid* 9.3 (2018), pp. 2371–2381. DOI: 10.1109/TSG.2017.2727227.

[RMT] R.M.Lee, M.J.Assante, and T.Conway. *Analysis of the Cyber Attack on the Ukrainian Power Grid : Defnse Use Case*. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[Rob16] T. Robert.M Michael.J. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. 2016. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. (accessed: 03.01.2021).

[Roy+19] G. K. Roy et al. "Inclusion of converter controller measurements into state estimation algorithm for hybrid ac-dc grid". In: *2019 IEEE Milan PowerTech*. 2019, pp. 1–6. DOI: 10.1109/PTC.2019.8810853.

[RPD14] S. Repo, F. Ponci, and D. Della Giustina. "Holistic view of active distribution network and evolution of distribution automation". In: *IEEE PES Innovative Smart Grid Technologies, Europe*. 2014, pp. 1–6. DOI: 10.1109/ISGTEurope.2014.7028980.

[RR17] P. Rodriguez and K. Rouzbehi. “Multi-terminal DC grids: challenges and prospects”. In: *Journal of Modern Power Systems and Clean Energy* 5.4 (July 2017), pp. 515–523. ISSN: 2196-5420. DOI: 10.1007/s40565-017-0305-0.

[Saa87] R. Saaty. “The analytic hierarchy process—what it is and how it is used”. In: *Mathematical Modelling* 9.3 (1987), pp. 161–176. ISSN: 0270-0255. DOI: https://doi.org/10.1016/0270-0255(87)90473-8. URL: http://www.sciencedirect.com/science/article/pii/0270025587904738.

[Sad+14] A. Sadu et al. “A platform for testing monitoring systems for the power distribution grid”. In: *2014 IEEE International Workshop on Applied Measurements for Power Systems Proceedings (AMPS)*. 2014, pp. 1–6. DOI: 10.1109/AMPS.2014.6947714.

[Sad+16] A. Sadu et al. “Impact of uncertainty propagation on the design of state estimation for hybrid ac-dc grids”. In: *2016 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. 2016, pp. 1–6.

[Sad+18] A. Sadu et al. “Resilient design of distribution grid automation system with CALVIN”. In: *2018 IEEE International Energy Conference (ENERGYCON)*. 2018, pp. 1–6.

[Sad+20a] A. Sadu et al. “A Stochastic Assessment of Attacks based on Continuous-Time Markov Chains”. In: *2020 6th IEEE International Energy Conference (ENERGYCon)*. 2020, pp. 11–16. DOI: 10.1109/ENERGYCon48941.2020.9236600.

[Sad+20b] A. Sadu et al. “Methodology for Reliability Analysis of Cyber-Physical MTdc Grids”. In: *IEEE Journal of Emerging and Selected Topics in Power Electronics* (2020), pp. 1–1.

[Sad+20c] A. Sadu et al. “Verfahren und Vorrichtungen für eine Lastzuweisung und Überwachung für eine zuzuweisende versorgungssicherheitskritische Ressource in einem Netzwerk”. U.S. pat. DE 10 2019 203 874.3. Mar. 1, 2020.

[Sad+21] A. Sadu et al. “Resilient Design of Distribution Grid Automation System against cyber-physical attacks using Blockchain and Smart Contract”. In: *Blockchain: Research and Applications* (2021), p. 100010. ISSN: 2096-7209. DOI: https://doi.org/10.1016/j.bcra.2021.100010. URL: https://www.sciencedirect.com/science/article/pii/S2096720921000051.

[SBL17] P. Stahl, J. Broberg, and B. Landfeldt. "Dynamic Fault-Tolerance and Mobility Provisioning for Services on Mobile Cloud Platforms". In: *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. Apr. 2017, pp. 131–138. DOI: 10.1109/MobileCloud.2017.7.

[SBV18] J. Sousa, A. Bessani, and M. Vukolic. "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform". In: *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2018, pp. 51–58. DOI: 10.1109/DSN.2018.00018.

[Sch17] M. Scherer. "Performance and Scalability of Blockchain Networks and Smart Contracts". MA thesis. Umeå University, Department of Computing Science, 2017, p. 46.

[Sch99] B. Schneier. "Attack trees". In: *Dr. Dobb's journal* 24.12 (1999), pp. 21–29.

[She+19] F. Shen et al. "Comprehensive Congestion Management for Distribution Networks Based on Dynamic Tariff, Reconfiguration, and Re-Profiling Product". In: *IEEE Transactions on Smart Grid* 10.5 (2019), pp. 4795–4805. DOI: 10.1109/TSG.2018.2868755.

[Sho72] M. L. Shooman. "PROBABILISTIC MODELS FOR SOFTWARE RELIABILITY PREDICTION". In: *Statistical Computer Performance Evaluation*. Ed. by W. Freiberger. Academic Press, 1972, pp. 485–502. ISBN: 978-0-12-266950-7. DOI: https://doi.org/10.1016/B978-0-12-266950-7.50029-3. URL: http://www.sciencedirect.com/science/article/pii/B9780122669507500293.

[Sho73] M. L. Shooman. "Operational testing and software reliability estimation during program development". In: 1973.

[Sil+21] R. Silva et al. "Characterization of TSO and DSO Grid System Services and TSO-DSO Basic Coordination Mechanisms in the Current Decarbonization Context". In: *Energies* 14.15 (2021). ISSN: 1996-1073. DOI: 10.3390/en14154451. URL: https://www.mdpi.com/1996-1073/14/15/4451.

[SM] S. Sinha and A. Morrison. URL: http://usblogs.pwc.com/emergingtechnology/%20a-%20primer-%20on-%20blockchain-%20infographic/. (accessed: 25.05.2018).

[Smi14] R. Smith. “Assault on California power station raises alarm on potential for terrorism”. In: *Wall Street Journal* (2014), pp. 1–7.

[Son99] I. Sonin. “The State Reduction and Related Algorithms and Their Applications to the Study of Markov Chains, Graph Theory, and the Optimal Stopping Problem”. In: *Advances in Mathematics* 145.2 (1999), pp. 159–188. ISSN: 0001-8708. DOI: https://doi.org/10.1006/aima.1998.1813. URL: http://www.sciencedirect.com/science/article/pii/S0001870898918138.

[SS14] S. Souissi and A. Serhrouchni. “AIDD: A novel generic attack modeling approach”. In: *2014 International Conference on High Performance Computing Simulation (HPCS)*. July 2014, pp. 580–583. DOI: 10.1109/HPCSim.2014.6903738.

[SUC] SUCCESS. *SUCCESS : SecUring CritiCal Energy InfraStructureS*. URL: https://www.success-energy.eu/. (accessed: 01.01.2021).

[Suc] Success-Consortium. *Securing Critical Energy Infrastructure*. URL: https://success-energy.eu/. (accessed: 25.06.2020).

[SW13] Y. Song and B. Wang. “Survey on Reliability of Power Electronic Systems”. In: *IEEE Transactions on Power Electronics* 28 (Jan. 2013), pp. 591–604. DOI: 10.1109/TPEL.2012.2192503.

[SWB04] J. Salmeron, K. Wood, and R. Baldick. “Analysis of electric grid security under terrorist threat”. In: *IEEE Transactions on Power Systems* 19.2 (2004), pp. 905–912. DOI: 10.1109/TPWRS.2004.825888.

[Sza] N. Szabo. URL: http://www.fon.hum.uva.nl/rob/Courses/%20InformationInSpeech/CDROM/Literature/LOTWinterschool2006/szabo.%20best%20.%20vwh%20.%20net%20/%20smart%20.%20contracts%20.%20html. (accessed: 16.05.2018).

[Tah+20] M. Tahir et al. “A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities”. In: *IEEE Access* 8 (2020), pp. 115876–115904. DOI: 10.1109/ACCESS.2020.3003020.

[TB17] K. S. Trivedi and A. Bobbio. *Reliability and Availability Engineering: Modeling, Analysis, and Applications*. Cambridge University Press, 2017. ISBN: 1107099501.

[TCF09] V. Terzija, D. Cai, and J. Fitch. “Protection scheme for blackout prevention in distribution networks with mixed energy resources”. In: *2009 International Conference on Sustainable Power Generation and Supply*. 2009, pp. 1–7. DOI: 10.1109/SUPERGEN.2009.5654665.

[Tha12] G. Thangamani. “Generalized Stochastic Petri Nets for Reliability Analysis of Lube Oil System with Common-Cause Failures”. In: *American Journal of Computational and Applied Mathematics* 2.4 (Aug. 2012), pp. 152–158. DOI: 10.5923/j.ajcam.20120204.03. URL: https://doi.org/10.5923%2Fj.ajcam.20120204.03.

[The16] The Times of Israel. *Steinitz: Israel’s Electric Authority Hit by ‘Severe’ Cyber-Attack*. 2016. URL: http://www.timesofisrael.com/steinitz-israels-electric-authority-hit-bysevere-%20cyber-attack/.

[TNV18] P. Thakkar, S. Nathan, and B. Viswanathan. “Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform”. In: *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. 2018, pp. 264–276. DOI: 10.1109/MASCOTS.2018.00034.

[Tre05] M. Treaster. “A Survey of Fault-Tolerance and Fault-Recovery Techniques in Parallel Systems”. In: *CoRR* abs/cs/0501002 (2005). arXiv: cs/0501002. URL: http://arxiv.org/abs/cs/0501002.

[Tzo19] D. Tzovaras. *Computer vision systems : 12th international conference, ICVS 2019, Thessaloniki, Greece, September 23-25, 2019, proceedings*. Cham: Springer, 2019. ISBN: 978-3-030-34995-0.

[UM15] T. UcedaVelez and M. Morana. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Wiley, 2015. ISBN: 9780470500965.

[Wan+14] H. Wang et al. “Transitioning to Physics-of-Failure as a Reliability Driver in Power Electronics”. In: *IEEE Journal of Emerging and Selected Topics in Power Electronics* 2.1 (Mar. 2014), pp. 97–114. ISSN: 2168-6785. DOI: 10.1109/JESTPE.2013.2290282.

[Wan12] J. Wang. *Timed Petri Nets - Theory and Application*. Berlin Heidelberg: Springer Science and Business Media, 2012. ISBN: 978-1-461-55537-7.

[WBQ18] C. Werner, T. Bedford, and J. Quigley. "Sequential refined partitioning for probabilistic dependence assessment". fr. In: *Risk Analysis* 38.12 (2018), pp. 2683–2702.

[WMB05] F. Wu, K. Moslehi, and A. Bose. "Power System Control Centers: Past, Present, and Future". In: *Proceedings of the IEEE* 93.11 (2005), pp. 1890–1908. DOI: 10.1109/JPROC.2005.857499.

[WTW16] B. Wu, A. Tang, and J. Wu. "Modeling cascading failures in interdependent infrastructures under terrorist attacks". en. In: *Reliability Engineering System Safety* 147 (2016), pp. 1–8.

[XDX15] M. Xu, G. Da, and S. Xu. "Cyber epidemic models with dependences". en. In: *Internet Mathematics* 11.1 (2015), pp. 62–92.

[Yue11] Z. Yue. "A method for group decision-making based on determining weights of decision makers using TOPSIS". In: *Applied Mathematical Modelling* 35.4 (2011), pp. 1926–1936. ISSN: 0307-904X. DOI: https://doi.org/10.1016/j.apm.2010.11.001. URL: http://www.sciencedirect.com/science/article/pii/S0307904X10004117.

[Zha+17] L. Zhang et al. "Modeling, control, and protection of modular multilevel converter-based multi-terminal HVDC systems: A review". In: *CSEE Journal of Power and Energy Systems* 3.4 (Dec. 2017), pp. 340–352. DOI: 10.17775/CSEEJPES.2017.00440.

[ZLW21] H. Zhang, B. Liu, and H. Wu. "Smart Grid Cyber-Physical Attack and Defense: A Review". In: *IEEE Access* 9 (2021), pp. 29641–29659. DOI: 10.1109/ACCESS.2021.3058628.

[Zog+21] I. Zografopoulos et al. "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies". In: *IEEE Access* 9 (2021), pp. 29775–29818. DOI: 10.1109/ACCESS.2021.3058403.

E.ON ERC Band 1
Streblow, R.
Thermal Sensation and Comfort Model for Inhomogeneous Indoor Environments
1. Auflage 2011
ISBN 978-3-942789-00-4

E.ON ERC Band 2
Naderi, A.
Multi-phase, multi-species reactive transport modeling as a tool for system analysis in geological carbon dioxide storage
1. Auflage 2011
ISBN 978-3-942789-01-1

E.ON ERC Band 3
Westner, G.
Four Essays related to Energy Economic Aspects of Combined Heat and Power Generation
1. Auflage 2012
ISBN 978-3-942789-02-8

E.ON ERC Band 4
Lohwasser, R.
Impact of Carbon Capture and Storage (CCS) on the European Electricity Market
1. Auflage 2012
ISBN 978-3-942789-03-5

E.ON ERC Band 5
Dick, C.
Multi-Resonant Converters as Photovoltaic Module-Integrated Maximum Power Point Tracker
1. Auflage 2012
ISBN 978-3-942789-04-2

E.ON ERC Band 6
Lenke, R.
A Contribution to the Design of Isolated DC-DC Converters for Utility Applications
1. Auflage 2012
ISBN 978-3-942789-05-9

E.ON ERC Band 7
Brännström, F.
Einsatz hybrider RANS-LES-Turbulenzmodelle in der Fahrzeugklimatisierung
1. Auflage 2012
ISBN 978-3-942789-06-6

E.ON ERC Band 8
Bragard, M.
The Integrated Emitter Turn-Off Thyristor - An Innovative MOS-Gated High-Power Device
1. Auflage 2012
ISBN 978-3-942789-07-3

E.ON ERC Band 9
Hoh, A.
Exergiebasierte Bewertung gebäudetechnischer Anlagen
1. Auflage 2013
ISBN 978-3-942789-08-0

E.ON ERC Band 10
Köllensperger, P.
The Internally Commutated Thyristor - Concept, Design and Application
1. Auflage 2013
ISBN 978-3-942789-09-7

E.ON ERC Band 11
Achtnicht, M.
Essays on Consumer Choices Relevant to Climate Change: Stated Preference Evidence from Germany
1. Auflage 2013
ISBN 978-3-942789-10-3

E.ON ERC Band 12
Panašková, J.
Olfaktorische Bewertung von Emissionen aus Bauprodukten
1. Auflage 2013
ISBN 978-3-942789-11-0

E.ON ERC Band 13
Vogt, C.
Optimization of Geothermal Energy Reservoir Modeling using Advanced Numerical Tools for Stochastic Parameter Estimation and Quantifying Uncertainties
1. Auflage 2013
ISBN 978-3-942789-12-7

E.ON ERC Band 14
Benigni, A.
Latency exploitation for parallelization of power systems simulation
1. Auflage 2013
ISBN 978-3-942789-13-4

E.ON ERC Band 15
Butschen, T.
Dual-ICT – A Clever Way to Unite Conduction and Switching Optimized Properties in a Single Wafer
1. Auflage 2013
ISBN 978-3-942789-14-1

E.ON ERC Band 16
Li, W.
Fault Detection and Protection inMedium Voltage DC Shipboard Power Systems
1. Auflage 2013
ISBN 978-3-942789-15-8

E.ON ERC Band 17
Shen, J.
Modeling Methodologies for Analysis and Synthesis of Controls and Modulation Schemes for High-Power Converters with Low Pulse Ratios
1. Auflage 2014
ISBN 978-3-942789-16-5

E.ON ERC Band 18
Flieger, B.
Innenraummodellierung einer Fahrzeugkabine in der Programmiersprache Modelica
1. Auflage 2014
ISBN 978-3-942789-17-2

E.ON ERC Band 19
Liu, J.
Measurement System and Technique for Future Active Distribution Grids
1. Auflage 2014
ISBN 978-3-942789-18-9

E.ON ERC Band 20
Kandzia, C.
Experimentelle Untersuchung der Strömungsstrukturen in einer Mischlüftung
1. Auflage 2014
ISBN 978-3-942789-19-6

E.ON ERC Band 21
Thomas, S.
A Medium-Voltage Multi-Level DC/DC Converter with High Voltage Transformation Ratio
1. Auflage 2014
ISBN 978-3-942789-20-2

E.ON ERC Band 22
Tang, J.
Probabilistic Analysis and Stability Assessment for Power Systems with Integration of Wind Generation and Synchrophasor Measurement
1. Auflage 2014
ISBN 978-3-942789-21-9

E.ON ERC Band 23
Sorda, G.
The Diffusion of Selected Renewable Energy Technologies: Modeling, Economic Impacts, and Policy Implications
1. Auflage 2014
ISBN 978-3-942789-22-6

E.ON ERC Band 24
Rosen, C.
Design considerations and functional analysis of local reserve energy markets for distributed generation
1. Auflage 2014
ISBN 978-3-942789-23-3

E.ON ERC Band 25
Ni, F.
Applications of Arbitrary Polynomial Chaos in Electrical Systems
1. Auflage 2015
ISBN 978-3-942789-24-0

E.ON ERC Band 26
Michelsen, C. C.
The *Energiewende* in the German Residential Sector: Empirical Essays on Homeowners' Choices of Space Heating Technologies
1. Auflage 2015
ISBN 978-3-942789-25-7

E.ON ERC Band 27
Rohlfs, W.
Decision-Making under Multi-Dimensional Price Uncertainty for Long-Lived Energy Investments
1. Auflage 2015
ISBN 978-3-942789-26-4

E.ON ERC Band 28
Wang, J.
Design of Novel Control algorithms of Power Converters for Distributed Generation
1. Auflage 2015
ISBN 978-3-942789-27-1

E.ON ERC Band 29
Helmedag, A.
System-Level Multi-Physics Power Hardware in the Loop Testing for Wind Energy Converters
1. Auflage 2015
ISBN 978-3-942789-28-8

E.ON ERC Band 30
Togawa, K.
Stochastics-based Methods Enabling Testing of Grid-related Algorithms through Simulation
1. Auflage 2015
ISBN 978-3-942789-29-5

E.ON ERC Band 31
Huchtemann, K.
Supply Temperature Control Concepts in Heat Pump Heating Systems
1. Auflage 2015
ISBN 978-3-942789-30-1

E.ON ERC Band 32
Molitor, C.
Residential City Districts as Flexibility Resource: Analysis, Simulation, and Decentralized Coordination Algorithms
1. Auflage 2015
ISBN 978-3-942789-31-8

E.ON ERC Band 33
Sunak, Y.
Spatial Perspectives on the Economics of Renewable Energy Technologies
1. Auflage 2015
ISBN 978-3-942789-32-5

E.ON ERC Band 34
Cupelli, M.
Advanced Control Methods for Robust Stability of MVDC Systems
1. Auflage 2015
ISBN 978-3-942789-33-2

E.ON ERC Band 35
Chen, K.
Active Thermal Management for Residential Air Source Heat Pump Systems
1. Auflage 2015
ISBN 978-3-942789-34-9

E.ON ERC Band 36
Pâques, G.
Development of SiC GTO Thyristors with Etched Junction Termination
1. Auflage 2016
ISBN 978-3-942789-35-6

E.ON ERC Band 37
Garnier, E.
Distributed Energy Resources and Virtual Power Plants: Economics of Investment and Operation
1. Auflage 2016
ISBN 978-3-942789-37-0

E.ON ERC Band 38
Calì, D.
Occupants' Behavior and its Impact upon the Energy Performance of Buildings
1. Auflage 2016
ISBN 978-3-942789-36-3

E.ON ERC Band 39
Isermann, T.
A Multi-Agent-based Component Control and Energy Management System for Electric Vehicles
1. Auflage 2016
ISBN 978-3-942789-38-7

E.ON ERC Band 40
Wu, X.
New Approaches to Dynamic Equivalent of Active Distribution Network for Transient Analysis
1. Auflage 2016
ISBN 978-3-942789-39-4

E.ON ERC Band 41
Garbuzova-Schiftler, M.
The Growing ESCO Market for Energy Efficiency in Russia: A Business and Risk Analysis
1. Auflage 2016
ISBN 978-3-942789-40-0

E.ON ERC Band 42
Huber, M.
Agentenbasierte Gebäudeautomation für raumlufttechnische Anlagen
1. Auflage 2016
ISBN 978-3-942789-41-7

E.ON ERC Band 43
Soltau, N.
High-Power Medium-Voltage DC-DC Converters: Design, Control and Demonstration
1. Auflage 2017
ISBN 978-3-942789-42-4

E.ON ERC Band 44
Stieneker, M.
Analysis of Medium-Voltage Direct-Current Collector Grids in Offshore Wind Parks
1. Auflage 2017
ISBN 978-3-942789-43-1

E.ON ERC Band 45
Bader, A.
Entwicklung eines Verfahrens zur Strompreisvorhersage im kurzfristigen Intraday-Handelszeitraum
1. Auflage 2017
ISBN 978-3-942789-44-8

E.ON ERC Band 46
Chen, T.
Upscaling Permeability for Fractured Porous Rocks and Modeling Anisotropic Flow and Heat Transport
1. Auflage 2017
ISBN 978-3-942789-45-5

E.ON ERC Band 47
Ferdowsi, M.
Data-Driven Approaches for Monitoring of Distribution Grids
1. Auflage 2017
ISBN 978-3-942789-46-2

E.ON ERC Band 48
Kopmann, N.
Betriebsverhalten freier Heizflächen unter zeitlich variablen Randbedingungen
1. Auflage 2017
ISBN 978-3-942789-47-9

E.ON ERC Band 49
Fütterer, J.
Tuning of PID Controllers within Building Energy Systems
1. Auflage 2017
ISBN 978-3-942789-48-6

E.ON ERC Band 50
Adler, F.
A Digital Hardware Platform for Distributed Real-Time Simulation of Power Electronic Systems
1. Auflage 2017
ISBN 978-3-942789-49-3

E.ON ERC Band 51
Harb, H.
Predictive Demand Side Management Strategies for Residential Building Energy Systems
1. Auflage 2017
ISBN 978-3-942789-50-9

E.ON ERC Band 52
Jahangiri, P.
Applications of Paraffin-Water Dispersions in Energy Distribution Systems
1. Auflage 2017
ISBN 978-3-942789-51-6

E.ON ERC Band 53
Adolph, M.
Identification of Characteristic User Behavior with a Simple User Interface in the Context of Space Heating
1. Auflage 2018
ISBN 978-3-942789-52-3

E.ON ERC Band 54
Galassi, V.
Experimental evidence of private energy consumer and prosumer preferences in the sustainable energy transition
1. Auflage 2017
ISBN 978-3-942789-53-0

E.ON ERC Band 55
Sangi, R.
Development of Exergy-based Control Strategies for Building Energy Systems
1. Auflage 2018
ISBN 978-3-942789-54-7

E.ON ERC Band 56
Stinner, S.
Quantifying and Aggregating the Flexibility of Building Energy Systems
1. Auflage 2018
ISBN 978-3-942789-55-4

E.ON ERC Band 57
Fuchs, M.
Graph Framework for Automated Urban Energy System Modeling
1. Auflage 2018
ISBN 978-3-942789-56-1

E.ON ERC Band 58
Osterhage, T.
Messdatengestützte Analyse und Interpretation sanierungsbedingter Effizienzsteigerungen im Wohnungsbau
1. Auflage 2018
ISBN 978-3-942789-57-8

E.ON ERC Band 59
Frieling, J.
Quantifying the Role of Energy in Aggregate Production Functions for Industrialized Countries
1. Auflage 2018
ISBN 978-3-942789-58-5

E.ON ERC Band 60
Lauster, M.
Parametrierbare Gebäudemodelle für dynamische Energiebedarfsrechnungen von Stadtquartieren
1. Auflage 2018
ISBN 978-3-942789-59-2

E.ON ERC Band 61
Zhu, L.
Modeling, Control and Hardware in the Loop in Medium Voltage DC Shipboard Power Systems
1. Auflage 2018
ISBN 978-3-942789-60-8

E.ON ERC Band 62
Feron, B.
An optimality assessment methodology for Home Energy Management System approaches based on uncertainty analysis
1. Auflage 2018
ISBN 978-3-942789-61-5

E.ON ERC Band 63
Diekerhof, M.
Distributed Optimization for the Exploitation of Multi-Energy Flexibility under Uncertainty in City Districts
1. Auflage 2018
ISBN 978-3-942789-62-2

E.ON ERC Band 64
Wolisz, H.
Transient Thermal Comfort Constraints for Model Predictive Heating Control
1. Auflage 2018
ISBN 978-3-942789-63-9

E.ON ERC Band 65
Pickartz, S.
Virtualization as an Enabler for Dynamic Resource Allocation in HPC
1. Auflage 2019
ISBN 978-3-942789-64-6

E.ON ERC Band 66
Khayyamim, S.
Centralized-decentralized Energy Management in Railway System
1. Auflage 2019
ISBN 978-3-942789-65-3

E.ON ERC Band 67
Schlösser, T.
Methodology for Holistic Evaluation of Building Energy Systems under Dynamic Boundary Conditions
1. Auflage 2019
ISBN 978-3-942789-66-0

E.ON ERC Band 68
Cui, S.
Modular Multilevel DC-DC Converters Interconnecting High-Voltage and Medium-Voltage DC Grids
1. Auflage 2019
ISBN 978-3-942789-67-7

E.ON ERC Band 69
Hu, J.
Modulation and Dynamic Control of Intelligent Dual-Active-Bridge Converter Based Substations for Flexible DC Grids
1. Auflage 2019
ISBN 978-3-942789-68-4

E.ON ERC Band 70
Schiefelbein, J.
Optimized Placement of Thermo-Electric Energy Systems in City Districts under Uncertainty
1. Auflage 2019
ISBN 978-3-942789-69-1

E.ON ERC Band 71
Ferdinand, R.
Grid Operation of HVDC-Connected Offshore Wind Farms: Power Quality and Switching Strategies
1. Auflage 2019
ISBN 978-3-942789-70-7

E.ON ERC Band 72
Musa, A.
Advanced Control Strategies for Stability Enhancement of Future Hybrid AC/DC Networks
1. Auflage 2019
ISBN 978-3-942789-71-4

E.ON ERC Band 73
Angioni, A.
Uncertainty modeling for analysis and design of monitoring systems for dynamic electrical distribution grids
1. Auflage 2019
ISBN 978-3-942789-72-1

E.ON ERC Band 74
Möhlenkamp, M.
Thermischer Komfort bei Quellluftströmungen
1. Auflage 2019
ISBN 978-3-942789-73-8

E.ON ERC Band 75
Voss, J.
Multi-Megawatt Three-Phase Dual-Active Bridge DC-DC Converter
1. Auflage 2019
ISBN 978-3-942789-74-5

E.ON ERC Band 76
Siddique, H.
The Three-Phase Dual-Active Bridge Converter Family: Modeling, Analysis, Optimization and Comparison of Two-Level and Three-Level Converter Variants
1. Auflage 2019
ISBN 978-3-942789-75-2

E.ON ERC Band 77
Heesen, F.
An Interdisciplinary Analysis of Heat Energy Consumption in Energy-Efficient Homes: Essays on Economic, Technical and Behavioral Aspects
1. Auflage 2019
ISBN 978-3-942789-76-9

E.ON ERC Band 78
Möller, R.
Untersuchung der Durchschlagspannung von Mineral-, Silikonölen und synthetischen Estern bei mittelfrequenten Spannungen
1. Auflage 2020
ISBN 978-3-942789-77-6

E.ON ERC Band 79
Höfer, T.
Transition Towards a Renewable Energy Infrastructure: Spatial Interdependencies and Stakeholder Preferences
1. Auflage 2020
ISBN 978-3-942789-78-3

E.ON ERC Band 80
Freitag, H.
Investigation of the Internal Flow Behavior in Active Chilled Beams
1. Auflage 2020
ISBN 978-3-942789-79-0

E.ON ERC Band 81
Razik, L.
High-Performance Computing Methods in Large-Scale Power System Simulation
1. Auflage 2020
ISBN 978-3-942789-80-6

E.ON ERC Band 82
Mirz, M.
A Dynamic Phasor Real-Time Simulation Based Digital Twin for Power Systems
1. Auflage 2020
ISBN 978-3-942789-81-3

E.ON ERC Band 83
Schmitz, H.
Energy Consumption Behavior of Private Households: Heterogeneity, Prosuming, and Rebound
1. Auflage 2020
ISBN 978-3-942789-82-0

E.ON ERC Band 84
Cupelli, L.
Data-driven Methods for Voltage Control in Distribution Networks: A Bottom-Up Approach
1. Auflage 2020
ISBN 978-3-942789-83-7

E.ON ERC Band 85
Happ, S.
A Scalable Simulation Method for Cyber-Physical Power Systems
1. Auflage 2020
ISBN 978-3-942789-84-4

E.ON ERC Band 86
Rewitz, K.
Modellierung des thermischen Komforts in Kabinen-innenräumen
1. Auflage 2021
ISBN 978-3-948234-00-3

E.ON ERC Band 87
Wesseling, M.
Probabilistische Bewertung von Entrauchungsanlagen
1. Auflage 2021
ISBN 978-3-948234-01-0

E.ON ERC Band 88
Stoyanova, I.
Cooperative Energy Management and Cross-Domain Optimization for Electro-Thermal Devices at City-District and City-Level
1. Auflage 2021
ISBN 978-3-948234-02-7

E.ON ERC Band 89
Tran, T.
Advanced hierarchical control structure for Virtual Oscillator-based distributed generation in multi-bus microgrids under different grid dynamics and disturbances
1. Auflage 2021
ISBN 978-3-948234-03-4

E.ON ERC Band 90
Yang, Z.
On the Stability of Three-Phase Grid-Tied Photovoltaic Inverter Systems
1. Auflage 2021
ISBN 978-3-948234-04-1

E.ON ERC Band 91
Wang, T.
Fault Detection and Isolation in DC Distribution Grids
1. Auflage 2021
ISBN 978-3-948234-05-8

E.ON ERC Band 92
Beushausen, S.
A GaN-Based Switched-Mode Gate-Drive Unit for Medium-Voltage IGBTs
1. Auflage 2021
ISBN 978-3-948234-06-5

E.ON ERC Band 93
Schumacher, M.
Design and Assessment of Grid-driven Distributed Cogeneration
1. Auflage 2021
ISBN 978-3-948234-07-2

E.ON ERC Band 94
Joebges, P.
Distributed Real-Time Simulation of Modular Bidirectional DC-DC Converters for Control-Hardware-in-the-Loop
1. Auflage 2021
ISBN 978-3-948234-08-9

E.ON ERC Band 95
Averous, R.
Analysis of the Application of a Grid Emulator to Conduct Grid Compliance Tests for Multi-Megawatt Wind Turbines A Contribution towards Ground Testing of Wind Turbines
1. Auflage 2021
ISBN 978-3-948234-09-6

E.ON ERC Band 96
Virdag, A.
Design, Implementation and Analysis of DC Circuit-breaker for Low-Voltage DC Grids with Counter-current Injection Principle
1. Auflage 2021
ISBN 978-3-948234-10-2

E.ON ERC Band 97
Dähling, S.
Cloud-based Multi-Agent Systems for Flexibility Management in Future Distribution Grids
1. Auflage 2021
ISBN 978-3-948234-11-9

E.ON ERC Band 98
Qawasmi, A.
Fault Current Interruption Analysis and Development of a Power Semiconductor Switch for a Medium-Voltage DC Hybrid Circuit Breaker
1. Auflage 2021
ISBN 978-3-948234-12-6

E.ON ERC Band 99
Nolting, L.
Die Versorgungssicherheit mit Elektrizität im Kontext von Liberalisierung und Energiewende
1. Auflage 2021
ISBN 978-3-948234-13-3

E.ON ERC Band 100
Mathis, P.
Heat Transfer Enhancement in Natural Convective Channel Flows by Vortex Streets
1. Auflage 2022
ISBN 978-3-948234-14-0

E.ON ERC Band 101
Wolff, S.
Stated Preferences Concerning Private Passenger and Light-Duty Electric Vehicles in Germany
1. Auflage 2022
ISBN 978-3-948234-15-7

E.ON ERC Band 102
Hackbarth, A.
Private Households' Preferences for Alternative Fuel Vehicles in Germany – An Empirically Founded Analysis of Adoption Decisions, Willingness-to-Pay, and Policy Scenarios
1. Auflage 2022
ISBN 978-3-948234-16-4

E.ON ERC Band 103
Ge, L.
Performance Enhancement of Switched Reluctance Machines for High-speed Backup Generators: Design, Measurement and Control
1. Auflage 2022
ISBN 978-3-948234-17-1

E.ON ERC Band 104
Atasoy, T.
Strategic and Behavioral Responses of Consumers and Producers to Energy and Environmental Policies
1. Auflage 2022
ISBN 978-3-948234-18-8

E.ON ERC Band 105
Remmen, P.
Automated Calibration of Non-Residential Urban Building Energy Modeling
1. Auflage 2022
ISBN 978-3-948234-19-5

E.ON ERC Band 106
Schild, T.
Systematische Entwicklung strukturierter Steuerungs-algorithmen für die Gebäude- und Anlagentechnik
1. Auflage 2022
ISBN 978-3-948234-20-1

E.ON ERC Band 107
Sidik, Y.
Modeling, Control, and Dynamic Stability Analysis of Two-Stage DC Collector Grids in Offshore Wind Park Clusters
1. Auflage 2022
ISBN 978-3-948234-21-8

A resilient Distribution Grid Automation (DGA) system ensures safe and reliable operation of active distribution grids and its supply security . For resilient design of the DGA system its reliability against random component failures and the susceptibility to targeted attacks must be evaluated, so that appropriate component redundancies and cyber & physical security measures could be implemented. Hence, a Continuous Time Markov Chain (CTMC) based methodology, incorporating the Multi Domain Reliability Matrix (MDRM) is proposed for the reliability evaluation DGA systems that captures the cyber-physical interdependence. Furthermore, to evaluate the susceptibility of the DGA systems against cyber-physical attacks and study the impact of the security countermeasures, a CTMC based methodology incorporating a Multi- Criteria-Decision-Making methodology is presented. Finally, a Blockchain, and Smart contract based resilient design of DGA systems is proposed that ensures high availability of DGA functions even against random failures and targetted attacks on the DGA systems.

ISBN 978-3-948234-22-5

Thinking the Future
Zukunft denken