Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften
Department für Informatik

Resilience Quantification of Interdependent Power and ICT Systems using Operational State Classification

Von der Fakultät für Informatik, Wirtschafts- und Rechtswissenschaften der Carl von Ossietzky Universität Oldenburg zur Erlangung des Grades und Titels

Doktor der Ingenieurwissenschaften (Dr.-Ing.)

angenommene Dissertation von

Herrn Anand Narayan

geboren am 27. November 1989 in Coimbatore (Indien)

Gutachter:

Prof. Dr. Sebastian Lehnhoff,
Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften,
Carl von Ossietzky Universität Oldenburg.

Weitere Gutachter:

Prof. Dr.-Ing. Christian Rehtanz,
Institut für Energiesysteme, Energieeffizienz und Energiewirtschaft (ie3),
Technische Universität Dortmund.

Tag der Disputation: 28. Mai 2024

Abstract

Power systems increasingly rely on information and communication technologies (ICT), giving rise to cyber-physical energy systems (CPESs). On the one hand, ICT aids in the safe, secure and reliable operation of the power system by enabling or improving the grid services, e.g., state estimation, tap-changer control, and redispatch. On the other hand, the increased interdependence between the systems introduces new challenges. ICT integration has not only widened the disturbance landscape with new and unforeseen disturbances but also caused these disturbances to propagate further across system boundaries, resulting in multi-domain cascading and escalating disturbances. This is also expected to increase in the future with increasing digitalisation. The safety-critical nature of CPESs mandates designing resilient systems, which, in addition to known disturbances, are also capable of handling new and unforeseen ones.

A necessary precursor for designing resilient systems is to quantify their performance to plan measures to improve the performance in case of degradation. In this regard, operational state classification is a widely used tool to assess the performance of power systems in terms of state degradation (via disturbances) and recovery (via remedial actions). However, this operational state classification does not adequately capture the impact of ICT disturbances on the interconnected power system. Specifically, it does not represent the possible performance degradation of the ICT-enabled grid services. This limits its application to the comprehensive analysis of interdependent power and ICT systems, particularly regarding the propagation of disturbances and the quantification of resilience. This dissertation aims to address these issues via its two main contributions.

First, a joint operational state model for CPESs is developed, considering the structural and functional dependencies between power and ICT systems. Based on an investigation into the role of ICT in CPESs, an operational state model for ICT-enabled grid services is developed using finite state automata, which is then integrated with the existing power system operational states. Simulations on a CIGRE benchmark power grid augmented with an ICT system are used to show that the developed model can analyse the propagation of disturbances between power and ICT systems based on their operational states. This operational state model offers better trace-

ability for analysing cascading and escalating disturbances, which can then be used to study complex CPESs and implement measures to remedy such disturbances.

Second, this operational state model is used to develop a novel methodology and metrics to quantify the resilience of ICT-enabled grid services. The focus here is on these grid services, which significantly influence the operation of the interconnected power system. The operational states are used to capture the performance of a grid service, which is required for quantifying its resilience. The sequential Monte Carlo method is used to simulate the behaviour of ICT components and compute the operational state trajectory of the grid services. Metrics are then derived to quantify the individual phases of resilience, as well as the overall resilience, of the grid services. Simulations considering several ICT system designs are used to show that the developed methodology and metrics can capture the differences between the designs using the proposed metrics. This contribution can be used to analyse and compare different ICT technologies and architectures, which can then be used to improve the resilience of the ICT-enabled grid services. Due to the interdependencies, this could improve the resilience of the whole CPES.

Zusammenfassung

Elektrische Energieversorgungssysteme stützen sich zunehmend auf Informations- und Kommunikationstechnologien (IKT), was zu cyber-physischen Energiesystemen (CPESs) führt. Einerseits trägt die IKT zur sicheren und zuverlässigen Energieversorgung bei, indem sie Netzdienste, wie z.B. die Netzzustandsschätzung, Stufenschaltersteuerung und Redispatch, ermöglicht oder verbessert. Andererseits bringt die zunehmende Interdependenz zwischen den Systemen neue Herausforderungen mit sich. Die Integration von IKT hat nicht nur die Störungslandschaft um neue und unvorhergesehene Störungen erweitert, sondern auch dazu geführt, dass sich diese Störungen weiter über die Systemgrenzen hinweg ausbreiten. Es wird erwartet, dass daraus resultierende bereichsübergreifende Kaskadierung und Eskalation von Störungen in Zukunft mit der Digitalisierung noch zunehmen werden. Da CPESs als sicherheitskritische Systeme gelten, ist es erforderlich, diese Systeme resilient zu gestalten. Dadurch können neue und unvorhergesehene Störereignisse abgefangen werden, ohne dass diese Schaden am System verursachen oder der normale Betriebszustand kann in kurzer Zeit mit möglichst geringem Schaden wiederhergestellt werden.

Um resiliente Systeme konzipieren zu können, ist es zunächst wichtig, die Versorgungsleistung quantifizieren zu können, um darauf basierend im Falle einer Verschlechterung der Leistung entsprechende Maßnahmen zu planen. In diesem Zusammenhang ist die Klassifizierung der Betriebszustände ein weit verbreitetes Instrument zur Bewertung der Versorgungsleistung von Energiesystemen. Durch Störungen wechselt das System in einen schlechteren Zustand und durch Gegenmaßnahmen kann der Zustand verbessert werden. Diese Klassifizierung der Betriebszustände erfasst jedoch nicht in angemessener Weise die Auswirkungen von IKT-Störungen auf das Stromsystem. Insbesondere ist die mögliche Leistungsverschlechterung der IKT-gestützten Netzdienste bisher nicht darstellbar. Dadurch kann die Klassifizierung nicht für die umfassende Analyse von CPESs genutzt werden, insbesondere im Hinblick auf die Ausbreitung von Störungen zwischen Strom- und IKT System und die Quantifizierung der Resilienz. Um diese Probleme zu lösen, werden im Rahmen dieser Dissertation zwei Artefakte ausgearbeitet.

Im ersten Schritt wird ein gemeinsames Betriebszustandsmodell für CPESs entwickelt, das die strukturellen und funktionalen Abhängigkeiten zwischen Strom- und IKT-Systemen berücksichtigt. Die Betriebszustände von IKT-gestützten Netzdiensten sind dabei durch endliche Zustandsautomaten dargestellt, die dann in die bestehende Klassifizierung der Betriebszustände des Stromsystems integriert werden. Anhand von Simulationen in einem CIGRE-Benchmark-Stromsystem, das um ein IKT-System erweitert wurde, wird gezeigt, dass das entwickelte Modell die Ausbreitung von Störungen zwischen Strom- und IKT-Systemen auf der Grundlage ihrer Betriebszustände analysieren kann. Dieses Betriebszustandsmodell bietet eine bessere Nachvollziehbarkeit für die Analyse von kaskadierenden und eskalierenden Störungen, die wiederum zur Untersuchung komplexer CPESs und zur Umsetzung von Maßnahmen zur Behebung solcher Störungen verwendet werden kann.

Im nächsten Schritt wird dieses Betriebszustandsmodell verwendet, um eine neuartige Methodik und Messgrößen zur Quantifizierung der Resilienz von IKT-gestützten Netzdiensten zu entwickeln. Der Schwerpunkt liegt hier auf solchen Netzdiensten, die den Betrieb eines Verbundnetzes erheblich beeinflussen. Die Betriebszustände werden verwendet, um die Leistung eines Netzdienstes zu erfassen, die für die Quantifizierung der Resilienz dieses Netzdienstes erforderlich ist. Mit Hilfe eines sequentiellen Monte-Carlo-Verfahrens wird das Verhalten der IKT-Komponenten simuliert und die Entwicklung des Betriebszustands der Netzdienstleistungen über die Zeit berechnet. Anschließend werden Metriken abgeleitet, um die einzelnen Phasen der Resilienz sowie die Gesamtresilienz der Netzdienste zu quantifizieren. Anhand von Simulationen, die verschiedene IKT-Systemdesigns berücksichtigen, wird gezeigt, dass die entwickelte Methodik die Unterschiede zwischen den Systemdesigns mit Hilfe der vorgeschlagenen Metriken erfassen kann. Dieses Artefakt kann entsprechend genutzt werden, um verschiedene IKT-Technologien und -Architekturen zu analysieren und vergleichen. Dies kann zur Verbesserung der Ausfallsicherheit der IKT-gestützten Netzdienste eingesetzt werden und die Resilienz des gesamten CPES verbessern.

Acknowledgement

The PhD journey is long and arduous, filled with many triumphs, challenges, and lessons. It is something that cannot be travelled alone, and I am grateful to have individuals who have accompanied and guided me throughout this journey.

First and foremost, I would like to express my deepest gratitude to my supervisor, Prof. Dr. Sebastian Lehnhoff, who guided, encouraged and positively challenged me during this journey. Your open ear for my ideas and our many discussions have been deeply enlightening and have widened my horizons. I would also like to thank my co-supervisor, Prof. Dr.-Ing. Christian Rehtanz, for the consistently helpful feedback. I always came out more motivated after talking to you. Working with the two of you over these years has been an incredibly enriching experience. Additionally, I would like to thank Prof. Dr. Andreas Peter, Prof. Dr.-Ing. Astrid Nieße, and Dr.-Ing. Andreas Solsbach for being a part of my PhD examination committee and creating a wonderful atmosphere during the examination.

During my PhD, I have been a part of OFFIS - Institute for Informatics, where I got the opportunity to work on multiple research projects on various exciting topics. This gave me a broader perspective and helped me advance my PhD. My heartfelt thanks to my colleagues in the *Automation, Communication and Control (A2C)* group, *Resilient Monitoring and Control (ROC)* group and the OFFIS-Energy division for your continual support, discussions and feedback. All the coffee and the Flur chats with you helped me immensely in different aspects of my journey - from technical to organisational to motivational to venting frustration. Here, I would like to highlight Michael Brand, who, as my group manager, fellow PhD candidate, and friend, gave me the freedom and boost to learn and develop myself. I gained several new perspectives from you, especially regarding management and self-organisation. I would also like to thank Davood Babazadeh, who was pivotal in my decision to pursue this PhD journey and provided me with the initial support and direction. A special thanks to Marcel Klaes from TU Dortmund, my project partner in the PhD journey. I am happy to have shared this experience with you, and I learned a great deal from you, both personally and professionally.

This achievement would not have been possible without the love and support of my family. I am extremely grateful to my parents and all my family (both in India and

Germany) for your unwavering belief, support, and understanding throughout this journey. Your constant presence, blessings and prayers, even from afar, gave me joy, meaning and strength to strive for success. Last but not least, a larger-than-life thank you to my wife and colleague, Sanja, for accompanying me through this journey's highs and lows. You celebrated my success, often more than I did, kept me calm and encouraged me to look at the positives. This journey and success is as much yours as it is mine.

Funding: This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – project number 359778999 - as part of the priority program DFG SPP 1984 - Hybrid and Multimodal Energy Systems: System theory methods for the transformation and operation of complex networks.

Oldenburg, 14, June 2024

Anand Narayan

Contents

1 Introduction

The emphasis on combating climate change and reducing the emission of greenhouse gasses has led to the decarbonisation of the energy sector. This can be achieved by replacing electricity generation from conventional thermal power plants based on oil and coal with renewable energy sources like hydro, solar and wind [1]. Unlike the former, which are larger and typically centralised around fuel sources, the latter are relatively smaller and can be geographically distributed. The latter are, therefore, referred to as distributed energy resources (DERs). In contrast to the controllable and predictable electricity generation from thermal power plants, DERs are unpredictable due to their dependence on stochastic aspects such as weather [2]. Furthermore, the unbundling of electricity markets has increased the number of market participants. Traditional electricity consumers, especially in distribution grids, can now have DERs on their premises to produce and trade electricity. These factors have altered the power flows from unidirectional or top-down (i.e., from generation to transmission to distribution grids) to bidirectional and stochastic, increasing the complexity of the energy system [3].

Despite these complexities, the power system (PS) as a safety-critical infrastructure has to operate in a stable, safe, reliable and cost-effective manner to provide electricity to its customers. To do so, transmission and distribution system operators (TSOs and DSOs) use ancillary services, which include generation scheduling and dispatch, voltage and frequency control and restoration [4]. They enable the operators to adjust physical parameters such as active and reactive power, voltage, frequency and line loadings to prevent and mitigate the impact of disturbances or for economic optimisation. However, the rising complexity of PSs makes it challenging to reliably provide these ancillary services [5]. For example, the provision of frequency control requires guaranteed active power reserves, which is challenging when using DERs due to their unpredictability. This also increases the importance of DSOs in grid operation since most of the DERs are connected to the low voltage or medium voltage distribution grids [2]. Furthermore, active management and sophisticated coordination are required to fully use the potential of these DERs and maintain the required levels of performance of ancillary services [6].

1.1 Digitalisation in Power Systems

To address the aforementioned challenges, information and communication technology (ICT) is integrated into PSs, giving rise to cyber-physical energy systems (CPESs)[1] [3]. The term CPES originates from cyber-physical systems, where intelligent computer systems monitor and control a physical system [7]. ICT introduces enhanced monitoring, automation, communication and decision-making required to operate complex PSs. Specifically, the integration of ICT brings in the automation needed for the *grid services*, which aid in the better provision of ancillary services [8]. Examples of such grid services are state estimation, coordinated voltage control, redispatch and protection systems. While services like state estimation enable real-time monitoring of power grids, services like voltage control and redispatch involve controlling various grid equipment. Although these grid services have been a part of traditional PSs, the introduction of ICT systems has enhanced their monitoring, communication and control capabilities [8]. A typical ICT system comprises hardware and software of field devices such as sensors and controllers, communication network devices such as routers, antennas and links, and servers for computation, which are typically located in a control room [9]. Examples of sensors and controllers include smart meters, remote terminal units (RTUs) and intelligent electronic devices (IEDs). The grid services are then enabled by different combinations of these ICT components.

A CPES is characterised by strong interdependencies between power and ICT systems, which is expected to increase in the future as more grid services are integrated into the system [10]. The ICT system depends on the PS for electrical power supply and, in return, enables the grid services which aid in PS operation [11]. However, this interdependence between the systems further increases the overall complexity, leading to new threats and vulnerabilities that can harm the CPES. This can be better understood by analysing the role of ICT in historical blackouts. In the remainder of this dissertation, the term grid refers to the power system, while the term network refers to the ICT system.

1.2 Role of ICT in Historical Blackouts

This subsection presents an overview of historical blackouts that have either been caused directly or indirectly by disturbances in ICT systems.

[1] In the scope of this dissertation, a CPES is limited to interconnected power and ICT systems. Other domains, such as mobility and gas, are beyond its scope.

2003 North America: This blackout affected around 55 million people with an estimated $6 billion in damages [12]. The first disturbance was the tripping of a generator at a TSO because of an exciter malfunction. This was followed by a transmission line trip due to tree contact, which increased the loading on other transmission lines. During this time, the software of the state estimation service, a grid service that enables PS monitoring, at the system operator failed due to a software bug. This prevented the operator from having correct awareness of the grid. The operators were unable to predict the possible overloading of the lines. This was aggravated by a failure of the alarm system, the role of which was to warn the operator in case of critical situations. Following this, another transmission line failed due to overload, which triggered a voltage collapse, eventually leading to the blackout.

2005 Switzerland: On June 22, 2005, the Swiss railway network failed due to a PS collapse [13]. All their 1,500 trains stopped running, affecting around 200,000 people. Two of the three major power lines were out of service for maintenance. During this time, electricity trading continued due to improper coordination, causing the third line to trip due to overload. The control room was then flooded with around 18,000 error messages from the protection devices within the next hour, causing congestion in the communication network and servers. As a result, these messages were not processed in time. 3,400 of these messages were important, and four among them, when received on time, could have prevented the blackout.

2013 Austria: In May 2013, a large number of messages were circulated between controllers, causing congestion in the communication network. This hindered the transfer of control commands from the central control room to field controllers, almost resulting in a blackout [13]. The reason was the use of an unapproved version of IEC 90870-5-101 and -104 protocols by a system operator. As a result, an erroneous acknowledgement was broadcasted to numerous controllers, which was then further re-broadcasted among themselves. Several power plants and substations had to be switched to manual operation to ease network traffic, which was then remedied by the coordinated separation of communication lines between the communication network operators. A firmware update for the protocol was then carried out at the operator using the unapproved protocol version.

2015 and 2017 Ukraine: In December 2015, a cyber-attack in Ukraine caused a blackout affecting around 225,000 customers for several hours [14]. The control room was hacked using phishing emails. The hackers then remotely switched off substations, causing major parts of the grid to lose power supply. The ICT-enabled grid services were mainly targeted to prevent the operator from monitoring and restoring the grid. The attackers could inject false data into the ICT system and manipulate measurements as they knew the power system topology as well as certain critical parameters. This was followed up by another cyber-attack in June 2017, which, in addition to the power grid, impacted other domains such as banks, ministries, telecommunication services and railways [15].

These blackouts show that modern CPESs, in addition to PS disturbances, face a wide range of new disturbances from the ICT system. The 2003 North American blackout showed that software failures could result in insufficient awareness, preventing the operators from remedying other PS disturbances [16]. The Ukraine blackouts showed that PSs could be harmed by a cyber-attack on the grid services. It can, therefore, be concluded that the ICT system has a strong influence on the interconnected PS, as ICT disturbances can now propagate beyond its boundaries and impact the overall CPES. This makes it necessary to model and analyse the ICT system, grid services, and the interdependencies for planning and operating CPESs, especially because some of these blackouts could have been prevented with the timely detection and remedy of the underlying ICT disturbance.

1.3 Need for a Resilient System

The analysis of past blackouts shows that modern CPESs face a newer and broader disturbance landscape. As safety-critical systems, they should be designed to survive, among others, power and ICT disturbances. Traditional systems are designed to withstand (i.e., be robust against) disturbances with a high impact and a high occurrence probability [17]. This is achieved via measures such as N-1 redundancy, equipment derating (i.e., operating a piece of equipment at less than its rated maximum capacity) and ensuring more generation reserves [18]. However, disturbances in CPESs have complex modes of propagation between power and ICT systems because of their interdependencies [10]. Additionally, owing to the recency of such systems, operators have fewer experiences in dealing with such novel disturbances [17]. Consequentially, there is a lack of statistical data about them. Furthermore, certain disturbances such as cyber-attacks and software bugs, which were once rare or had a negligible impact, are now prevalent and can be severe [5, 19]. As a result, ensuring the robustness of a CPES against the full range of disturbances is infeasible and costly. In this regard, resilience is an emerging concept [20]. In contrast to traditional robust systems designed considering only known and highly probable disturbances, a resilient system should be able to absorb (without failing) and then recover from new, unforeseen and low probable disturbances as well [21]. Since disturbances in a system are inevitable due to external factors, resilience is not about preventing them but managing how the system behaves during a disturbance and the subsequent recovery [22].

The concept of resilience can be depicted using the *bathtub curve* in Fig. 1.1. This figure shows an exemplary performance over time of a resilient and a non-resilient system. When faced with a disturbance, a non-resilient system fails, i.e., performance drops nearly to zero. On the contrary, a resilient system stabilizes itself at a lower level of performance and returns to normal performance without completely failing. Resilience, in principle, deals with the performance of a system over time [21]. In this regard, the PS operational state classification proposed by the European Network of Transmission System Operators for Electricity (ENTSO-E) is widely used by system operators to determine the current performance of a PS [23]. Based on certain parameters, the performance of a PS can be classified into one of five operational states - Normal, Alert, Emergency, Blackout and Restoration. These states give an overview of the current PS performance, and the sequence of states over time is referred to as the *operational state trajectory*. Disturbances can cause transitions from a better to a worse state, referred to as state degradation (e.g., Normal to Alert, Emergency to Blackout). Depending on which state the PS is in, suitable remedial actions using grid services can be applied to improve the state. This is called state recovery (e.g., Alert to Normal). A detailed explanation of the ENTSO-E state classification is presented in [23]. A drawback of these operational states is that they do not adequately capture the impact of ICT disturbances on the interconnected PS. Specifically, the impact of performance degradation of the ICT-enabled grid services on the state of PS is not considered. This limits its applicability in analysing the behaviour of CPESs.

1.4 Challenges and Research Gap

The limitation of the PS operational states can be better understood by investigating the sequence of disturbances and the resulting operational state trajectory of the aforementioned 2003 North American blackout. Fig. 1.2 shows the corresponding trajectory with the operational states representing the PS performance on the y-axis with time and disturbances on the x-axis. PS disturbances are denoted using red arrows, and ICT disturbances using red crosses. The solid black line shows the state trajectory, the details of which can be found in [12]. Since the generator trip did not cause a state degradation, it can be said that the PS absorbs (or is robust to) this disturbance. Contrarily, the next three PS disturbances, i.e., *DP&L* line trip,

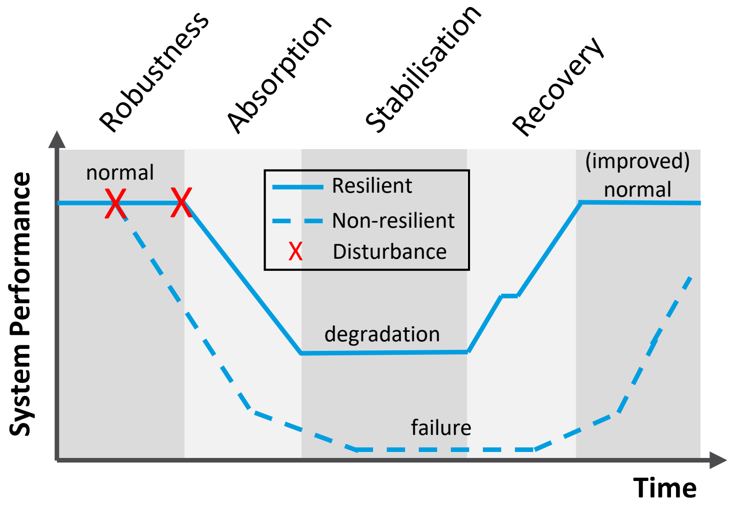


Fig. 1.1: Bathtub curve showing behaviours of a resilient and a non-resilient system.

chamberline line trip and the resulting voltage collapse, cause degradation to Alert, Emergency and Blackout, respectively. From the figure, it is evident that while the operational states capture the impact of PS disturbances, they cannot capture the impact of ICT disturbances. In particular, the failures of the state estimation service and the alarm system cannot be represented using these operational states. As a result, the impact of ICT disturbances is hidden from an operator, who uses these states to monitor the system. This emphasises the need for a joint operational state classification for CPESs, which can track not only the performance of the PS but also the interconnected ICT system as well as the interdependencies between the systems. Specifically, the performance of the ICT-enabled grid services should also be tracked as they are used to monitor and control the underlying PS. As demonstrated by the blackouts in Sec. 1.2, disturbances in ICT systems impact the performance of the grid services, which then impacts the PS performance. Although operational states of CPESs have been a focus in literature, they only partially consider the interdependencies [24, 25, 26], do not consider the ICT-enabled grid services at all [27, 28] or are limited to certain grid services [29, 30].

As concluded by [12, 16], the North American blackout could have been prevented by timely detection of the ICT disturbances. Remedial actions using suitable grid services could have been deployed to recover the operational state trajectory, as indicated by the green arrows and dotted black lines in Fig. 1.2. It can be seen that the recovery trajectory in Fig. 1.2 resembles the trajectory of a resilient system depicted by the bathtub curve in Fig. 1.1. This indicates that the operational state

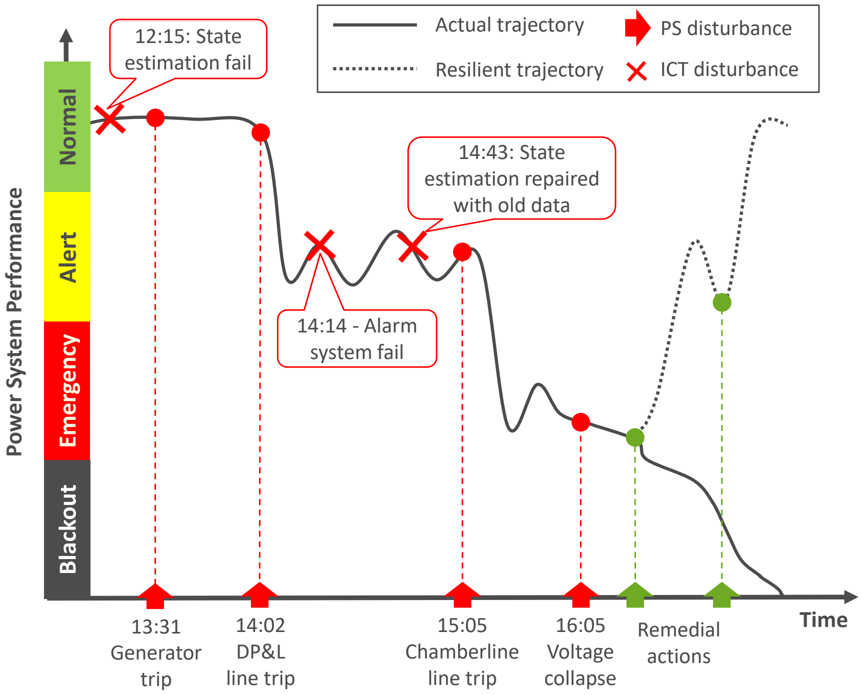


Fig. 1.2: PS operational state trajectory during the 2003 North American blackout [12].

trajectory of a system can be used to assess its resilience, especially because the operational states capture the system's performance. As mentioned in Sec. 1.3, modern CPESs should be designed to be resilient since they have new and complex modes of disturbance propagation, particularly via the ICT-enabled grid services (cf. Sec. 1.3). This requires a methodology and metrics to assess their resilience. In this regard, existing research does not focus specifically on the resilience of ICT-enabled grid services [31, 32, 33], the failure of which, as shown in Fig. 1.2, can impact the PS and, consequentially, the overall CPES.

1.5 Research Questions and Objectives

Based on the research gap presented in the previous section, this section describes the two research questions of this dissertation, along with the requirements of their corresponding artefacts. The first research question is as follows:

RQ1: *How to model the operational state trajectory of a CPES, considering the interdependencies between power and ICT systems?*

This research question aims to develop a formal joint operational state model for CPESs considering the constituting power and ICT systems. Following an investigation of the interdependencies between the two systems, a novel operational state model for the ICT system will be developed and formalised with a focus on the ICT-enabled grid services. This is because these grid services have a direct impact on the operation of the interconnected PS and are, therefore, an important aspect of the interdependencies. For the PS states, the aforementioned and established PS operational states by ENTSO-E are used. Although these states are well described in the literature [23], they are formalised for the purpose of simulation studies in this dissertation. The combination of these models yields a formal *joint operational state model for CPESs*, which is the artefact of RQ1. This model should be able to analyse the propagation of multi-domain, i.e., PS and ICT, disturbances in terms of the operational state trajectory of the PS and the ICT-enabled grid services. In the scope of this dissertation, the developed model should satisfy the following functional requirements.

FR1: The model should consider the interdependencies between power and ICT systems. Specifically, the two types of interdependencies, namely, structural (via physical connection) and functional (via logical connection) [10], should be modelled.

FR2: The model should be able to analyse degradation (caused by disturbances) and recovery (caused by remedial actions) using operational state trajectory.

FR3: The model should be able to analyse the two types of disturbance propagation, namely, cascading (one disturbance causing another) and escalating (one disturbance exacerbating the impact of another) [10].

The quantification and assessment of a system's resilience, however, requires the analysis of its behaviour (or state trajectory) considering a wide range of disturbances. This not only requires certain modifications to the model from RQ1 but also requires suitable metrics to quantify resilience. Based on this, the second research question can be defined.

RQ2: *How to quantify and assess the resilience of the ICT system in CPESs with a focus on the grid services?*

The focus here is on the resilience of the ICT-enabled grid services as they are an essential aspect of the dependence of the PS on the ICT system [34]. Following an investigation of the phases of resilience, metrics will be developed to quantify the resilience and the performance of the grid services based on their corresponding state trajectory. Then, the operational state model for the ICT-enabled grid services from RQ1 will be extended to consider a wide range of input disturbances based on which the developed metrics will be calculated. This *methodology and metrics for quantifying the resilience of ICT-enabled grid services* is the artefact of RQ2, which can be used to analyse and compare different ICT design options based on the resilience of the grid services. This contributes towards the design of resilient CPESs. In the scope of this dissertation, this artefact should satisfy the following functional requirements:

FR4: The methodology and metrics should be able to quantify the performance and resilience of ICT-enabled grid services in CPESs.

FR5: The methodology and metrics should be able to measure the contribution of individual phases on the overall resilience of grid services.

The research questions are deemed to be answered if the resulting artefacts satisfy all the functional requirements. To evaluate the practical relevance and future-proof nature of the developed artefacts, the following four non-functional requirements are identified. While the functional requirements are the main objectives of the artefacts, the non-functional requirements evaluate the boundaries of the artefacts in achieving these objectives. Note that the first two non-functional requirements are applicable for the joint operational state model (artefact of RQ1), and the last two are for methodology and metrics to assess the resilience of ICT-enabled grid services (artefact of RQ2).

NFR1: *Adaptability* evaluates the ability of the developed model to analyse different types of PS and ICT disturbances. This is relevant because modern CPESs face a wide range of power and ICT disturbances, which, as discussed in Sec. 1.2, can propagate across the boundaries of the respective system.

NFR2: *Extensibility* evaluates the ability of the developed model to include additional grid services. This is relevant because, due to increased ICT penetration, future PSs will be more reliant on ICT-enabled grid services for their operation, which can then result in the inclusion of more grid services.

NFR3: *Scalability* evaluates the ability of the developed methodology to consider ICT systems of various sizes and is relevant due to the large-scale nature of CPESs.

NFR4: *Comparability* evaluates the ability of the developed methodology and metrics to compare different ICT system designs based on the resilience of the grid services. This requirement is relevant as several options exist to design ICT systems for CPES, mainly due to the rapid development of ICT technologies.

1.6 Methodology and Structure of this Dissertation

To systematically answer the research questions, this dissertation follows the design science research process (DSRP) [35]. It is a methodology suited for the design and development of research artefacts and has six phases: (i) motivation and problem identification, (ii) defining objectives of the solution, (iii) design and development, (iv) demonstration (v) evaluation and (vi) communication. The phases build upon one another, and phases ii to vi can be iterated for improving or modifying the artefact based on the outcome of other phases. Fig. 1.3 shows the structure of this dissertation following the DSRP phases, which are shown in blue bubbles. The arrows represent the linkage between the chapters.

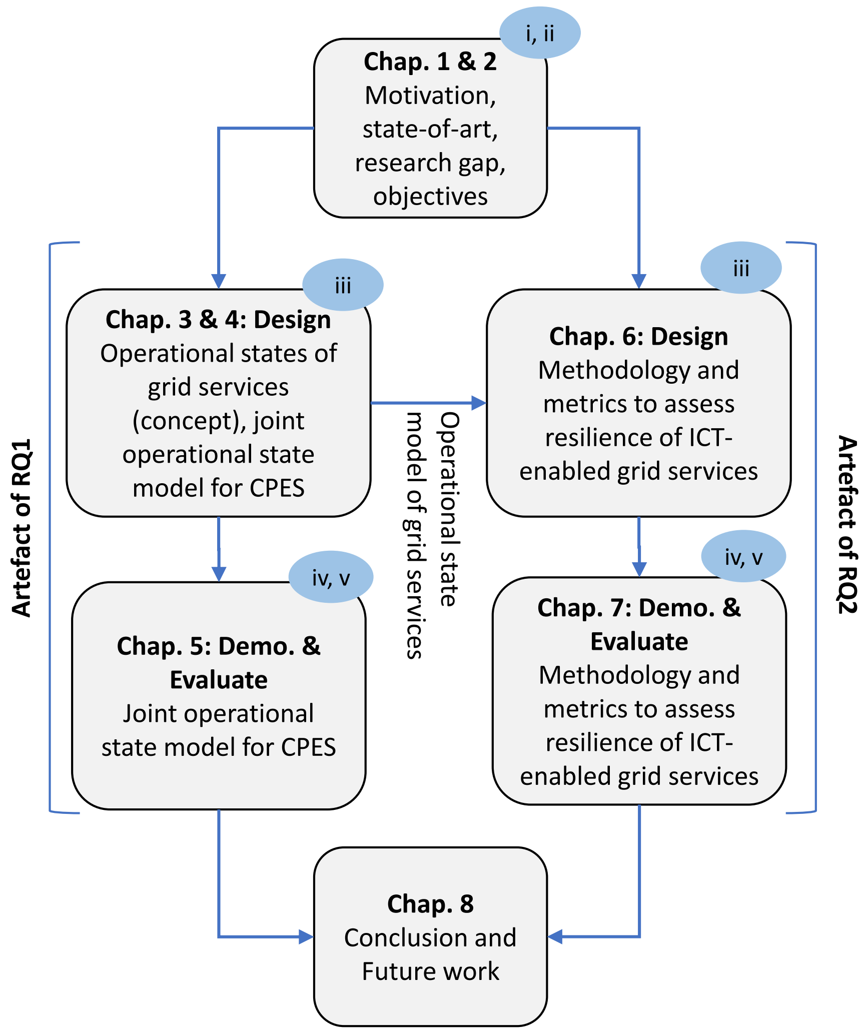


Fig. 1.3: Structure of the dissertation based on DSRP. The phases are shown in the blue circles [35].

Chapters 1 (the current chapter) and 2 correspond to phases i and ii. This chapter motivates the underlying problem and identifies the research gap and objectives of the two artefacts. Chapter 2 provides an in-depth analysis of the relevant state of the art, where the fundamental concepts used in this dissertation are also discussed. Specifically, Secs. 2.6 and 2.7.2 discuss the state of the art corresponding to RQ1 and RQ2, respectively. These sections also provide further reasoning on the choice of the objectives in Sec.1.5.

Chapters 3 and 4 correspond to the DSRP phase iii. Chapter 3 conceptualises the operational states of the ICT-enabled grid services, a core aspect of this dissertation. It also presents case studies on the operational states of three grid services, namely, state estimation, on-load tap changer-based voltage control and redispatch of DERs. Using this concept, Chapter 4 presents the formal description of CPES and then develops the operational state model of the ICT-enabled grid services. This model is then further used to develop the joint operational state model for CPES, which is the artefact of RQ1.

Chapter 5 corresponds to DSRP phases iv and v, where the developed artefact of RQ1 from Chapter 4 is demonstrated and evaluated. This is done using simulations with power and ICT system simulators. The goal is to demonstrate the ability of the developed model to analyse the propagation of multi-domain disturbances between the two systems using the operational state trajectory. These simulations are also used to validate the developed model. The evaluation of the developed model (artefact of RQ1) is also summarised in Chapter 5. Here, the identified functional and non-functional requirements are qualitatively evaluated using simulation results from the demonstration.

Since this dissertation has two artefacts corresponding to the two research questions, the DSRP phases iii, vi and v are performed twice (once for each artefact). This can be seen in Fig. 1.3. Chapter 6 also corresponds to phase iii, which developed the methodology and metrics to assess the resilience of ICT-enabled grid services. This chapter builds on the concept and the operational state model from Chapters 3 and 4, representing the linkage between the artefacts of this dissertation. The result of this chapter is the artefact of RQ2.

Chapter 7 also corresponds to DSRP phases iv and v, where the developed artefact of RQ2 from Chapter 6 is demonstrated and evaluated. This is done using simulations considering only the ICT system. The goal is to demonstrate the ability of the methodology and metrics to quantify the resilience (and its constituting phases) of ICT-enabled grid services considering different ICT system designs. This chapter also quantitatively evaluates the artefact of RQ2 based on the identified functional and non-functional requirements. Here, ICT systems of different sizes and designs are used.

Chapter 8 finally summarises the dissertation and identifies several future research directions.

Phase vi of the DSRP is the dissemination of the results obtained in the above phases and is, therefore, not shown in Fig. 1.3. Since this dissertation lies in the intersection of electrical power systems and computer science, relevant conferences and journals from both disciplines were targeted. A detailed list of publications associated with this dissertation can be found at the end of this dissertation under *Own Publications*. The feedback from these publications was incorporated into the artefacts by suitably iterating over the relevant DSRP phases. While [36] and [37] motivate the research questions, [9] and [38] focus on the operational states of the ICT-enabled grid services (part of RQ1 artefact). The joint operational state model for CPESs (artefact of RQ1) was then conceptualised, designed and demonstrated in [34], [39] and [11], respectively; whereas the method and metrics for resilience assessment (artefact of RQ2) were conceptualised, designed and demonstrated in [40]. Initial ideas for some of the future research of this dissertation are then discussed in Refs. [41, 8, 42]. Furthermore, this dissertation serves as a comprehensive publication for both artefacts.

Collaborative work: Certain parts of the conceptualisation, development and demonstration of the joint operational state model for CPESs (artefact of RQ1) was done in collaboration with Marcel Klaes of the ie3 Institute at the TU Dortmund University. His focus was primarily on the power system aspects, the integration of the ENTSO-E operational states and operational decisions based on optimal power flow (Secs. 4.4.4 and 4.4.5). These are further elaborated in his dissertation, where he also analyses the dynamic aspects of the power system.

2 Fundamentals and State of the Art

This chapter first presents the fundamentals and the definitions used in this dissertation. This is followed by the state of the art pertaining to the two research questions, based on which the concrete objectives for the artefacts in Sec. 1.5 were identified.

2.1 Cyber-Physical Energy Systems (CPESs)

As mentioned in Sec. 1.1, ICT is integrated to monitor and control modern-day PSs with increased renewables, giving rise to CPESs. An ICT system comprises hardware and software components to enable advanced monitoring and control, fast data transfer and processing, and real-time decision-making. PS operation relies on the grid services, which in turn rely on different combinations of the aforementioned ICT components. CPESs typically have a network of computer systems interacting with each other and the PS via physical inputs and outputs. Fig. 2.1 shows a CPES, where the power and ICT systems are represented as layers. The solid lines represent the interaction among the components within a layer, and the arrows show the information passed across the layers. The ICT system consists of three layers, namely, operational technology, information technology and decision-making. The layers of a CPES are explained in the following sections.

2.1.1 Power System

This layer comprises physical equipment for generating, transmitting, and distributing power to the end consumers. A typical PS geographically spans large areas and includes equipment such as power generators, power lines, transformers, switches, circuit breakers, capacitor banks and loads. An electrical substation is a collection of PS equipment where voltage is transformed from high to low or vice-versa for transmission, distribution, transformation and switching. Power flows through several substations at different voltage levels between the generating stations and the consumers. The role of PS is to reliably supply power to its consumers whilst

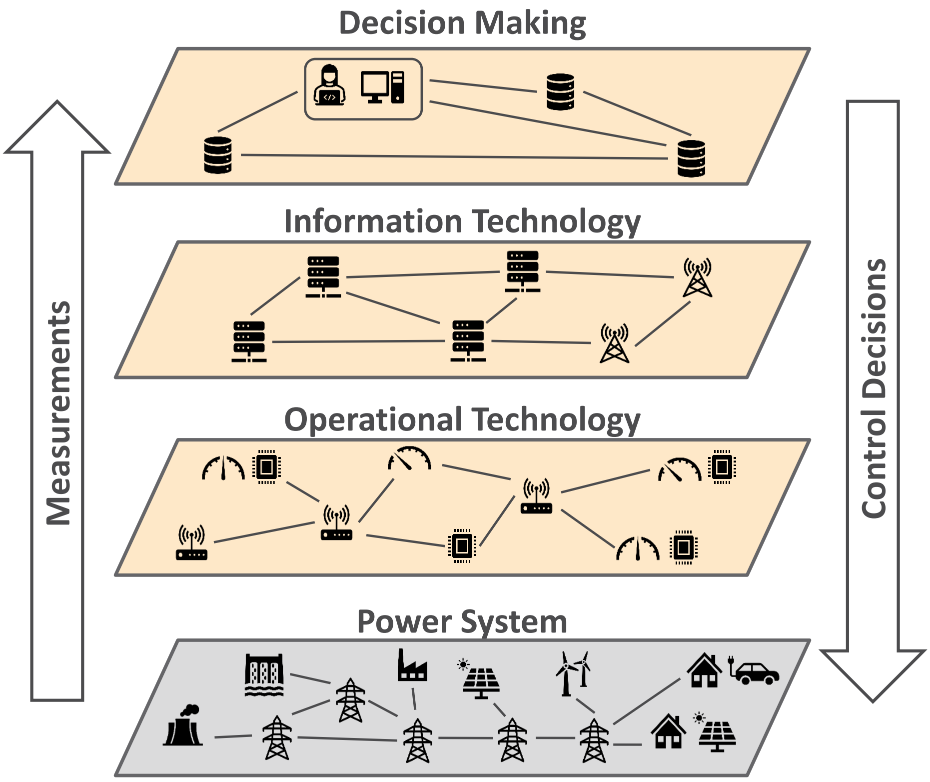


Fig. 2.1: Overview of a cyber-physical energy system.

ensuring the safety of its equipment and operating personnel. This requires monitoring and control of the PS and is provided by the ICT system. Furthermore, due to the penetration of DERs, especially at the medium and the low voltage levels, traditional consumers can now produce and exchange power, bringing in the need for monitoring and control (and consequentially ICT) on these voltage levels as well. Further information on PS equipment and its operation can be found in [43] and [44].

2.1.2 Operational Technology

The operational technology (OT) layer is a part of the ICT system and consists of devices for gathering measurements and performing both automatic and manual control (or actuation) on the PS. In conventional power grids, OT refers to the devices in the supervisory control and data acquisition (SCADA) environment. This layer is typically located at the substations and consumer premises. OT devices can have different functionalities; for example, phasor measurement units (PMUs) can only measure parameters. In contrast, intelligent electronic devices (IEDs), programmable logic controllers and smart meters can measure parameters as well as control PS equipment. The type of OT devices also varies depending on the type of substation. While PMUs are common in the transmission substations (extra-high and high voltage levels), they are yet to be prevalent in the distribution substations (medium voltage level) [45]. Examples of measurements from sensors are voltage, current, power injections and switch state, while examples of control actions are changing the tap position of a transformer and the power output of a generator. These devices use the communication network for exchanging measurement and control data. Based on [46], OT is defined as:

Definition 1 *Operational technology (OT) consists of programmable devices with hardware and software that either interact directly with the physical environment or manage devices that interact with the physical environment. OT devices can detect or cause a change through monitoring and/or make suitable decisions to control the physical equipment and assets.*

2.1.3 Information Technology

Information technology (IT) refers to the communication network comprising devices such as routers, antennas, fibre optic cables and hubs. This layer handles the transfer of data between the OT devices, as well as between the OT layer and the decision-making layer. The IT network within a substation is referred to as a field area network (FAN), and the IT network between substations or between substations (or between substations and control room) is referred to as a wide area network (WAN). Considering the increasing ICT at the low voltage level, consumer premises (e.g., households and office buildings) can also have a communication network called a building area network (BAN). Since FAN and BAN are typically within premises, i.e., substations and buildings, respectively, they can be referred to as local area networks (LANs). Based on [47], IT is defined as:

Definition 2 *Information technology (IT) encompasses all technologies for information transfer, including software, hardware, communications technologies and related services. In general, IT excludes embedded technologies that generate data on their own but focus on transferring the data generated from the OT and the decision-making layers.*

Fig. 2.2 shows the differentiation of WAN, FAN and BAN based on the data rate and coverage range requirements [48]. It can be seen that the data rate requirement increases along with the coverage range. This can be attributed to the requirements of various grid services that use the communication network. Services that use BANs typically are home/building automation and energy management, which require exchanging measurements between the OT devices within a consumer premise. They require only a low data rate (up to 100kbps) with a short coverage distance (up to 100m). BANs can be connected to FANs using a smart meter gateway. Services on FAN include smart metering and demand response, where data is exchanged between many OT devices within a substation as well as between BANs. Compared to BAN, the grid services that use FANs require a higher data rate (10kbps - 10Mbps) and larger coverage disturbance (up to 10km). Note that FANs can also connect substations in close proximity. Grid services that use WAN include wide-area monitoring protection and control, state estimation and islanding, which require exchanging large amounts of data at a much higher data rate (10 Mbps–1 Gbps). These services are crucial for the stability of the PS as a whole. WAN facilitate data exchange among substations or between substations and the control centre. Since PSs are spread over large distances, WANs also have an extended coverage range (up to 100 km). The IT requirements of the grid services are referred to as quality of service requirements [8]. In addition to data rate and coverage distance, grid services may also have other requirements, such as latency and packet loss [49]. Fig. 2.2 also shows the typical technologies used in BAN, FAN and WAN. Here, a distinction can be made between wired and wireless technologies. Wired technologies are more secure and can offer higher speeds but have a higher installation cost and effort. They are prominent in the power transmission system, where the TSOs privately own and operate the IT network. Such networks are dedicated only to the PS. Contrarily, wireless technologies have lower installation costs but are less secure and comparatively offer lower speeds. They are prominent in the distribution grids (medium and low voltage levels), where the DSOs typically use shared public infrastructure such as cellular. Although using such networks is cheaper and has less overhead for the grid operator, due to their shared nature, they may not always guarantee the resources required for running all the grid services in it [49]. Details on these communication technologies can be found in [48, 50].

2.1.4 Decision-making

This layer processes the data received from the IT layer to derive suitable control actions. Depending on the system architecture, the decision-making can occur at servers in control rooms or at the OT devices themselves. Transmission grids typically have a control room, where data from the OT layers are gathered for decision-making.

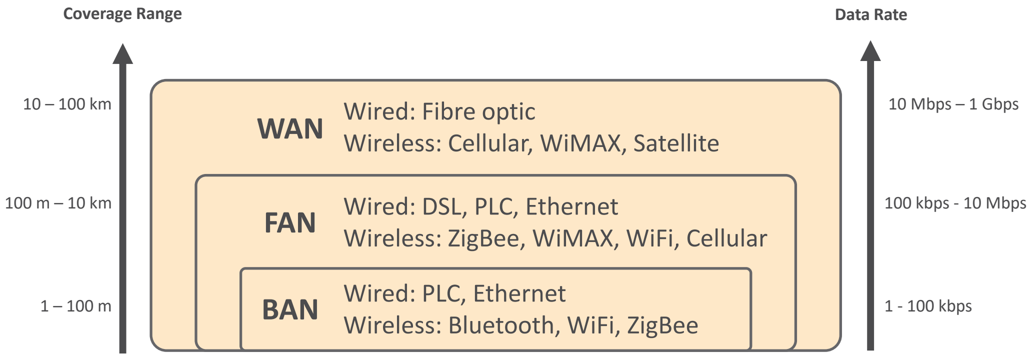


Fig. 2.2: Data rate and coverage distance for IT technologies and network hierarchies.

Contrarily, decision-making in substations occurs at the OT devices, in which case, communication between the OT devices would be required. These decisions can be, for instance, via devices such as IEDs and programmable logic controllers having industrial computer systems that process the received data, resulting in control actions on the PS component connected directly or indirectly to them [3]. These actions could be broadly classified into three categories [43]:

- **Preventive** actions are taken preemptively before a disturbance to prevent the system from entering an insecure (or undesired) state, possibly restoring it to a secure state. Examples of such actions are activating non-spinning reserves or switching on compensators.
- **Curative** actions are taken as a reaction to a disturbance to mitigate its impact and, eventually, restore the system to a secure state. These actions are taken when the system is already in an insecure state. Examples include fault isolation, tripping of generators and, in extreme cases, load shedding and islanding.
- **Economic** actions aim to decrease the operating cost of the system. They are taken only when the system is secure and there is no disturbance prognosis. Examples of such actions include using economic dispatch of generators and peak shaving.

Furthermore, due to the strong coupling between power and ICT systems in CPESs, the decision-making could also be aimed at ICT problems. Examples include rerouting traffic in the IT network in case of congestion, restarting a server in case of a crash and reallocating services in case of a hardware failure [42]. However, ICT decision-making would require its own tools and devices to monitor and control the ICT system. Examples of such tools are software-defined networks and network function virtualisation [8]. The ICT decisions could also be categorised into preventive and curative actions. From the ICT perspective, economic actions are done during system planning and not during operation [51].

In a nutshell, the ICT system has four functions, namely, measuring, actuation, data transfer and processing (computation). The sensors in the OT layer measure physical parameters (e.g., voltage, temperature, active power) as well as the status of PS components (e.g., switch state, transformer tap position), which are then transferred via the communication (IT) network to the decision-making layer. Here, the received data, i.e., measurements and statuses, are processed, and suitable control actions are derived. These actions are then transferred back via the communication network to the OT layer, where controllers (or actuators) make the required modifications to the PS equipment. Note that certain OT devices are also capable of making decisions, in which case, communication between the devices in the OT layer would be required.

2.2 ICT-enabled Grid Services

This section presents an overview of ICT-enabled grid services in CPESs. Its definition and types are first discussed, followed by their typical architectures.

2.2.1 Defintion and Types

The layers of the ICT system in CPES enable different grid services, which aid in grid operation. In this dissertation, they are defined as:

Definition 3 *ICT-enabled grid services comprise a combination of hardware and software components of the ICT system that support the operation of a CPES. This includes services for monitoring and data processing, economic optimisation, as well as preventive and curative actions against potential emergency situations.*

Based on the ENTSO-E system operation guideliens [52], the grid services, depending on their functionality, can be broadly classified into two categories [34]:

High-level services comprise grid services that aid monitoring PSs by gathering measurements (e.g., voltage, current) and provide situational awareness[1] to the

[1] Situational awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future [16].

grid operator. They correspond to the *tools and facilities* from [53]. Examples include state estimation, communication between the control room of other TSOs and operational security analysis (e.g., power flow and contingency analysis).

Remedial actions are the countermeasures that can restore PSs when they are in an undesirable state and prevent them from entering that state in the first place. As mentioned in Sec. 2.1.4, the former is called curative actions, while the latter is preventive actions. These actions actuate PS equipment based on the monitoring information from the high-level services. Examples include changing transformer taps, switching topology and changing setpoints of DERs. A non-exhaustive list of remedial actions can be found in [54].

Remedial actions are essential only when the grid is in an undesired state or when there is a prognosis of an undesired state. In contrast, as evident from the 2003 North American blackout (cf. Sec. 1.2), high-level services are always essential as suitable remedial actions can only be deployed with the correct knowledge of the underlying problem in the PS. Furthermore, one high-level service can impact multiple remedial actions. For instance, all remedial actions that are deployed from the control room depend on state estimation [55].

2.2.2 Architectures

The design of ICT systems in CPESs consists of designing the grid services considering their quality of service requirements. Due to the complex nature of PS operation, these grid services share and combine several ICT components on different geographic levels, time scales and quality of services [49]. For example, an IED can provide measurements from a PS component for both state estimation and demand response at different data rates [38]. In this regard, the architecture of the grid services influences the flow of data between the OT devices and the location of decision making. Although several definitions exist for system architectures for several disciplines, such as control theory, software development and communication systems, this dissertation follows [56], where the following five architectures of ICT-enabled grid services are identified. These architectures are illustrated using a medium voltage power grid in Figs. 2.3 and 2.4. The dashed orange lines represent location area communication.

Local: This is limited to the control of one PS equipment and is typically realised using a single OT device, which is located at the controlled equipment. The OT device measures the required parameters locally (or directly), processes them and sends control actions back to the equipment. In Fig. 2.3, this is illustrated by OT5, which controls the transformer T3. As there is no external communication, this architecture does not use the IT layer. Simple grid services, like changing transformer taps based on local voltage or opening a circuit breaker based on the local current measurements, can be realised using this architecture.

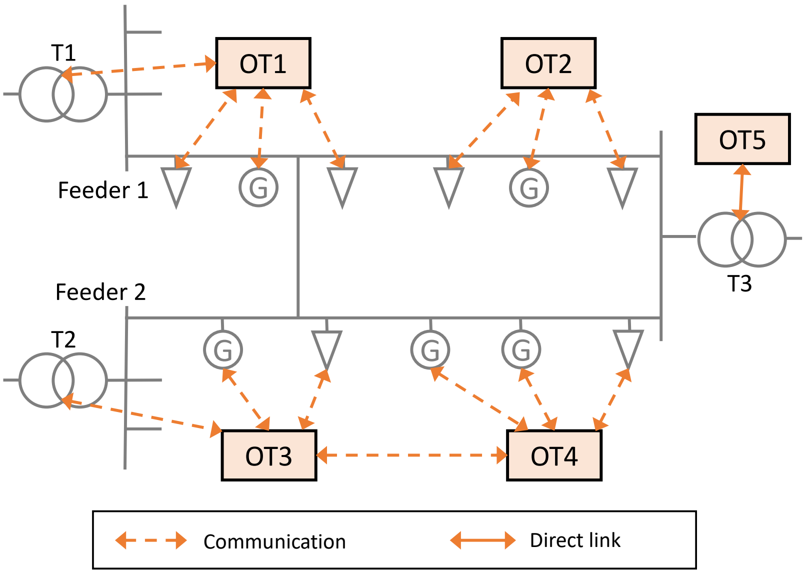


Fig. 2.3: Architectures of ICT-enabled drid services - local (OT5), decentral (OT1, OT2) and distributed (OT3 and OT4).

Central: Here, a central entity controls all PS equipment. In this architecture, data is transmitted via the IT network to a central entity, where the received data is processed, and decisions are made either automatically by software programs or manually by humans. In Fig. 2.4, this is illustrated by OT4, which controls all the PS equipment in Feeder 2. Grid services such as topology management and contingency analysis that require the overview of the whole grid belong to this category [44].

Decentral: In this architecture, groups of PS equipment are controlled using one or more OT devices. Communication via the IT layer is present within the group but not across the groups. This implies that there is no dynamic (i.e., during operation) coordination between the decentral groups. In Fig. 2.3, OT1 and OT2 each control three PS equipment of Feeder 1 in a decentral manner. The authors in [57] present a decentral voltage control with the PS partitioned into groups, each with its own controller that gathers measurements from and controls the PS equipment in that group. Here, the coordination between the groups is done statically (i.e., during the design phase) using PV and VQ curves.

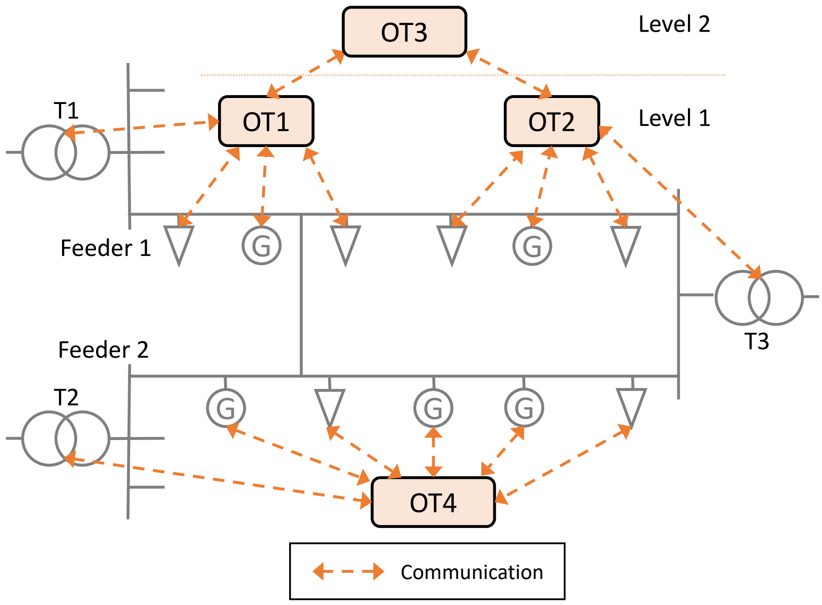


Fig. 2.4: Architectures of ICT-enabled grid services - central (OT3) and hierarchical (OT1 and OT2).

Distributed: Similar to the decentral architecture, a distributed architecture also has groups of PS equipment controlled by one or more OT devices but with communication within and between the groups. This implies that the groups can cooperate to reach a collective decision according to the goals that have been set. In Fig. 2.3, OT3 and OT4 control three PS equipment of Feeder 2 in a distributed manner with communication between them. Multi-agent systems belong to this category. An agent-based distributed redispatch service is presented in [58]. Here, the substations of a transmission grid are equipped with an agent, which communicates and controls the PS equipment of that substation to remedy overloads.

Hierarchical: This can be regarded as a mixture of the above categories, where the devices are organised in two or more hierarchical levels. The higher level coordinates the lower levels, which control either single or groups of PS equipment in a local, decentral or distributed manner. OT1 and OT2 in Fig. 2.4 are in a hierarchical architecture with OT3. From a substation perspective, OT1 and OT2 can be at the bay level, while OT3 can be at the station level. In the hierarchical state estimation from [59], the substations run state estimation using local measurements in a decentral manner. The local estimates are transferred to a central control centre, which then coordinates the local estimates using the power flow measurements from the branches that interconnect the substations. The main benefit is that the control centre requires less computational effort since there is a reduced amount of data transmitted from substations to the control centre.

While local, central and decentral grid services have been a part of traditional PSs, the increased ICT penetration in medium and low voltage levels has increased distributed and hierarchical grid services [57]. This can also be attributed to the rising prominence of multi-agent systems [60]. Central services can also communicate at high speeds across large distances using IT technologies shown in Fig. 2.2.

The type of architecture also depends on the perspective of the system and the grid services. An OT device controlling PS equipment in a substation can be considered a central architecture from the substation's perspective. This can, however, also be regarded as decentral if the same is applied to the whole PS with several substations, each controlling its underlying equipment. For example, in Fig. 2.3, OT1 can be regarded as a central controller from the perspective of transformer T1 but as a decentral controller from the perspective of Feeder 1.

The choice of architectures for designing grid services depends on factors such as cost, complexity, communication overhead and fault tolerance. While central services are cheaper and easier to set up and maintain, the failure of the central entity will result in the failure of the whole grid service (single point of failure). Decentral and distributed systems, by definition, do not have a single point of failure, as parts of the system can still be operational despite failures. However, they are costly and complex to set up and maintain compared to centralised grid services. Furthermore, distributed grid services are more fault tolerant but more costly and complex to set up and maintain than their decentral counterparts. Since hierarchical grid services are a mixture of the other types, they are between central and distributed in terms of their pros and cons. Central grid services typically exchange large volumes of data between the field and the central control room, resulting in high communication overhead. Decentral, distributed and hierarchical schemes have comparatively more data flow between the field devices (within the hierarchy) but reduced or even no data flow to the control room (between hierarchies). Additionally, there exist countermeasures that can address some of the drawbacks of these architectures. Measures such as redundancy [37] and local fallback modes [11] can make central grid services resistant to a single point of failure. Virtualisation-based measures can change the grid service architecture during operation by reorganising and rerouting the data flow dynamically [42, 61]. However, such measures typically come with an increased cost and complexity. To summarise, there exist several options for designing ICT systems in CPESs, the choice of which should be decided based on the desired (fault tolerant) behaviour of the grid services, keeping costs and complexity in mind.

2.3 Disturbances in Power and ICT Systems

In this section, unless otherwise specified, the ICT terminologies are adapted from [62], and the PS terminologies are adapted from [63, 64].

The aim of system design is to ensure that the system operates at the required level of performance considering available resources (e.g., cost). However, certain events, both natural from the environment and man-made, challenge a system's performance, potentially pushing the system to an undesired state. Authors from PS and ICT domains refer to such events using different names.

In the ICT domain, a distinction is made between faults, errors and failures, and is illustrated in Fig. 2.5. A *fault* refers to a problem or defect in a component or system that can cause an incorrect or unexpected behaviour. Faults can be internal (e.g., software bug, hardware defect) or external (e.g., temperature, physical interference). A fault is said to be active when it manifests as an error. Otherwise, it is dormant. *Error* is the deviation between the actual and expected output and can result from faults or other external events. Errors are associated with the internal parts or components that interact and constitute a system. As shown in Fig. 2.5, errors can propagate among the internal parts of a component (or a system). A *failure* occurs when an error or a set of errors unacceptably alters the service delivered by the system, i.e., the system does not offer the desired level of performance. Here, the term system can also refer to a component (e.g., server) comprised of several sub-components (e.g., processor, hard disk). Component failures can cause faults in the encompassing system or in other components that are interfaced with it. Similarly, system failures can cause faults in the other systems to which it provides a service. In Fig. 2.5, the level of service provided by the component decreases (i.e., failure of the component) when the underlying errors reach the corresponding interface. In a nutshell, a fault can cause an error in one or more internal components of a system. However, a failure occurs only when these errors propagate to the interface and impact the service delivered by the system. For example, an incorrect part of the code (error) from a developer, when activated by an input that uses this part of the code (fault), may cause the program to terminate (failure).

These terminologies are used differently in the PS domain. Here, a *fault* in a PS is an abnormal condition that interferes with the normal (or desired) power flow. PS faults can be broadly classified into open-circuit and short-circuit. The origin of a fault, known as *causes*, can be internal (e.g., ageing, improper maintenance) or external (e.g., tree falling, human damage). Faults can also occur within a component, potentially damaging the component (e.g., transformer damaged due

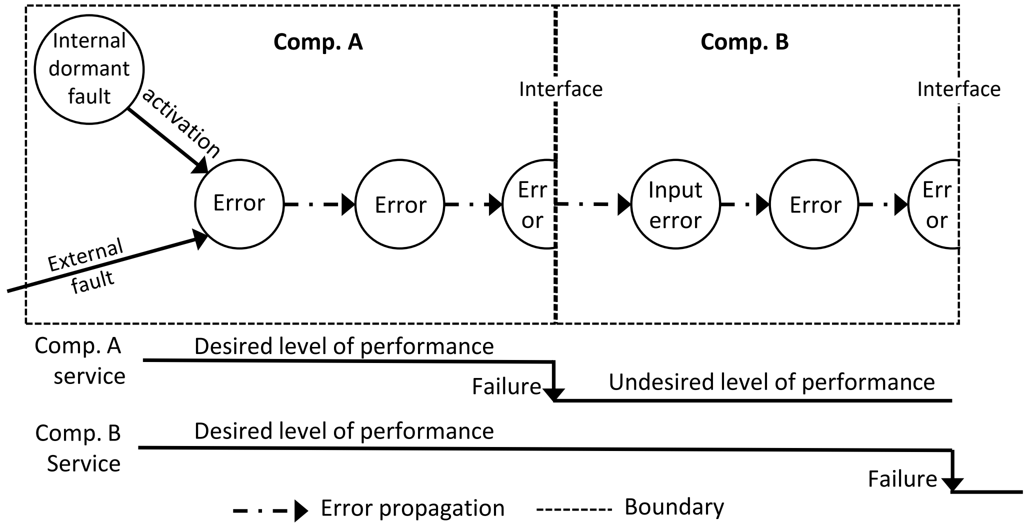


Fig. 2.5: Fault, error and failure in the ICT domain [62].

to overheating). A fault may cause a *failure*, which is the incapability of a system or a component to fulfil its desired function. From a system perspective, failures refer to power outages, and from a component perspective, they refer to damage or maloperation. For example, a tree branch falling on an overhead line (cause) can result in a short circuit (fault), which, when not isolated by the protection system, will result in a power outage to some consumers (failure). Similar to the ICT domain, certain PS failures may also lead to faults. Impurities (cause) can lead to insulation breakdown (failure) in an underground cable, leading to a line-ground short circuit (fault). Since PSs are typically designed with N-1 redundancy, failures in a PS (i.e., blackouts) are caused by combinations of component failures and other influencing factors [65].

A key difference between the PS and ICT terminologies is that events, such as ageing and tree falling, are referred to as *faults* in the ICT domains but as *causes* (which lead to faults or failures) in the PS domain. Additionally, although the term *error* is not widely used in PSs (but is well established in the ICT domain), certain authors such as [16, 66] use it to capture incorrect human actions such as faulty relay settings or tap change. Still, malicious actions such as vandalism and cyber-attacks are considered as causes. Furthermore, based on the disciplines of analysis, numerous terms exist for the events that challenge the functionality and performance of a component or a system [20]. Tab. 2.1 lists some of these terms. To maintain a consistent nomenclature in this interdisciplinary dissertation considering PS and ICT systems, the term disturbance is used and will include all terms in Tab. 2.1 and is defined as follows:

Definition 4 *A disturbance is an unexpected event that can cause damage and/or disrupt system performance. Disturbances can be from both PS and ICT systems and will often require remedial actions to be taken. Examples of disturbances are disruptions of power lines, sudden generation fluctuation, transformer malfunction, software bugs, cyber-attacks and failure of servers [64].*

Tab. 2.1: Different terms to denote disturbances in the literature of CPESs [20].

Perturbations	Anomalies	Harmful events	Emergency
Disruptions	Threats	Losses	Hazards
Adversity	Shocks	Stressors	

In this dissertation, the term *disturbance* refers to the impact of faults and causes on the CPES. For instance, a power line could be disrupted (disturbance) because of weather, overload or tree contact, all of which are causes. In the ICT system, software can give incorrect output (disturbance) due to bugs, user errors or cyber-attacks, all of which are faults. These disturbances, as explained later in Sec. 2.5, can also propagate to cause or aggravate other disturbances. A CPES should be designed so that disturbances (as many as possible) should have either no or minimal disruption on the system's performance, considering available resources.

2.4 Operational States of Power Systems

The operational states of a PS capture its current performance. The literature presents different versions of PS operational states. The German Association of Energy and Water Industries (BDEW) presents the *smart grid traffic light concept* [67], which is proposed for distribution grids and is aimed at the use of grid flexibility and market participants. For a particular time period, the status of a PS segment can be classified into green, amber and red states (or phases). Each state has specific rules for the interaction between market participants (e.g., suppliers, balancing group managers, generators) and the grid operator. The state classification is done by the operators using forecasts based on parameters such as load profiles and weather data from their grid segment. These states indicate the general need for flexibility in the corresponding grid segment. Fig 2.6 presents a summary of this traffic light concept, which has been applied to operate agent-based distribution grids in [68]. The three states are as follows:

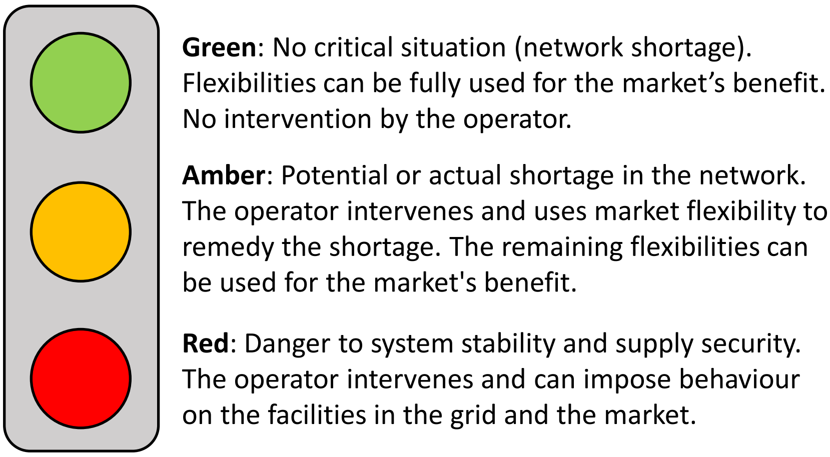


Fig. 2.6: Smart grid traffic light concept from BDEW.

Green: A PS segment is in the green state (known as the market phase) if there is no critical grid situation regarding grid shortages. All market flexibility products can be supplied and demanded without any restrictions or intervention from the grid operator. The market participants use flexibility exclusively for the benefit of the market.

Amber: A PS segment is in the amber state (known as the interaction phase) if there is a potential or actual shortage regarding flexibility. The operator calls upon contracted flexibility from the market participants to remedy the situation. The remaining flexibilities can be used for the benefit of the market. Consumers can adjust their behaviour and profit from contributing to the system’s stability.

Red: A PS segment is in the red state (known as the network phase) if there is a risk to the system’s stability and, thus, the security of supply. In addition to the measures in the amber phase, the operator directly intervenes in a controlling or balancing manner in their own operational facilities, the facilities of downstream grid operators and the market. The PS segment is in this phase when the operator uses non-market-based regulation or control measures to ensure system stability.

The authors in [43, 18] propose a five-state classification model for PS. These models are driven by disturbances and contrast the BDEW traffic light model, which is driven by markets. Based on a combination of measurements (e.g., voltage, current) and grid information (e.g., number of loads and generators), the current performance of a PS can be classified in one of five states – Normal, Alert, Emergency, Blackout and Restoration, which are shown in Fig. 2.7. Disturbances can cause transitions from a better to a worse state, referred to as state degradation. Depending on the PS state, suitable grid services can be applied to improve the state (curative actions) or prevent further system degradation (preventive actions), both of which fall under remedial actions. This five-state model is both mandated and comprehensively documented by ENTSO-E in [23].

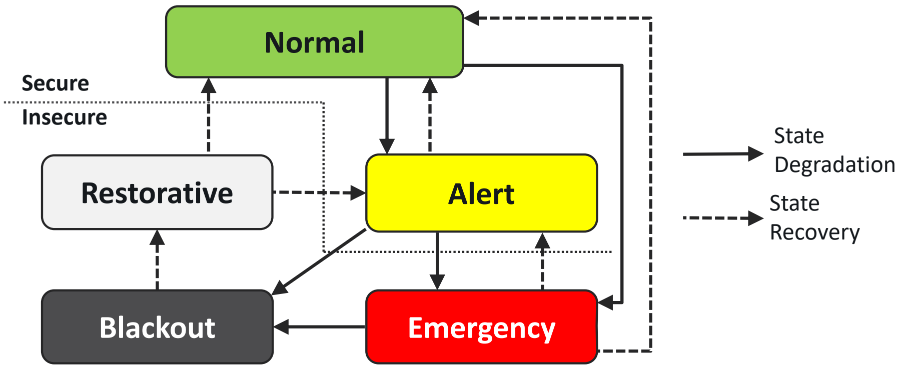


Fig. 2.7: Operational states of a power system.

The aforementioned traffic light concept is mainly aimed at flexibility deployment considering markets. The five-state model is used in this dissertation because markets are beyond its scope. Furthermore, this model is widely used across Europe, covers a wider range of system behaviours (e.g., Blackout and Restorative states), and its applicability to distribution grids has been discussed in [34]. In the remainder of this dissertation, PS operational states refer to the five-state model.

The elements necessary for the state classification are first defined in the following sections, and then the state classification process is explained. This explanation summarises the vast information in [23] and is based on [34].

2.4.1 Elements of Power System Operational State Assessment

The following elements are required to assess the operational state of a PS:

Operational security limits: This is the most important criterion for the state classification process, and it describes explicit operational thresholds for various PS parameters such as system frequency, voltages at all buses, currents on all lines and number of loads served. These thresholds are specific to each state, and typical values can be found in [69].

High-level services and remedial actions: As explained in Sec. 2.2.1, high-level services like state estimation provide situational awareness to system operators, enabling them to detect disturbances via corresponding operational limit violations.

Suitable remedial actions can then be deployed to counteract the disturbance and remedy the operational limit violation. When high-level services are lost, the operator becomes blind to disturbances and, therefore, cannot deploy the required remedial actions. This can potentially result in blackouts [16]. The system operator gathers a list of available high-level services and remedial actions for assessing the operational state.

Contingency list: This list consists of all viable contingencies[2] in a PS and is compiled by the system operator. It includes all possible disturbances in components like generators, transformers, buses and power lines that endanger the operational limits of the grid, along with their occurrence probabilities. This list is updated and exchanged regularly among neighbouring system operators. Additionally, a list of exceptional contingencies is also created and exchanged. This includes uncommon (or low probability) combinations of disturbances such as loss of double lines, loss of a busbar, and common mode failures of generating units and direct current (DC) links. Detailed information on this list can be found in [71].

Contingency analysis: In this analysis, each contingency from the contingency list is simulated based on the most recent situation from the high-level services, mainly using the state estimation results. Suitable remedial actions are then identified for all the contingencies that would violate the operational limits. These are referred to as *critical contingencies*, which are simulated once again considering the identified remedial actions. The result of this analysis is a list of contingencies that, even after utilisation of all available remedial actions, would still lead to an operational limit violation. Detailed information on contingency analysis can be found in [72].

2.4.2 Power System State Assessment Process

Using the aforementioned elements, Fig. 2.8 summarises the PS state assessment process, which is repeated at each required time instance. The Restoration state is not shown in Fig. 2.8 as it is a special state subsequent to the Blackout state and is not a direct result of the state assessment process. The explanation of the states and their implication for system operation is as follows:

Normal: A PS is said to be in the Normal state if no operational limits are violated and if the resulting list from the contingency analysis is empty. This implies that all potential contingencies can be remedied using the available remedial actions. This

[2] A PS contingency is an identified, possible or already occurred fault of a component, including the assets of the system operator as other significant grid users [70].

state indicates that the system is working as desired, and therefore, the focus can be on economic optimisation by decreasing operational costs.

Alert: A PS is said to be in the Alert state if the contingency analysis, based on the current situation using the currently available high-level services and remedial actions, has identified at least one contingency that would violate the operational limits. This implies that there is at least one contingency for which there is currently no available countermeasure. In this state, since operational limits are yet to be violated, preventive actions are deployed to potentially restore the system to its Normal state.

Emergency: A PS is in the Emergency State if any operational limit is violated (e.g., over/under voltage, overcurrent in lines) or if any of the tools and facilities (i.e., the high-level services) have failed for more than 30 minutes. Note that the impact on the system state when the failure of these tools and facilities is less than 30 minutes is not defined in [23]. In this state, suitable curative actions have to be deployed to remedy the problem and improve the system state.

Blackout: A PS is said to be in the Blackout state if more than 50 % of loads are lost or if there is a loss of voltage (less than 60-80% of rated voltage [73]) for more than 3 minutes. This is the worst possible state for a PS and is typically characterised by the system being split into unsynchronised islands. Suitable actions such as restoration and black start should be applied to eventually return the system to its Normal state.

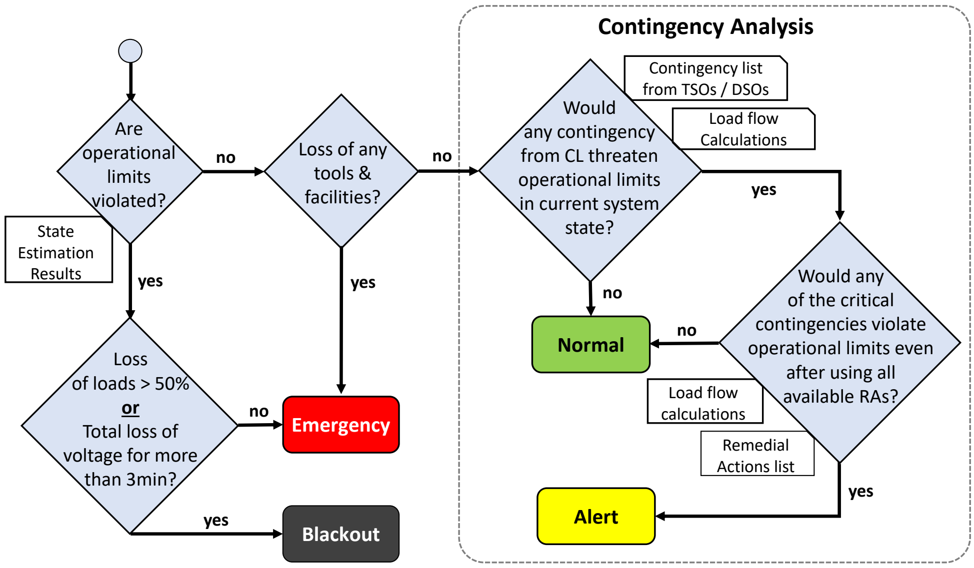


Fig. 2.8: ENTSO-E power system state assessment process (CL stands for contingency list and RA for remedial actions).

2.5 Interdependencies between Power and ICT Systems

One main drawback of the aforementioned PS operational states is that they are based solely on PS parameters and do not adequately capture the performance of the ICT system. In other words, the PS operational states can capture the impact of PS disturbances but not ICT disturbances. This is relevant because past blackouts have also shown that disturbances can impact the performance of the ICT system (cf. Sec. 1.2), thereby impacting the performance of the whole CPES. This limits the application of the PS operational state to CPES with interdependent PS and ICT systems.

To assess the performance of a CPES, the interdependencies between the power and ICT systems should be considered. In this regard, interdependencies in critical infrastructures (or systems), particularly cyber-physical systems, were explored in [74]. Here, interdependence is defined as follows:

Definition 5 *Interdependence is a bidirectional relationship between two infrastructures through which the state (or performance) of each infrastructure influences or is correlated to the state (or performance) of the other[74].*

The authors also identify four types of interdependencies, namely physical, cyber, geographical and logical. Ref. [75] presents a simpler classification with two types. This classification is used in this dissertation and is as follows:

Structural: A structural (or physical) interdependence arises from a physical linkage between the inputs and outputs of two systems. An example is the PS providing power supply to ICT system components. This dependence can, however, be decoupled using a battery backup for the ICT components.

Functional: A functional (or logical) interdependence arises when a system is necessary to operate another system. The operation of a CPES, to a large degree, depends on the data transmitted through ICT systems and the resulting operational decisions. ICT disturbances, such as IT congestion, may result in delayed or incorrect control action in the interconnected PS. This interdependence is also related to controlling schemes that link two systems, e.g., special protection schemes [16].

Interdependencies increase the overall risk as disturbances can now propagate beyond the boundaries of a system through them and impact the connected system. In [10] and [26], three types of disturbance propagation, which can occur due to the presence of one or more aforementioned interdependencies, are identified. They are as follows:

Cascading: This is referred to as the domino effect, where disturbances in one system cause a disturbance in the interconnected system. Examples are a substation failure resulting in loss of power supply to the connected ICT components and a cyber-attack in the control room causing power interruption in certain parts of the PS.

Escalating: This is characterised by an existing disturbance in a system exacerbating an independent disturbance in the interconnected system, increasing its severity or the recovery time. For example, a protection system malfunction can worsen the impact of a short circuit, resulting in a loss of power supply to larger parts of the PS.

Common-cause: This is a consequence of spatial interdependence where a common disturbance could simultaneously impact both systems in close proximity. Natural disasters typically cause such disturbances. For example, a fire can damage power and communication lines in the same place. Since natural disasters are beyond the scope of this dissertation, this type of disturbance propagation is not considered.

2.6 Joint Operational States of Power and ICT Systems

A joint operational state model enables the operator to assess the state (or performance) of a CPES, potentially allowing the detection of early degradation and is the focus of RQ1 of this dissertation (cf. Sec. 1.5). Such a model should account for the aforementioned interdependencies between the power and ICT systems. Due to its critical nature, several research works model PS-ICT interdependencies for analysing the propagation of disturbances. This section presents this literature by categorising them into *operational state models* and *interdependence models*. While the former aims to develop general operational state models for PS and ICT systems, the latter models the interdependencies for analysing specific use cases and does not focus on operational states. Fig. 2.9 depicts an overview of the literature considered in this dissertation. This section concludes with a summary of the literature review on joint PS and ICT state models.

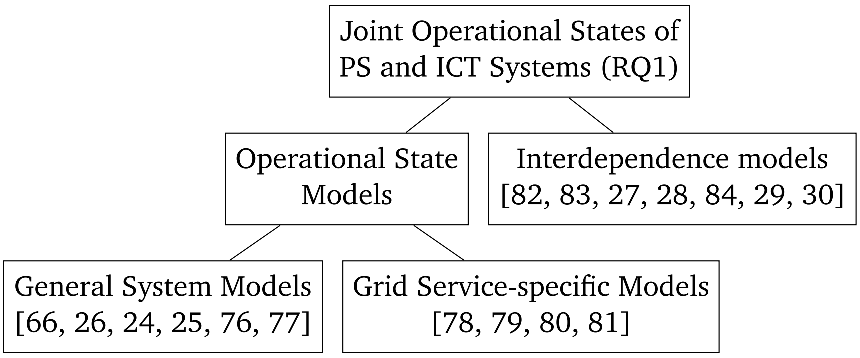


Fig. 2.9: Categorisation of literature on joint operational state of PS and ICT systems.

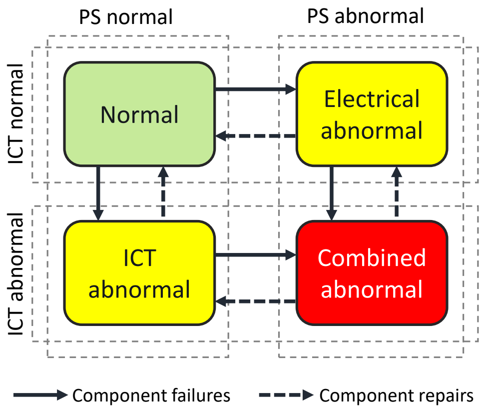
2.6.1 Operational State Models

The literature on operational state models is further categorised into *general system models* and *grid service-specific models*. While the former aims at modelling joint operational states of PS and ICT systems as a whole, the latter focuses on the operational states of specific ICT-enabled grid services.

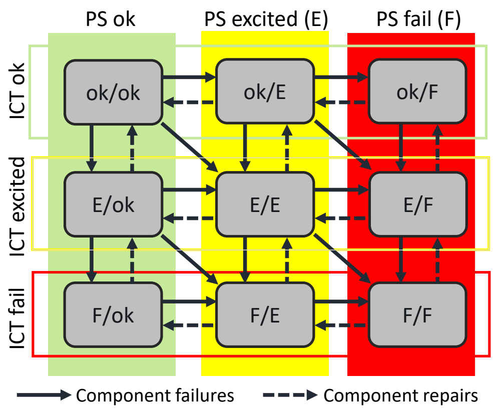
General System Models

The pioneer joint model from [24] considers binary states for both PS and ICT systems and is shown in Fig. 2.10a. When both PS and ICT systems are in their *normal* states, the joint system is in the *normal* state. The ICT *abnormal* state is reached when any electronic components, including software, fail. The joint *abnormal* state is worse than individual *abnormal* states as information from the other system cannot be used for restoration. This model is extended in [25] considering component failure and repair rates to analyse the contribution of ICT disturbances to PS blackouts. Particularly, the impact of inadequate operator situation awareness, i.e., the discrepancy between the perceived state in the control room and the actual system state, is investigated. Markov chains and Monte Carlo simulations are used in this research.

Ref. [66] presents a model with PS and ICT systems having three states each - *ok*, *excited* and *failure*, as shown in Fig. 2.10b. It is aimed at operational support tools for control centres and can describe past incidents by tracing their trajectories considering the interdependencies. The *excited* state indicates that the system is working correctly but may soon face a critical situation, e.g., N-1 redundancy is harmed in the PS and a failure of a redundant ICT component. This model is used in [76] to show how ICT can aid in the detection of disturbances and recovery of the interconnected PS. Although [66] and [76] also discuss a service-centric approach, i.e., consider the ICT-enabled grid services in the state models, they do not present use cases based on it.



(a) Model from [24].



(b) Model from [66].

Fig. 2.10: Joint operational state models from the literature.

Ref. [26] proposes a joint model with PS and ICT systems having four and five states, respectively, specifically for describing cascading, escalating and common-cause disturbance propagations. The model is formalised using Petri nets. While [24, 25] model PS and ICT systems with binary operational states, the authors in [66, 26] model the intermediate (*excited* or *partial outage*) states of the two systems. This is essential as complex systems, especially ICT systems, exhibit graceful degradation, i.e., operate with limited performance even when certain system parts have been rendered inoperative by disturbances.

From a purely IT (or communication) network perspective, the authors of [77] present the ResiliNets framework. The state of an IT network is depicted in a 3x3 matrix consisting of two dimensions, i.e., *operational states* and *service parameters*. The former represents the functionality of its physical components, and the latter represents the service provided by the network. Fig. 2.11 shows the ResiliNets state space with an exemplary state trajectory of an IT system. Here, transitions T_1 and T_2 represent degradations, whereas T_3 and T_4 represent recoveries.

Grid Service-specific Models

The authors of [78] use the binary state model to investigate the impact of demand and generation side management services on the reliability of the interconnected

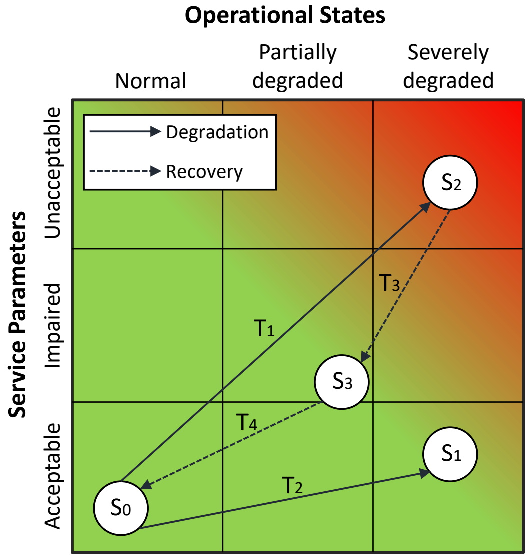


Fig. 2.11: Resilinets state space from [77].

PS. These services are assumed to be implemented using IEDs and a simple communication network. ICT disturbances can cause the grid service to transition from the Normal to the Failed state. The aforementioned *general system model* [66] is formalised using Markov models and is applied for the advanced metering infrastructure service in [79]. The results show the impact of failure/repair rates of ICT components such as antennas, servers and smart meters on the overall unavailability of the PS infrastructure. The impact of the operational states of three grid services – decentralised grid automation, on-load tap changer, and line voltage regulator, is proposed in [80]. A three-state Markov model is developed specifically for each of the three grid services, and the state transitions are based on component failures and repair. This work introduces the so-called *Limited* state, where a grid service exhibits a reduced but acceptable performance. This approach is applied to special protection schemes (SPS) in [81], where different *Limited* states representing the loss of different functionalities are proposed. The impact of the states of SPS is then analysed, considering preventive and curative disturbance scenarios.

Limitations of Operational State Models: The literature in this category has certain common limitations. The *general system models* focus only on structural dependencies and not on functional dependencies, i.e., they do not consider the ICT-enabled grid services. This is essential since they link the operation of the power and ICT systems [34]. While [24, 66] are only conceptual, [25, 26] consider rather small power and ICT systems. The Resilinets framework from [77] is applied for a realistic IT system but does not consider PSs. In *general system models*, it is assumed that the failure or repair of a single ICT component will lead to a state transition.

However, considering large-scale systems, a single component does not necessarily impact the overall performance due to, for instance, the presence of non-critical or redundant components. On the other hand, *grid service-specific models* lack generality as they use different models for different grid services. While they consider the states of grid services, they do not model the dependencies between them (e.g., redispatch from control rooms using state estimation results). The state definitions used are specific to these models and do not hold any meaning outside the respective model context. The conditions to identify the state of the grid services, especially the Limited state, are also not formalised. Additionally, the states and transitions are only based on component failures/ recoveries and do not consider other ICT system aspects such as latency and accuracy into consideration.

2.6.2 Interdependence Models

The research in this category focuses on the interdependence between power and ICT systems to analyse vulnerabilities and propagation of disturbances but does not focus on operational states. Graph theoretical approaches are used in [82, 83, 27] to model interdependencies to assess the vulnerabilities of interconnected power and ICT systems. The authors in [82] apply the theory of complex numbers to graph networks to represent the topological interconnections. Critical nodes are then identified using node degree and node efficiency as metrics. A graph-based optimisation problem is proposed in [83] to detect critical PS nodes, which, when removed, can cause cascading disturbances in the connected ICT system. However, it does not model the impact of ICT node removal of the PS. The authors in [27] use power flow dynamics considering ICT dependencies as constraints to identify critical power lines and communication links. It, however, focuses only on cascading disturbances caused by malicious cyber and physical disturbances. The objective functions in [83, 27] are the number of connected components and loss in the served load, respectively. In addition to modelling cascading disturbance considering the ICT system, Ref. [28] includes the human operator. A three-layer Markov chain is used considering the number of power lines and communication link failures, as well as the operator performance level. Note that these works consider both structural and functional interdependencies.

Some works also model the interdependence to analyse specific grid services. Considering the impact of ICT vulnerabilities on emergency control, [84] formulates the load shedding service as an optimisation problem considering ICT disturbances via structural interdependencies. A similar approach is presented in [29] but considering the dynamical modelling of a PS and multiple communicating areas for an ICT system. The authors [30] use stochastic activity nets to model the interdependence focusing on the redispatch service. Here, the availability of ICT components and PS line overload probabilities are investigated. These works also consider structural and functional interdependencies, but the latter is limited only to the specific grid services.

Limitations of Interdependence Models: The literature on *interdependence models* also have certain limitations. They mainly focus only on cascading disturbances and do not consider escalating disturbances. While [82, 83, 27, 28] aim to model interdependent power and ICT systems in general, [84, 29, 30] focus on specific grid services. The former does not consider these services (focuses only on components), and the latter does not consider multiple grid services and their dependencies. Furthermore, since these works do not consider operational states, they cannot provide an aggregated view of the performance of interconnected power and ICT systems.

2.6.3 Summary of Joint Operational States

The RQ1 of this dissertation aims to address some of the aforementioned limitations by developing a joint operation state model for power and ICT systems considering structural and functional interdependencies for analysing cascading and escalating disturbances. For the PS states, the proposed model builds on the well-established ENTSO-E operational state classification discussed in Sec. 2.4. For the ICT system, a new model representing the states of the grid services, especially their degraded performance, is developed in this dissertation. These states are designed to be general to consider multiple grid services as well as their dependencies among one another. The operation states are modelled using discrete finite state machines due to their popularity in literature to model discrete states and transitions among them (cf. Sec. 2.6.1). The PS, ICT system and their interdependencies are modelled using graphs since the literature (cf. Sec. 2.6.2) suggests graph theory to be suitable for modelling interconnected complex networks. The resulting model should be capable of assessing the propagation of multi-domain (i.e., PS and ICT system) disturbances in terms of the operational state trajectory of CPES while being able to consider multiple grid services. These requirements of the joint operational state model have been summarised in Sec. 1.5.

2.7 System Resilience

Followed by a brief definition of resilience, this section presents the state of the art in resilience assessment and concludes with a summary.

2.7.1 Definition of Resilience

Resilience, a concept that originated in psychology and ecology, is multi-disciplinary with several different definitions [85], some of which are summarised in [20]. It shows that resilience is typically about the behaviour and response of a system to high-impact disturbances. As discussed in Sec. 1.3, resilience is not about preventing disturbances from occurring but managing the performance of the system when faced with disturbances. Even with regard to PSs, several definitions and notions of resilience can be found, such as the ones in [20, 17, 21, 86]. For the sake of cohesion, this dissertation uses the notion of resilience from the German Energy Systems of the Future (ESYS) initiative [21], which is:

Definition 6 *Resilience is defined as the ability of the system to absorb the impact of disturbances without collapsing and then return to normal operation as fast as possible.*

As presented in Sec. 1.3, resilience can be depicted by the *bathtub curve* in Fig. 1.1. A resilient system, when faced with a disturbance, can stabilise itself at a lower level of performance (i.e., degraded performance) and return to normal performance as fast as possible without completely failing. The figure also shows that the behaviour of a resilient system has four constituting phases, which are described as follows:

Robustness is the ability of the system to withstand (or resist) disturbances without performance degradation. In Fig. 1.1, it can be seen that the resilient system is robust against the first disturbance, while the same disturbance causes the performance of the non-resilient system to degrade.

Absorption is the ability of the system to respond to a disturbance by moving to a lower level of performance without failing (or collapsing). In Fig. 1.1, the resilient system absorbs the second disturbance by transitioning from normal to degraded performance. In contrast, the non-resilient system does not absorb the disturbance, and as a consequence, this system fails.

Stabilisation is the ability of the system to maintain itself in the lower level of performance without further degradation. The resilient system in Fig. 1.1 shows a stable operation with degraded performance. This phase is essential for dynamic systems, where external disturbances may cause instabilities, which may manifest themselves in terms of performance degradation after some time.

Recovery is the ability of the system to restore itself to normal operation. The resilient system in Fig. 1.1 is recovered from a degraded to normal performance faster than a non-resilient system. A resilient system after recovery is said to be in the *improved normal* state, indicating that the system would learn and adapt itself from past disturbances.

These phases are referred to by different names in the literature. For example, robustness is referred to as resistance [85] or persistence [87], while absorption and stabilisation are collectively referred to as resourcefulness [17] or self-organisation [19]. While literature agrees about the last three phases, authors such as [21, 77] consider robustness as a part of resilience, whereas [17, 31] do not.

Based on the time scale, resilience can be classified into short-term resilience considering individual disturbances and long-term resilience considering a set of disturbances [17, 19]. This dissertation focuses on the latter.

Short-term resilience pertains to the time before, during and after a disturbance and can range from seconds to weeks. In case of natural disasters, this can go up to months. Here, the PS behaviour is influenced by preventive and curative services such as reserve planning, generation redispatch and ensuring black start capability.

Long-term resilience pertains to system design and the improvements from past disturbances. This can range from months to years and is an enabler for short-term resilience. Examples include improving emergency plans, upgrading components, and better personnel training.

2.7.2 Assessing Resilience of CPESs

A necessary precursor for designing resilient systems is a method to assess and compare the resilience of different design options quantitatively. The reason is that, as discussed in Secs. 2.1 and 2.2, several options exist to design CPESs, particularly the ICT system. This subsection presents a literature review on the resilience assessment of CPESs. As shown in Fig. 2.12, this is categorised into *surveys & concepts* and *methods & metrics*.

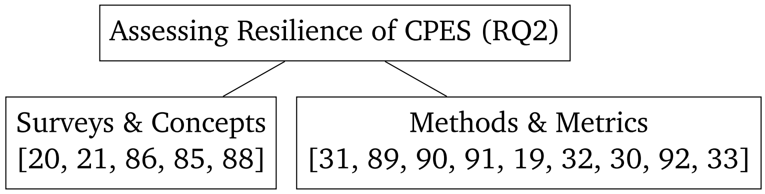


Fig. 2.12: Categorisation of literature on assessing the resilience of CPESs.

The literature under *surveys & concepts* constitute either literature surveys or conceptual frameworks without concrete methods and use cases. Refs. [17, 20, 85] comprehensively summarises assessment methods, quantification metrics and improvement measures. They conclude that the quantification and assessment of resilience is still nascent research, including several subtopics such as reliability, robustness, risk and security. Although several methods exist to assess and metrics to quantify resilience, they are yet to be universally accepted or standardised for CPESs [85]. Ref. [86] is one of the first to apply the *bathtub curve* to assess PS resilience. This is improved by the authors in [88], where socio-economic tradeoffs for assessing and improving resilience are discussed. Both these works conclude that ICT integration is an essential enabler for resilient PSs as ICT can enable the detection and potential mitigation of extreme disturbances. Ref. [21] discussed resilience with a focus on reducing the risk of blackouts. The authors conclude that the integration of ICT as well as understanding the interactions between power and ICT systems, are important for a resilient CPES. This implies that designing resilient individual subsystems will improve the resilience of the whole CPES.

The literature under *methods & methods* proposes methods to quantitatively assess resilience, which are then demonstrated with use cases. In [31], a quantitative approach for interdependent systems is proposed using an area-under-curve metric called *measure of performance* (MOP). Resilience is calculated by integrating the MOP over time. This is shown by the shaded area in Fig. 2.13, which consists of three phases, namely, original steady, disruptive and recovery. The phase after the recovery is the new steady state, where the system has learned and improved from the disturbance. A use case of a Swiss high voltage grid is presented with available power lines and power demand served as MOPs. Utility data, i.e., outages and repair of components from historical events, is fundamental to quantifying resilience and motivating system improvements [89]. Here, a resilience metric is derived using probabilistic distributions of outages and repairs of various components. Resilience is essentially calculated as the difference between the outage and repair curves. This method, however, focuses only on the resilience of individual components and not the whole system. The authors in [91] propose several quantitative resilience metrics, referred to as indicators. In addition to the aforementioned area-under-the-curve *performance indicators* (e.g., unserved loads, disruption cost), they also propose *capacity indicators*. The former indicates *how* resilient a system is in the case of disturbances, while the latter indicates *what* makes a system resilient. Capacity indicators encompass system design aspects such as energy reserves, import dependence and generation mix diversity.

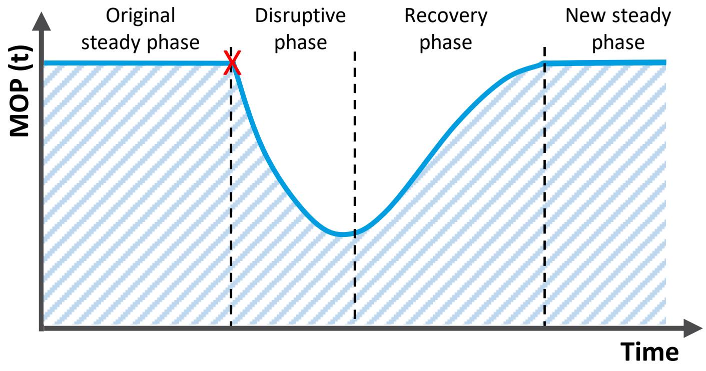


Fig. 2.13: System resilience and measure of performance (MOP) [31].

The authors in [90] present a resilience evaluation framework consisting of four steps, namely, recognise disturbances (e.g., natural disaster, cyber-attacks), define resilience metrics (e.g., restoration time, load shredded), choose a methodology (e.g., simulation- or probability-based) and obtain evaluation results (e.g., resilience value, expected value). Simulation scenarios on the IEEE 33 bus grid with load restored and the corresponding time taken as metrics are presented.

An assessment of PS resilience based on its operational states (cf. Sec. 2.4.2) is discussed in [19]. Fig. 2.14 shows how these states can be mapped to the concept of resilience, with the state transitions indicating changes in system performance. Here, a sequential Monte Carlo-based simulation using the failure and repair rates of components is proposed to assess PS resilience. This approach is similar to the aforementioned Ref. [89], which uses utility data.

Regarding the resilience of ICT systems, Ref. [32] uses the Resilinets framework from [77] to assess resilience and suggest improvement measures. Here, resilience is quantified as the area under the trajectory through the state space shown in Fig. 2.11. For example, the trajectory $T1 - T3 - T4$ indicates resilience, whereas $T2$ does not. The authors in [30] also use the ResiliNets framework for analysing CPES resilience, using the number of overloaded power lines and the availability of ICT components as resilience metrics. ICT resilience for the early detection and recovery during natural disasters using metrics such as the number of damaged telecommunication lines and base transceiver stations is investigated in [92]. Resilience in interdependent

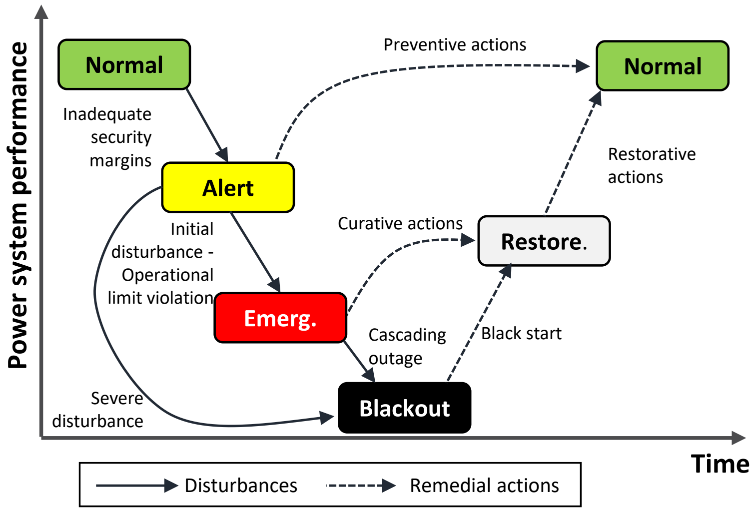


Fig. 2.14: Mapping of PS performance to resilience bathtub curve [19].

power and ICT systems is surveyed in [33], which discusses metrics such as the probability of wireless transmission failure and change in telecommunication quality of service.

Limitations: Although several methods and metrics for assessing resilience exist in the literature, they are yet to be universally accepted or standardised [85]. A common shortcoming is that the literature focuses only on the PS and does not explicitly consider the ICT system. ICT components (e.g., IEDs, routers, software) have a faster innovation cycle than PS components and, therefore, undergo modifications more frequently [86]. As a result, several options exist for designing ICT systems for CPESs. Some options are already discussed in Secs. 2.1 and 2.2, such as different IT technologies (e.g., cellular, ethernet), architectures (e.g., central, distributed) and network topology (e.g., radial, meshed). This necessitates investigating the impact of such design aspects on the performance and resilience of ICT systems. Furthermore, the ICT-focused research considers only infrastructural aspects, emphasising data transfer. They do not consider the grid services, which impact the short-term resilience of the PS and, consequentially, the overall CPES. Furthermore, the existing area-under-curve metrics have unbounded domains (e.g., from zero to large values), making them hard to comprehend and challenging to use for comparing systems.

2.7.3 Summary of Resilience Assessment

To summarise, the current literature lacks methods and metrics to quantify the resilience of ICT-enabled grid services. The ICT system should be designed such that the grid services it enables are resilient, i.e., they should bounce back from disturbances without collapsing. The RQ2 of this dissertation addresses some of the aforementioned limitations by proposing a method and metrics to quantify and assess the resilience of ICT-enabled grid services. This model builds upon the operational state model from RQ1. Following the work of [19], the operational states of grid services will be used to measure their corresponding performance determined using sequential Monte Carlo simulations. The resulting method and metrics should enable a comparison of different ICT design options in terms of the resilience of grid services. These requirements for the methodology to quantify resilience have already been summarised in Sec. 1.5.

3 Operational States of ICT-enabled Grid Services

This chapter conceptualises the operational states of ICT-enabled grid services in CPESs. First, the properties of the ICT system are discussed, based on which the operational states of the grid services are defined. These states are then applied to three case studies, namely, state estimation, on-load tap changer-based voltage control, and redispatch of DERs. While this chapter conceptualises the operational states of grid services and the PS-ICT interdependencies, the following Chapter 4 presents their formal modelling. The contents of this chapter are partly published in [34] and [11].

3.1 Properties of ICT System

As discussed in Sec. 2.2, the main functions of the ICT layers are measuring and actuation (OT), data transfer (IT), and processing (decision making). The grid services use a combination of hardware and software components from the three ICT layers. Each grid service imposes certain requirements on the functions of ICT layers referred to as quality of service requirements. Examples of these requirements are the availability of sensors at certain buses, the speed of data transfer, and computational resources for processing in servers [49, 38]. Violating these requirements will result in abnormal operation of the corresponding grid service [8, 42]. Therefore, the ICT system should be designed to satisfy the requirements of the grid services in it.

In this dissertation, the requirements of these services are represented by three properties of the ICT system. Since the requirements are specific to each grid service, so are these properties. They are defined as follows:

Availability is attributed to components and data of OT and decision-making layers. Component availability is the state of being operational at a specific time and can be measured, for instance, using heartbeats [42]. Since grid services rely on ICT components, their performance is affected by the availability of the ICT components. For example, a voltage control service requires the tap-changing controller to be functional, and a state estimation service requires a server to process the received measurements. Data availability pertains to the required data (e.g., measurements, setpoints) being present and accessible at a specific time. Examples of data availability are field measurements required for state estimation service and open/close commands to switches for the topology management service.

Timeliness is the total time lapse between the transmission of measurements and the reception of data (e.g., measurements and setpoints). Timeliness corresponds to different delays in the layers of the ICT system and is illustrated in Fig. 3.1. The speed of data transfer through the IT network, called latency, constitutes the majority of the overall timeliness. The reason is that the serialisation and queuing delays depend on the distances and technologies in the IT network [48]. Certain aspects of timeliness, such as delays in the OT layer, are constant. However, other aspects, such as the latency of the IT network and processing delays, can vary depending on the data traffic. While latency of the IT network can be measured by pinging [93], the processing delays at the decision-making layer can be measured using ICT monitoring tools as shown in [55].

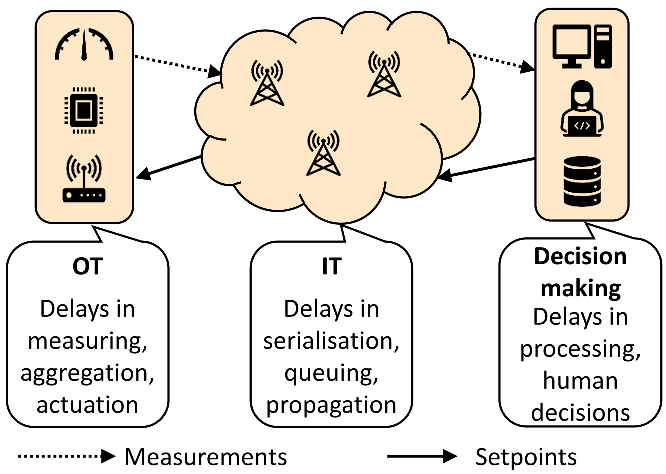


Fig. 3.1: Different aspects of timeliness corresponding to the ICT layers.

High-level services, such as state estimation, are typically run at regular intervals of time [94]. This imposes a timeliness requirement for the field measurements to reach the server where they will be processed. Alternatively, since remedial actions counteract the impact of PS disturbances, their timeliness requirements depend on the severity of the disturbance and the dynamics of the corresponding physical phenomena [95].

Correctness is attributed to data and is defined as the closeness of data to its ground truth. The correctness of data, such as measurements, influences the grid services using this data. The correctness of measurements is influenced by the accuracy of the sensors, which is defined as a percentage deviation of its reading, e.g., 1% or 3% [96]. The accuracy of a sensor is static and can be estimated using bad data detectors [97]. Correctness can also be impacted by noise interference and malicious manipulations, which, in contrast to accuracy, can result in large deviations of data from its ground truth. In such cases, estimating correctness is challenging since the ground truth is typically unknown. Several metrics such as variance [34], largest normalised residual test [98], uncertainities [94] and trust [99, 41] are proposed in the literature to quantify correctness.

The grid services need not necessarily have requirements based on all three properties, e.g., timeliness is critical for remedial actions such as protection services but is not so for certain economic services. These three properties can capture various ICT disturbances, which impact the functions of the ICT system, i.e., measurement and actuation, data transfer and computation (cf. Sec. 2.1). Tab. 3.1 shows how a non-exhaustive list of ICT disturbances can be mapped to the ICT properties. For example, ICT hardware failure due to power supply loss or damage will affect its availability. Cyber-attacks can manipulate data (correctness) and/or perform denial of service (availability). A distinction is made between the software of ICT components and the servers because the former impacts only the individual component, while the latter is more critical as it impacts the whole grid service. In this regard, a software crash affects the grid service's availability, while bugs can either delay the result (timeliness) or yield wrong results (correctness).

3.2 Operational States of ICT-enabled Grid Services

The operational states of ICT-enabled grid services, which capture their performance, are defined using the three aforementioned properties. They are as follows:

Normal: In this state, the grid service is fully functional (ideal performance) and can be used by the operator as intended. This implies that the required components are available and the required data is available, correct and transmitted in time (i.e., timeliness is satisfied). Therefore, coordinated decision-making and control using the ICT system are possible. A grid service is said to be in the Normal state if no disturbance has occurred or if the occured disturbances have been absorbed by the robustness of the ICT system (e.g., via redundant components), resulting in no impact on the performance of the service.

Tab. 3.1: Exemplary ICT Disturbances mapped to Availability (A), Timeliness (T) and Correctness (C) from [36]. 'All' refers to all three layers of the ICT system.

ICT Disturbances	Affected ICT Layers	Examples	A	T	C
Hardware failure	All	Sensor looses power supply Controller gets damaged	✓		
Hardware malfunction	All except links	Controller performs faulty actions			✓
		RTU sends untimely data		✓	
Cyber-attack	All	Data manipulation			✓
		Denial of service	✓		
Congestion	IT	Retransmissions, collisions		✓	
Device software failure	All except links	Router or IED software fails	✓		
Device software malfunction	All except links	Faulty control algorithm in IED			✓
		Bugs in routing protocol		✓	
Grid service software failure	Decision making	State estimation software crash	✓		
Grid service software malfunction	Decision making	Bugs in state estimation algorithm		✓	✓

Limited: In this state, the grid service has partial performance degradation due to certain disturbances, which has impacted its availability, timeliness and/or correctness. Disturbances that impact non-critical ICT components typically reduce the performance of a grid service without causing it to fail completely. However, depending on the disturbance, there is an increased risk of further state degradation of that grid service and other dependent ones. This state is typically characterised by disturbed communication, limiting coordination among various actors. A grid service is in a Limited state if it resorts to its fallback mode (e.g. using historical measurements when real-time field measurements are lost). The Limited state indicates high uncertainties when using the grid service, implying that the operators should use it cautiously while aiming to recover it to its Normal state. This state is similar to the Alert state of the PS (cf. Sec.2.4) and captures the graceful degradation[1] of the grid services, where it offers reduced but acceptable performance.

Failed: In this state, the grid service is no longer functional, i.e. not available, too slow/late or gives grossly incorrect results. The operator should immediately take suitable actions to restore its functionality. A grid service is said to be in its Failed

[1] Graceful degradation is the ability of a system to maintain limited functionality even when a large portion of it has been destroyed or rendered inoperative [77].

state when disturbances have impacted critical hardware or software components beyond the scope of the fallback measures.

These operational states are for individual grid services and are not aggregated into a unified set of states for the entire ICT system. This is because the relevance of grid services, especially the remedial actions, vary depending on the exact situation in the PS. For instance, in the case of a line overload, the congestion management service is required to reroute or redispatch power. Contrary, in the case of an under-voltage at a bus, the voltage control service is required to boost the voltage at that bus. Although the PS is in the Emergency state in both cases, the services required for remedy depend on the underlying disturbance. Furthermore, as discussed in Sec. 2.2.1, high-level services are always critical as they provide the situational awareness needed to activate the corresponding remedial actions.

3.3 Conceptual Model of Power-ICT Interdependencies

Fig. 3.2 shows the conceptual model of the interdependencies between PS and ICT Systems developed in this dissertation. This model uses the aforementioned properties of the ICT system from Sec. 3.1 and the operational states of ICT-enabled grid services from Sec. 3.2. On the left are the four main functions of the ICT systems, namely, measuring, actuation, data transfer and computation. Disturbances in the ICT system impacting its functions can be mapped to its properties as shown in Tab. 3.1. The three properties represent the requirements of the individual grid services on the functions of the ICT system. The operational states of each grid service can then be assessed using the corresponding set of properties, which bridge the general ICT functions with the states of specific grid services. As discussed in Sec. 2.2, the grid services can detect and counteract disturbances in PS, potentially improving the operational state. However, a state degradation of the grid service can lead to incorrect control actions in the interconnected PS, causing its state to degrade (cf. Sec 1.2). A change in PS state, by either PS disturbances or incorrect control action, is associated with certain buses gaining or losing power supply, which affects the connected ICT components by causing them to gain or lose power supply, respectively. This then affects the functions of the ICT system and, consequentially, its properties, the states of the grid services and so on, thus depicting the circular interdependence as well as propagation of disturbances between the power and ICT systems. This model can also capture both functional (i.e., the impact of the state of ICT-enabled grid services on PS operation) and structural (i.e., the physical connection of ICT components to the PS buses) interdependencies. In Fig. 3.2, the light orange arrows represent functional interdependence, whereas the grey arrow represents structural interdependence.

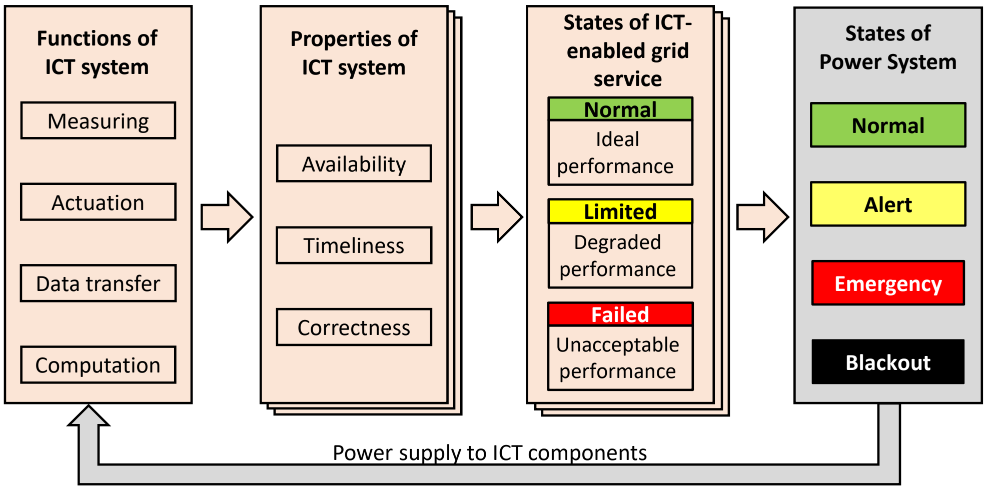


Fig. 3.2: Conceptual model of interdependencies between power and ICT systems.

3.4 Case Studies

This section presents case studies for the operational states of three ICT-enabled grid services, namely state estimation (SE), on-load tap changer-based voltage control and DER redispatch. After outlining the exemplary CPES setup considered, the operational states of the three services are discussed individually. Note that the state description of the grid services depends on their implementation and that other variations are possible.

Fig. 3.3 shows the exemplary medium voltage (MV) CPES with the three aforementioned grid services. Measurements from different parts of the grid are gathered using OT devices such as RTUs. These measurements are transmitted to the server located in the monitoring and control system [100] via the wide-area IT network with devices such as routers, links and antennas. The IT network could be both wired or wireless, with cellular being the popular option in the case of distribution grids (cf. Sec. 2.1.3). Note that the dotted lines in Fig. 3.3 represent the logical communication overlay[2]. The grid services are assumed to have a centralised architecture, i.e., run on a central server in the monitoring and control system. Here, the received measurements are first processed by the SE service. If the SE results

[2]A logical overlay network consists of virtual links, which correspond to a path, perhaps through several physical nodes and links of the underlying physical communication network

indicate an operational limit violation, the voltage control and redispatch services can be suitably deployed. The resulting setpoints are then transferred via the same IT network to the OT devices, which suitably actuate the connected PS equipment – in this case, a transformer, a photovoltaic panel and two wind turbines. Note that the measuring, data transfer, processing, and actuation have timeliness associated with them.

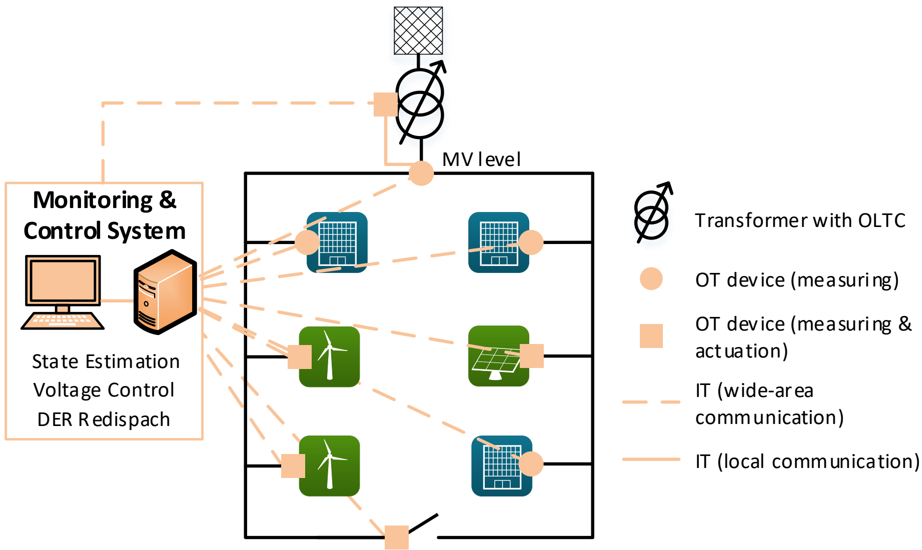


Fig. 3.3: Exemplary CPES with state estimation, OLTC-based voltage control and DER redispatch services.

The OT controllers have two operational models: remote and local. In the remote mode, these devices receive setpoints from the server via the IT network. In the absence of these setpoints, the controllers resort to the local mode of operation as a fallback, where they act solely based on local measurements. Therefore, coordinated control is no longer possible. This fallback measure is essential for capturing the intermediate level of performance and the Limited state of the grid service.

3.4.1 State Estimation

State Estimation (SE) is one of the most important high-level services, which performs real-time monitoring of PS and provides situational awareness [94]. It estimates the system state variables, namely voltage magnitude and angles, at any given time using the measurements gathered from the OT devices. Typical field measurements include active and reactive power flows, currents, voltage magnitudes and active and reactive power injections. It also uses the statuses of circuit breakers and switches to determine the current grid topology. The SE service provides situational awareness to the operator and is an integral part of its operational state assessment (cf. Sec. 2.4).

To model the operational states (or performance) of the SE service, its requirements are to be investigated. The most important requirement for central SE is the availability of the server that hosts the SE algorithm. Assuming the weighted least squares (WLS) algorithm, which is one of the most common SE algorithms [94, 101], the necessary and sufficient condition for the solvability of SE is

$$rank(H) = n^{sv}. \tag{3.1}$$

Here, H is the Jacobian matrix, calculated based on the available field measurements, and n^{sv} is the number of PS state variables [102]. A successful run of the SE requires sufficient field measurements to satisfy this condition. To have an updated situational awareness, SE is performed at fixed time intervals using the available measurements. This imposes a timeliness requirement on the field measurements to reach the server. Since the timeliness of measuring and processing are typically constant (cf. Sec. 3.1), the timeliness requirement of SE can be attributed to the timeliness of the IT network. This requirement varies depending on the implementation of the SE service, with examples being 0.1 s with PMUs and 30 s – 2 min without them [48]. Furthermore, since WLS is a deterministic algorithm, the correctness of the SE results is primarily influenced by the correctness of the input measurements. In this case, correctness is quantified by the variance of measurements. Typical SE implementations are equipped with bad data detectors that only allow measurements with a certain level of correctness to be considered. This represents the correctness requirement of the service.

ICT disturbances such as sensor failure and IT congestion may result in a complete loss or delayed arrival of certain measurements at the central server. Contrarily, disturbances such as noise interference can negatively impact the correctness. Such measurements will not be considered by the SE algorithm, which may violate the solvability condition. In this case, the solvability can be satisfied by substituting the missing measurements with corresponding pseudo-measurements [94]. This is a fallback measure that ensures solvability but also increases the uncertainties in SE results. This is because pseudo-measurements are typically calculated based on historical measurements, and therefore, recent events may not be reflected in them [103]. Note that typical SE implementations, especially in the transmission grid, have redundant measurements so that a single measurement's loss, delay or corruption does not impact its operational state [94]. The operational states of the SE service, which reflect its performance, can then be defined as follows and are summarised in Tab. 3.3.

Normal: The SE service is in the Normal state when the SE server is available and when the solvability condition is satisfied only using field measurements. This implies sufficient field measurements are transmitted to the server in time and that they are correct. In this state, the operator can confidently use the SE results for operational decisions.

Limited: The SE is in the Limited state when fallback measures, such as pseudo-measurements, are used to satisfy the solvability condition. This implies that sufficient measurements are not available, too late or discarded by the bad data detectors. In this state, the operator should use the results with caution while aiming to restore SE to the Normal state.

Failed: The SE is in the Failed state if the solvability condition cannot be satisfied even with the use of pseudo-measurements. This indicates severe disturbances causing numerous measurements to be unavailable, delayed or incorrect. Since the server is critical for a centralised SE, its failure will cause the SE service to fail unless there is a backup (or redundant) server. The Failed state represents a loss of situational awareness for the operator, which causes the PS to transition to the Emergency state (cf. Sec. 2.4).

3.4.2 On-load Tap Changer based Voltage Control

Disturbances such as power line failure and generation/load fluctuations can cause the bus voltages to vary, potentially causing over-/under-voltages. The voltage control (VC) aims to remedy such situations by restoring the bus voltages within normal operating thresholds such as the ones specified in [69] (for transmission systems) and [104] (for distribution systems). Although the VC service can be realised using several means, e.g., shunt/series capacitors and synchronous condensers [43], the on-load tap changer (OLTC) is considered here. Contrary to conventional transformers with fixed ratios, an OLTC-equipped transformer can vary its tap position during operation by dynamically adjusting its ratio, thus providing better control capabilities [105]. The voltage of the secondary side can be adjusted by suitably changing the tap position of the transformer,

An essential requirement for this VC service is the availability of the controller (cf. Fig. 3.3), which, as discussed earlier, can operate in remote and local (fallback) modes. The remote mode considers setpoints from the server, typically based on SE results [11]. This captures the dependence between the grid services in a CPES. Unlike SE with a fixed timeliness requirement, the timeliness of the VC service depends on the severity of the voltage problem, e.g., larger and faster voltage problems require faster remedies [43, 95]. The correctness of setpoints from the server can impact the performance of the VC service. However, this is challenging to detect from the OLTC controller's perspective due to its limited computational resources and view of the system. ICT disturbances can cause the remote setpoints to be unavailable, delayed or incorrect. In this case, the OLTC resorts to the local mode using the voltage measurement from the secondary side, which it receives via the local IT network, i.e., direct fibre-option connection. Note that this represents one possible implementation of this grid service. The authors in [80], for example, present an alternative OLTC implementation, which operates based on a remote measurement from voltage-wise the most critical node of the grid, in this case, the farthest bus from the transformer. This, however, can only be applied to radial feeders with a strictly decreasing voltage profile. The operational states of the VC service, which reflect its performance, can then be defined as follows and are summarised in Tab. 3.3.

Normal: The VC service is in the Normal state when the OLTC receives remote measurements (based on SE results) correctly and on time. In this state, the grid service has a wide-area view (due to SE results) and, therefore, can detect and potentially remedy voltage problems in the whole PS connected to the secondary side of the transformer.

Limited: When remote measurements are unavailable, too late or incorrect, the OLTC uses the local fallback measurement and hence, can only remedy local voltage problems, i.e., at the secondary side bus. In the case of a meshed grid with DERs, this may cause voltage problems in the other parts of the grid [106]. Therefore, the VC service must be used cautiously when in this state.

Failed: ICT disturbances such as outages of the OLTC controller, local sensor (OT) failure or local communication failure can hinder the transformer tap adjustment, especially when the grid service is already in its Limited state. This represents the Failed state of the VC service, where it cannot be used to remedy voltage problems. In this case, measures could be implemented to reset the OLTC to a default mode, e.g., mid position or rest on the last tap position [80].

3.4.3 Redispatch of Distributed Energy Resources

While the VC service considered in this dissertation involves only one controller, the redispatch service involves the coordinated control of multiple DER controllers and is also a remedial action. In the exemplary CPES shown by Fig. 3.3, the setpoints of the three DERs (two wind turbines and one PV panel) can be adjusted from the central server. These DERs can also represent aggregated flexibility units such as active distribution networks or virtual power plants. Redispatch is an essential and versatile grid service considering the ongoing renewable energy transition. It could remedy various PS disturbances such as congestion, under-frequency and over/under-voltage while also aiding economic dispatch [107].

Although multiple possible implementations exist for the redispatch service, this dissertation follows [108]. Here, the flexibility measurements from the available DER controllers are transferred to a central server. Optimisation algorithms like optimal power flow are solved based on the received measurements, resulting in the setpoint for the DERs. The objective of the algorithm is to dispatch the flexibility required for remedying the PS disturbance while keeping the PS parameters within their respective operational limits. The availability of the SE service is essential for such algorithms as they require the bus voltages [108]. Depending on the severity of the disturbance, the setpoints of the DERs are calculated by the redispatch algorithm. They are then transferred back to the available DER controllers, which then perform the required actuation on the corresponding DERs. The timeliness requirement of the redispatch service also depends on the severity of the PS disturbance it aims to remedy. In this case, it is based on the DER controllers that are reachable from the server within a specific latency. The typical timescales for PS dynamical problems are given in [43, 95], and the timeliness of an exemplary redispatch service is discussed in [107]. Since DERs have increased stochasticity due to their dependence on weather patterns, their uncertainties impact the performance of the service. The uncertainty of the DERs represents the correctness requirement. The operational states of the redispatch service, which reflect its performance, can then be defined as follows and are summarised in Tab. 3.3.

Normal: The redispatch service is in the Normal state if the PS disturbance could be remedied only by using the flexibilities of the DERs that are reachable within the timeliness requirement and have an acceptable level of correctness, i.e., DER uncertainty is below a defined threshold. In this state, the service can guarantee a remedy to the disturbance.

Limited: The redispatch service is in the Limited state if the PS disturbance could be remedied by using the flexibilities of DERs, which are reachable with the timeliness requirement but requires at least one incorrect DER, i.e., DER uncertainty is greater than a defined threshold. In this state, the grid service should be used cautiously as it does not guarantee the required flexibility due to the uncertain DERs.

Failed: The redispatch service is in the Failed state if the DER controllers required to provide flexibility are either unavailable or not reachable with the timeliness requirement, also considering the incorrect DERs. The failure of the SE service will also cause the redispatch service to fail due to its dependencies. This state indicates that the DERs cannot be used to remedy the PS disturbance under consideration. Note that the local mode of DER controllers is not used in this case study so as to show the application of the developed operational states for different implementations of grid services.

An alternative definition for the states of redispatch service, based on data loss (availability), data delay (timeliness) and corruption of measurement and control data (correctness), is presented in [107] and is shown in Tab. 3.2. These properties are quantified by percentage loss rate, communication latency (T_{tot}) and variance of measurements (σ_{meas}), respectively. The redispatch service in [107] represents a frequency control reserve provider aiming to provide active power flexibility. Here, data delay is simulated by varying the measuring and actuation delays (cf. Fig. 3.1). Data loss and data corruption are simulated by varying the loss rate of the control signal and by adding Gaussian noise to the control signal, respectively. For each value of data delay, data loss and data corruption, 100 simulations with different random seeds are performed. State transitions are triggered when the settling time of the controller's response exceeds $30\,\mathrm{s}$. based on which the thresholds in Tab. 3.2 are defined. The Normal state indicates that all simulation runs within those thresholds have a settling time of less than $30\,\mathrm{s}$, whereas the Limited state indicates that some of the runs within those thresholds can have a settling time greater than $30\,\mathrm{s}$. The Failed state indicates that most runs in those thresholds have settling time greater than $30\,\mathrm{s}$. Although these thresholds are specific to the implementation of the service in [107], this demonstrates the applicability of the proposed operational states to different implementations of the redispatch service.

Tab. 3.2: Operational state description of redispatch service based on data loss, delay and measurement corruption from [107].

Properties / States	Data loss (availability)	Delayed data (Timeliness)	Measurement corruption (correctness)
Normal	Loss Rate < 70%	$T_{tot} \leq 0.9s$	$\sigma_{meas} \leq 0.01$
Limited	70% < Loss Rate < 85%	$0.9s < T_{tot} \leq 1.0s$	$0.01 < \sigma_{meas} \leq 0.025$
Failed	Loss Rate > 85%	$T_{tot} > 1.0s$	$\sigma_{meas} \geq 0.025$

3.5 Chapter Summary

This chapter conceptualises the operational states of the ICT-enabled grid services, a core element for both the artefacts of this dissertation. The contributions in this chapter can be summarised as follows:

- Three properties of the ICT system, namely availability, timeliness and correctness, have been identified. They represent the requirements of the grid services while also capturing the impact of various ICT disturbances on the ICT system. These properties are specific to each grid service, and a grid service need not necessarily have requirements based on all three of them.
- Novel operational states for ICT-enabled grid services for capturing their performance have been conceptualised. The definitions and assessment of these states, namely Normal, Limited and Failed, have been discussed. These states can be based on the aforementioned ICT properties and are not aggregated for the whole ICT system as different grid services have different importance regarding PS operation. The Limited state aims to capture the graceful degradation of ICT systems, where they offer a reduced by acceptable performance.
- A conceptual model of the interdependence between power and ICT systems has been outlined. The states of ICT-enabled grid services represent the functional dependence, while electric power supply to ICT components represents the structural dependence. The conceptual model shows how the operational states of power and ICT systems impact each other.

- Based on an exemplary CPES, the proposed operational states have been applied to three case studies of grid services, and their operational states have been discussed. These case studies are chosen to represent both high-level services and remedial actions and are summarised in Tab. 3.3. The state definitions are specific to a grid service and its implementation.

Tab. 3.3: Operational states of state estimation, OLTC-based voltage control and DER redispatch services.

	State Estimation (High-level service)	**OLTC-based voltage control (Remedial action)**	**DER redispatch (Remedial action)**
Normal	▪ Solvability condition satisfied using only field measurements ▪ SE gives correct estimates, which can be used for decision-making	▪ OLTC controller has wide-area view based on SE results from the monitoring and control system ▪ Can detect and possibly remedy voltage problems in the whole grid	▪ Required flexibility can be provided with available, reachable on time and correct DERs ▪ Guarantee remedy for the PS disturbance
Limited	▪ Solvability condition satisfied using both field and pseudo-measurements (fall-back) ▪ Potentially incorrect SE results as pseudo-measurements are based on historical data ▪ Use SE results for decision-making but with caution	▪ SE results not available at OLTC – Operate based on local measurements (fall-back) ▪ Detect and possibly remedy only local voltage problems ▪ Tap decision potentially wrong in meshed grids – Use the VC grid service with caution	▪ Required flexibility can be provided only by using at least one incorrect DER ▪ No guaranteed remedy for the PS disturbance as the required flexibility is not guaranteed – Use the grid service with caution
Failed	▪ Solvability condition cannot be satisfied or SE server unavailable ▪ Loss of situational awareness – Cannot take decisions using SE results – restore this grid service	▪ OLTC controller failure or unavailability of both local and remote measurements ▪ OLTC cannot remedy voltage problems – use alternative remedial actions and restore this grid service	▪ Required flexibility cannot be provided by DERs available and reachable in time ▪ DER redispatch cannot be used to remedy the PS disturbance – use alternative remedial actions and restore this grid service

4 Joint Operational State Model for CPESs

Using the concepts from Chapter 3, this chapter formally models the interdependence between the power and ICT systems considering their operational states. The formal description of CPESs with power and ICT systems is presented, followed by their respective operational state models. This is followed by the formal modelling of the joint operational states of CPESs, which contributes to RQ1 of this dissertation. Since this dissertation focuses on the ICT system with the grid services, its modelling is presented in more detail than that of the PS. An early version of the contents of this chapter is published in [39]. Note that, as mentioned in Sec. 1.6, the operational decisions based on optimal power flow (Sec. 4.4.4) and the impact of operational decisions (Sec. 4.4.5) are the focus of Marcel Klaes at the TU Dortmund university. Therefore, these concepts are only briefly summarised in this chapter.

4.1 Formal Description of CPESs

This section formally describes a CPES with its encompassing power and ICT systems. Property graph formulation is used since the literature review indicated it as a suitable approach (cf. Sec. 2.6.3). The property graph model used in this dissertation is adopted from [109].

The PS is modelled in static steady-state with components such as buses (representing substations), power lines, OLTC transformers, DERs and loads. The DERs are assumed to be controllable with flexible active P^G and reactive power Q^G injections. Both controllable and uncontrollable loads are considered. Uncontrollable loads have fixed active P^D and reactive power Q^D demands, whereas the power demands of controllable loads are in $[0, P^D]$ and $[0, Q^D]$. Transformers are denoted by T with a tap position $tp^{T,min} \leq tp^T \leq tp^{T,max}$. The PS can be represented as an undirected property graph $\mathcal{G}^P = (B, C, a, d)$, where

- B is a finite set of nodes representing buses;
- C is a finite set of edges representing the power lines between the buses;

- $a : C \to (B \times B)$ is a total function that associates each power line $c \in C$ with a pair of unordered buses in B, e.g., $a(c_1) = (b_1, b_2)$ indicates that power line c_1 connects buses b_1 and b_2. This function captures the PS topology.

- $d : (B \cup C) \times PR^P \to SET^+(V^P)$ is a partial function that associates the buses and lines with properties PR^P, and for each property, the function assigns a set of values from V^P. Given a property $(ow, pr) \in (B \cup C) \times PR^P$ and the assignment $d(ow, pr) = \{v_1^P, \ldots, v_n^P\}$, a single property can be represented as $(ow, pr) = v_i^P$ with $1 \leq i \leq |B \cup C|$. Here, ow, pr and v^P represent PS components, property name and property value, respectively.

Let Y be the admittance matrix of order $B \times B$ describing the PS topology. Then $\forall i, j \in B$, the term $y_{ij} \in Y$ represents self admittance if $i = j$ and mutual admittance if $i \neq j$. Detailed information on the construction and characteristics of an admittance matrix can be found in [43, 95]. Two disconnected buses i and j have $y_{ij} = 0$. Therefore, a relationship connecting Y and the function a can be defined as $\exists (i, j) \in C \leftrightarrow y_{ij} \neq 0$, i.e., an edge exists if and only if the corresponding element in the admittance matrix is not zero.

The set $d^B = \{P^G, Q^G, P^D, Q^D, t^T, y_b\}$ represents the properties of a PS node. Here, the generation and demand at the buses are aggregated, t^T is associated with the bus on the secondary side, and y_b represents the self-admittance of the bus $b \in B$. The set $d^C = \{y_c\}$ represents the properties of a PS edge, where y_c represents the mutual admittance of the buses connected by the PS edge $c \in C$, given by $a(c)$. Disturbances (e.g., open and short circuits) and remedial actions (e.g., opening and closing switches) that change the PS topology can be modelled by modifying the corresponding y_b and y_c. For a given grid, P^G, Q^G, P^D, Q^D, Y, t^T, y_b and y_c are the parameters that can be directly controlled. In contrast, bus voltages v_b $\forall b \in B$ and lines loadings l_c $\forall c \in C$ can be calculated based on the controllable parameters and power flow calculations [95].

Each PS bus can be connected to a sensor, router, server and/or actuator, all of which are ICT components. These components receive a power supply from the connected bus. In this dissertation, the ICT system is modelled as an undirected property graph $\mathcal{G}^I = (N, E, \alpha, \kappa, \pi)$. Here:

- N is a finite set of nodes representing ICT components;

- E is a finite set of edges between the nodes;

- $\alpha : E \to (N \times N)$ is a total function that associates each edge $e \in E$ with a pair of unordered nodes in N, e.g., $\alpha(e_1) = (n_1, n_2)$ indicates that edge e_1

connects nodes n_1 and n_2. α represents the incidence function of a graph and can be computed using a graph's adjacency (or connection) matrix.

- $\kappa : N \rightarrow SET^{+}(B)$ is a partial function that associates an ICT node with a set of PS buses, from which it receives a power supply. For example, $\kappa(n) = \{b\}$ indicates that the ICT node n receives power supply from the bus b. Note that ICT nodes, such as wireless base stations, can receive power from multiple buses. Additionally, $\kappa(n) = \{\phi\}$, i.e., a null set, indicates an alternate source, such as a battery, powers the node n.

- $\pi : (N \cup E) \times PR^{I} \rightarrow SET^{+}(V^{I})$ is a partial function that associates ICT nodes and edges with properties PR^{I}, and for each property, it assigns a set of values from V^{I}. This notation is similar to the function d in the aforementioned PS graph $\mathcal{G}^{\mathcal{P}}$.

Note that $\mathcal{G}^{\mathcal{I}}$ considers only the topological aspects of the ICT system and not the flow of data. The set $\pi^{N} = \{\psi, \rho, \eta, \xi, \epsilon, \sigma, \delta\}$ represents the properties of an ICT node, where $\rho \geq 0$ denotes the number of PS parameters measured by that node and $\sigma \in [0, 1]$ is a float denoting the correctness of the measurements from the ICT node. Here, $\sigma = 1$ indicates that the measurement is the same as the ground truth. Since correctness can be influenced by hardware, all measurements from a particular node are assumed to have the same σ. The properties ξ, ϵ, and η are binary and denote whether the corresponding node is a server ξ, an actuator η and/or a routing device ϵ, respectively. Note that an ICT node can have one or more of these functionalities.

The property ψ is also a binary denoting an ICT node's availability, which can be affected by power supply loss and ICT disturbances. An ICT node n is unavailable when the interconnected bus b has no voltage, i.e.,

$$v_b \leq 0.6\,\text{p.u.} \land \kappa(n) = \{b\} \rightarrow \pi^{N}(n, \psi) = 0. \tag{4.1}$$

A bus is assumed to have lost its voltage if $V_b \leq 0.6\,\text{p.u.}$ [73]. This equation captures the structural (or physical) dependence of the ICT system on the PS. ICT disturbances, such as hardware failures, can cause ICT nodes to become unavailable, i.e., $\pi^{N}(n, \psi) = 0$, irrespective of the voltage of the interconnected bus.

As discussed in Sec. 3.1, queuing and processing delays constitute the majority of an ICT node's timeliness. In this regard, the property δ is a float representing the timeliness as the sum of queuing and processing delays in milliseconds. While all nodes can have processing delays, only the nodes with routing capabilities, i.e., $\pi^{N}(n, \epsilon) = 1$, can have queuing delays.

The set $\pi^E = \{\psi, \delta\}$ represents the properties of an ICT edge. Similar to nodes, ψ represents the availability of edges. Since edges do not require a power supply, Eq. 4.1 does not apply to edges. Therefore, an edge $e \in E$ can only become unavailable, i.e., $\pi^E(e, \psi) = 0$ due to ICT disturbances (e.g., fibre optic cable damage). Furthermore, the δ for edges represents their serialisation and propagation delays in milliseconds.

Fig. 4.1 illustrates an example of power and ICT graphs along with their properties. The left side of the figure shows an example PS with the interconnected ICT system, and on the right are the corresponding graph representations. Some examples of nodes, edges and their properties are as follows:

- The PS nodes b_1 and b_2 have properties $d(b_1) = \{20\,\text{kW}, 10\,\text{kVAr}, 0, 0, 2, 1.1\,\text{p.u.}\}$ and $d(b_2) = \{0, 0, 22\,\text{kW}, 18\,\text{kVAr}, 0, 0.8\,\text{p.u.}\}$, respectively. This indicates that the b_1 has a generation of $P^G = 20\,\text{kW}$, $Q^G = 10\,\text{kVAr}$ and transformer with tap at $t_p^T = 2$ associated with it. The node b_2 has consumption of $P^D = 22\,\text{kW}$, $Q^D = 18\,\text{kVAr}$ associated with it. The self admittances of b_1 and b_2 are $1.1\,\text{p.u.}$ and $0.8\,\text{p.u.}$.

- The parallel power lines c_1 and c_2 are defined as $a(c_1) = (b_1, b_2)$ and $a(c_2) = (b_1, b_2)$ with properties $d(c_1) = \{1.8\,\text{p.u.}\}$ and $d(c_2) = \{1.8\,\text{p.u.}\}$. This indicates that they connect buses b_1 and b_2, which have a total mutual admittance of $3.6\,\text{p.u.}$.

- The nodes n_1 and n_2 represent IEDs with properties $\pi_1^N = \{1, 2, 1, 0, 0, 0.05, 50\,\text{ms}\}$ and $\pi_2^N = \{1, 4, 0, 0, 0, 0.05, 20\,\text{ms}\}$. This indicates that both nodes are available and measure two and four PS parameters, respectively, with a correctness of 0.05. Node n_1 actuates a PS equipment (i.e., OLTC), whereas n_2 has no actuation. The timeliness of n_1 is $50\,\text{ms}$ and that of n_2 is $20\,\text{ms}$. Also, the power supply to the nodes can be represented as $\kappa(n_1) = \{b_1\}$ and $\kappa(n_2) = \{b_2\}$.

- The node n_3 with properties $\pi_3^N = \{1, 0, 0, 0, 1, 0, 100\,\text{ms}\}$ represents a router. The properties indicate that it is available and has routing capabilities with timeliness of $100\,\text{ms}$.

- The edges e_1 and e_2 have properties $\pi_1^E = \{1, 30\,\text{ms}\}$ and $\pi_2^E = \{1, 60\,\text{ms}\}$. This indicates that they are both available and have timeliness of $30\,\text{ms}$ and $60\,\text{ms}$, respectively. Additionally, $\alpha(e_1) = (n_1, n_3)$ and $\alpha(e_2) = (n_2, n_4)$ represent the nodes associated with the edges.

The availability of a communication path is essential for transferring data between ICT components. Let $\Omega_{ij} = \{\omega_1, \omega_2, \dots\}$ be the set of all possible paths between

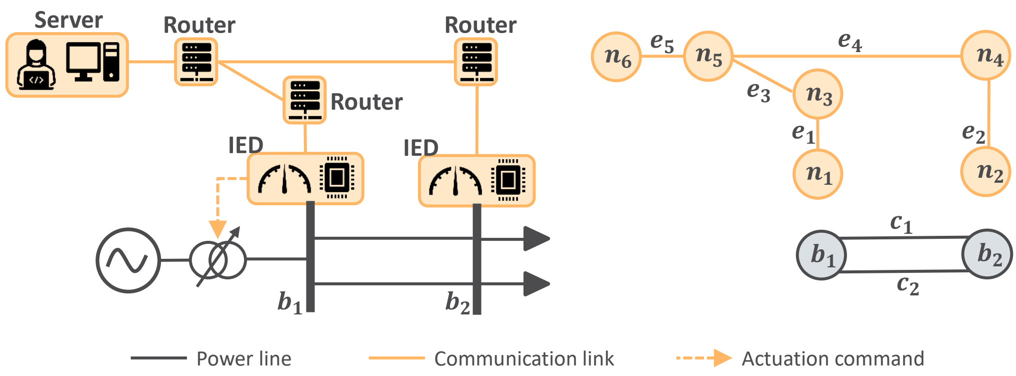


Fig. 4.1: Example of power and ICT system (left) with their graph representation (right).

nodes i and j. Each path $\omega \in \Omega$ is of the form $(i, \ldots, a, \ldots, j)$, where $i, a, j \in N$. An essential condition for any node $n \in N$ to be a part of a path ω is its availability, i.e., $\pi^N(n, \psi) = 1$. If i and j are adjacent, the path reduces to $\omega = (i, j)$ and is equivalent to the edge between them, i.e., $(i, j) \in E$. Then any node, for instance, a server, is said to be in a path ω if

$$\exists\, \omega \in \Omega_{ij} \text{ s.t. } k \in \omega \wedge \pi^N(k, \xi) = 1. \tag{4.2}$$

Here, the term $\pi^N(k, \xi) = 1$ is to ensure that the node k is a server. This description can be extended to represent any ICT node by using its corresponding property. Eq. (4.2) also captures the possibility of redundant communication paths since the same components will be a part of the redundant paths. Although multiple paths can exist between two nodes, in the remainder of this dissertation, $(i, \ldots, a, \ldots, j) = \omega_{ij}$ is defined as the set of nodes that represents the shortest path in terms of the end-to-end delay (timeliness) between source node i and destination node j. This is because typical routing protocols, e.g., open shortest path first (OSPF), transfer data over the shortest path available [42]. Let $\mathcal{G}^I[\omega_{ij}]$ be a subgraph of $\mathcal{G}^I$ consisting of the nodes in ω_{ij} and the edges of $\mathcal{G}^I$ that connect the nodes in ω_{ij}. Then, this set of edges of $\mathcal{G}^I[\omega_{ij}]$ can be defined as $E_{ij} = \{(a, b) \in E \mid a, b \in \omega_{ij}\}$, where E is the edges of $\mathcal{G}^I$. Similar to the case of nodes, the availability is an essential condition for any edge $e \in E_{ij}$ to be a part of path ω_{ij}, i.e., $\pi^E(e, \psi) = 1$. Assuming the open shortest path first routing, the end-to-end delay between the two ICT components δ_{ij} can thus be calculated as the sum of the delays of the nodes and edges in the shortest path ω_{ij}:

$$\delta_{ij} = \sum_{c \in \omega_{ij}} \pi^N(c, \delta) + \sum_{d \in E_{ij}} \pi^E(d, \delta) \tag{4.3}$$

A delay of zero $\delta_{ij} = 0$ indicates that the communication is local, e.g., a controller j receiving measurements from a sensor i located on the same unit. An infinite delay $\delta_{ij} = \infty$ indicates no available path between the two nodes. Furthermore, the correctness of data (measurements or setpoints) from a node i is influenced by all the nodes in the path ω_{ij} to the destination node j. This can be calculated as

$$\sigma(\omega_{ij}) = \sum_{x=i}^{j} \pi^N(x, \sigma). \tag{4.4}$$

Here, σ is the variance and is the metric used for correctness. The total correctness is then the sum of the correctnesses of all components in the path ω_{ij}, through which the data traverses. Note that the summation in Eq. (4.4) should be adapted accordingly when other metrics are used for correctness instead of variance. For example, the authors in [55] use trust as a metric for correctness, where the overall trust is regarded as the minimum trust of the components in the path.

4.2 Operational State Model of ICT-enabled Grid Services

This section presents the formal operational state model of ICT-enabled grid services using the property graph representation from Sec. 4.1. The modelling is done using finite state automata since the literature review (cf. Sec. 2.6.3) indicated it as a suitable approach to model discrete states and transitions among them. Furthermore, the automaton model suits the discrete-event nature of the ICT system. In the following, the models for SE and VC services are presented based on Secs. 3.4.1 and 3.4.2. The three properties, i.e., availability, timeliness and correctness, are first formalised, followed by the finite state automaton to assess the operational states of the grid services based on the properties. The fundamentals of finite state automata can be found in [110].

4.2.1 Finite State Automaton of State Estimation

This modelling is based on the centralised SE service discussed in Sec. 3.4.1. The server is the most critical component, without which the grid service fails. The set of available servers suitable for SE ($\Phi^{\xi,SE}$) can be determined by

$$\Phi^{\xi,SE} = \{i \in N \mid \pi^N(i, \psi) = 1 \wedge \pi^N(i, \xi) = 1\}. \tag{4.5}$$

This equation also captures the possibility of redundant servers. The server receives measurements from field sensors if the corresponding sensors are available (availability) and a communication path exists between the sensor and the server(reachability). The set of sensors available (Φ^{ρ}) at any instant of time in the ICT system can be determined by

$$\Phi^{\rho} = \{s \in N \mid \pi^N(s, \psi) = 1 \wedge \pi^N(s, \rho) > 0\} \tag{4.6}$$

and the reachability of an available sensor $s \in \Phi^{\rho}$ from the server $p \in \Phi^{\xi,SE}$ can be calculated as

$$\exists\, \omega_{ps} \text{ s.t. } \pi^N(p, \xi) = 1 \wedge \pi^N(s, \rho) > 0. \tag{4.7}$$

As discussed in Sec. 3.4.1, the SE service has timeliness and correctness requirements for the field measurements. Let $\delta^{th,SE}$ and $\sigma^{th,SE}$ be the thresholds for the timeliness and correctness of measurements, respectively. The end-to-end delay for the measurements from each available sensor $\forall s \in \Phi^{\rho}$ to an available server $p \in \Phi^{\xi,SE}$ can be calculated using Eq. (4.3) as δ_{sp}. Based on the timeliness requirement, only the measurements with $\delta_{sp} \leq \delta^{th,SE}$ will be considered by the SE algorithm. The correctness is then evaluated for these measurements. A similar threshold comparison is performed, typically by the bad data detectors using Eq. (4.4), to identify field measurements with low correctness. Measurements from a node s are considered incorrect and are discarded if $\sigma(\omega_{sp}) > \sigma^{th,SE}$. In summary, for evaluating the rank condition (cf. Eq. (3.1)), the SE algorithm will consider only the field measurements that reach the server and satisfy the timeliness and correctness conditions. These measurements can be defined as

$$\begin{aligned}\Phi^{\rho,SE} =& \{s \in \Phi^{\rho} \mid \pi^N(s, \psi) = 1 \;\wedge\; \pi^N(s, \rho) > 0 \;\wedge\; \delta_{sp} \leq \delta^{th,SE} \;\wedge \\ & \sigma(\omega_{sp}) < \sigma^{th,SE} \;\wedge\; p \in \Phi^{\xi,SE}\}.\end{aligned} \tag{4.8}$$

The impact of ICT disturbances on the ICT system and, consequentially, the grid services can be captured by first appropriately modifying the property graph $\mathcal{G}^I$ and then using Eqs. (4.5)-(4.8). As shown in Tab. 3.1, common ICT disturbances can be mapped to the availability, timeliness and correctness properties. Failure of an ICT component can be modelled by setting the corresponding ψ property to zero, which will then impact its availability. It can also be achieved by removing the corresponding node or edge in $\mathcal{G}^I$. For example, Eqs. (4.5), (4.6) and (4.7) capture the failure (or unavailability) of sensors, servers and communication paths, respectively. Disturbances such as IT component failures and congestion can impact the end-to-end delay of data transfer. This can be modelled by modifying the corresponding δ property, which will, in turn, impact Eqs. (4.3) and (4.7). Disturbances impacting the correctness can be modelled by modifying the corresponding σ property, affecting Eq. (4.4). Furthermore, some disturbances can impact multiple properties. For example, in case of an IT link failure, a new path will be calculated for the sensors based on Eq. (4.7), which may have a new end-to-end delay (Eq. (4.3)) as well as correctness (Eq. (4.4)). The modified graph G^I_{new}, along with its properties, reflect the new state of the ICT network.

An essential aspect of finite state automata is their guard conditions based on which state transitions are triggered. To derive these guards, grid service-specific piecewise continuous functions f are designed based on the availability, timeliness and correctness properties. The centralised SE service requires at least one server to be available. The corresponding function can be written as

$$f^{\xi,SE} = \begin{cases} 1 & |\Phi^{\xi,SE}| \geq 1 \\ 0 & \text{otherwise.} \end{cases} \tag{4.9}$$

Let $h : M \rightarrow H$ be a function that computes the Jacobian matrix H based on a set of measurements M. The necessary and sufficient condition for the solvability of SE is $rank(H) = n^{sv}$, where n^{sv} is the number of state variables (cf. Eq. (3.1)). The SE is in its Normal state when this condition is satisfied only using field measurements that are available on time and correct given by Eq. (4.8), i.e., $M \subseteq \Phi^{\rho,SE}$. This can be formalised as

$$f^{1,SE} = \begin{cases} 1 & (rank(H) = n^{sv}) \wedge M \subseteq \Phi^{\rho,SE} \\ 0 & \text{otherwise.} \end{cases} \tag{4.10}$$

If the solvability condition cannot be satisfied only using field measurements, a suitable set of pseudo-measurements, denoted by Φ^{PM}, could be used. The SE service is in its Limited state when the solvability condition is satisfied only by using both field measurements and pseudo-measurements. This can be defined as

$$f^{2,SE} = \begin{cases} 1 & (rank(H) = n^{sv}) \ \wedge \ M \subseteq (\Phi^{\rho,SE} \cup \Phi^{PM}) \ \wedge \ M \not\subseteq \Phi^{\rho,SE} \\ 0 & \text{otherwise.} \end{cases} \tag{4.11}$$

If $rank(H) \ll n^{sv}$, the maximum number of pseudo-measurements that can be used to achieve convergence depends on its implementation since it is futile to run SE when several field measurements are unavailable on time or incorrect. Furthermore, the SE service is in its Failed state when the solvability condition cannot be satisfied even with the field and pseudo measurement or if the SE server has failed. The automaton of the SE service can now be written as a quadruple

$$A^{SE} = (S^{SE}, \Lambda^{SE}, s_0^{SE}, G^{SE}), \tag{4.12}$$

where

$$\begin{aligned}
S^{SE} &= \{N, L, F\},\\
\Lambda^{SE} &= \{\lambda^{SE,NL}, \lambda^{SE,NF}, \lambda^{SE,LF}, \lambda^{SE,FN}, \lambda^{SE,FL}, \lambda^{SE,LN}\},\\
s_0^{SE} &= N,\\
G^{SE} &= \{g^{SE,NL}, g^{SE,NF}, g^{SE,LF}, g^{SE,FN}, g^{SE,FL}, g^{SE,LN}\},\\
g^{SE,NL} &:= f^{2,SE} \wedge f^{\xi,SE},\\
g^{SE,NF} &:= \neg f^{1,SE} \wedge \neg f^{2,SE} \vee \neg f^{\xi,SE},\\
g^{SE,LF} &:= \neg f^{1,SE} \wedge \neg f^{2,SE} \vee \neg f^{\xi,SE},\\
g^{SE,FN} &:= f^{1,SE} \wedge f^{\xi,SE},\\
g^{SE,FL} &:= \neg f^{1,SE} \wedge f^{2,SE} \wedge f^{\xi,SE},\\
g^{SE,LN} &:= f^{1,SE} \wedge f^{\xi,SE}.
\end{aligned}$$

Here, S^{SE} is the discrete states of the SE service, i.e., Normal (N), Limited (L), Failed (F), Λ^{SE} is the set of allowed state transitions, S^{SE} denotes the initial state and G^{SE} is the set of guard conditions associated with each transition in Λ^{SE}. A transition $\lambda^{SE,ss'} \in \Lambda^{SE}$ from a state $s \in S^{SE}$ to a state $s' \in S^{SE}$ can be defined as $\lambda^{SE,ss'} : s \xrightarrow{[g^{SE,ss'}]} s'$. The service is initially assumed to be in the undisturbed state, i.e., Normal. Fig. 4.2 shows the general representation of the finite state automaton of ICT-enabled grid services with the three states, six transitions and the corresponding guard conditions. Disturbances can cause the state to degrade, i.e., NL, NF, LF, and recovery actions can cause the state to improve, i.e., LN, FN, FL. Using this model, the impact of disturbances and recovery actions on the state of SE service can be analysed.

4.2.2 Finite State Automaton of Voltage Control

This modelling is based on the OLTC-based voltage control service discussed in Sec. 3.4.2 and follows the same structure as that of the SE service in the previous section. The properties for the VC service, along with the grid service-specific piece-wise continuous functions f required for the guard conditions, are first presented, followed by the automaton.

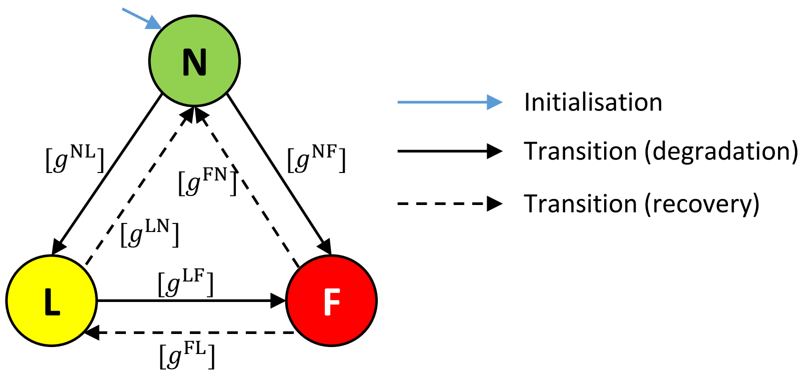


Fig. 4.2: Finite state automaton of an ICT-enabled grid service with three states.

Like the server for the SE service, the OLTC controller is a critical component of the VC service. The availability of the controller ($\Phi^{\eta,VC}$) can be determined similarly to Eq. (4.5) as

$$\Phi^{\eta,VC} = \{i \in N \mid \pi^N(i,\psi) = 1 \ \wedge \ \pi^N(i,\eta) = 1\}. \tag{4.13}$$

To perform the actuation, the VC service requires at least one controller to be available. The corresponding function can be defined as

$$f^{\eta,VC} = \begin{cases} 1 & |\Phi^{\eta,VC}| > 0 \\ 0 & \text{otherwise.} \end{cases} \tag{4.14}$$

The VC service is said to be in the Normal state if the OLTC controller receives setpoints based on SE results from the control room server. This requires the SE service to be in either Normal or Limited (i.e., not Failed) state and the existence of a valid path between the SE server and the OLTC controller. The former can be formulated as

$$f^{1,VC} = \begin{cases} 1 & s^{SE} = N \vee s^{SE} = L \\ 0 & \text{otherwise.} \end{cases} \tag{4.15}$$

This equation captures the dependence of the remedial actions on the high-level services. Actuating the OLTC controller based on SE results when the SE service in the Limited state ($s^{SE} = L$) is a design trade-off as, on the one hand, it can potentially remedy the voltage problems in the whole PS, but on the other, relies on potentially uncertain SE results as pseudo-measurements are used.

Let $\delta^{th,VC}$ and $\sigma^{th,VC}$ be the thresholds for the timeliness and correctness of measurements, respectively. Then, a valid communication path ω_{pr} from the SE server, i.e., $p \in \Phi^{\xi,SE}$ to the OLTC controller $r \in \Phi^{\eta,VC}$ should have $\delta_{pr} \leq \delta^{th,VC}$ and $\sigma(\omega_{pr}) \leq \sigma^{th,VC}$. This can be formalised as

$$f^{2,VC} = \begin{cases} 1 & \exists\, \omega_{pr} \text{ s.t. } \pi^N(p,\xi) = 1 \wedge \pi^N(r,\eta) = 1 \wedge \\ & \quad \delta_{pr} \leq \delta^{th,VC} \wedge \sigma(\omega_{pr}) \leq \sigma^{th,VC} \\ 0 & \text{otherwise.} \end{cases} \tag{4.16}$$

Contrary to the case of the SE service, estimating the correctness of the received set-points at the OLTC controller is challenging as controllers typically have neither the computational resources nor the intelligence to run bad data detection algorithms. This is part of the future work on the dissertation.

The OLTC controller resorts to using local measurements when remote setpoints are unavailable due to violation of either Eq. (4.15) or Eq. (4.16). The availability of the local measurement is given by

$$\Phi^{\rho,loc} = \{i \in N \mid \pi^N(i,\psi) = 1 \wedge \pi^N(i,\rho) \geq 1\}. \tag{4.17}$$

and the corresponding function, which has to be satisfied for the controller to use local measurement $l \in \Phi^{\rho,loc}$, is

$$f^{3,VC} = \begin{cases} 1 & \exists\, \omega_{lr} \text{ s.t. } \delta_{lr} \leq \delta^{th,VC} \wedge \sigma(\omega_{lr}) \leq \sigma^{th,VC} \wedge \\ & \quad |\Phi^{\rho,loc}| \geq 1 \\ 0 & \text{otherwise.} \end{cases} \tag{4.18}$$

Eqs. (4.13)-(4.18) can be used to map the impact of various ICT disturbances on the ICT graph $\mathcal{G}^I$ and consequentially, on the VC service. Using these equations, the finite state automaton of the VC service can be written as a quadruple

$$A^{VC} = (S^{VC}, \Lambda^{VC}, s_0^{VC}, G^{VC}), \tag{4.19}$$

where

$$\begin{aligned} S^{VC} &= \{N, L, F\}, \\ \Lambda^{VC} &= \{\lambda^{VC,NL}, \lambda^{VC,NF}, \lambda^{VC,LF}, \lambda^{VC,FN}, \lambda^{VC,FL}, \lambda^{VC,LN}\}, \\ s_0^{VC} &= N, \\ G^{VC} &= \{g^{VC,NL}, g^{VC,NF}, g^{VC,LF}, g^{VC,FN}, g^{VC,FL}, g^{VC,LN}\}, \end{aligned}$$

$$
\begin{aligned}
g^{VC,NL} &:= \neg(f^{1,VC} \vee f^{2,VC}) \wedge f^{3,VC} \wedge f^{\eta,VC}, \\
g^{VC,NF} &:= \neg(f^{1,VC} \vee f^{2,VC}) \wedge \neg f^{3,VC} \vee \neg f^{\eta,VC}, \\
g^{VC,LF} &:= \neg(f^{1,VC} \vee f^{2,VC}) \wedge \neg f^{3,VC} \vee \neg f^{\eta,VC}, \\
g^{VC,FN} &:= f^{1,VC} \wedge f^{2,VC} \wedge f^{\eta,VC}, \\
g^{VC,FL} &:= \neg(f^{1,VC} \vee f^{2,VC}) \wedge f^{3,VC} \wedge f^{\eta,VC}, \\
g^{VC,LN} &:= f^{1,VC} \wedge f^{2,VC} \wedge f^{\eta,VC}, \\
\lambda^{VC,ss'} &: s \xrightarrow{[g^{VC,ss'}]} s' \text{ with } s, s' \in S^{VC}.
\end{aligned} \tag{4.20}
$$

The definitions of these variables are the same as Eq. (4.12). The general finite state automaton in Fig. 4.2 also applies to the VC service. Based on the ICT graph and its properties, this model can be used to assess the impact of disturbances and recovery actions on the VC service. Furthermore, due to Eq. (4.15), this model can also determine how the state change in a grid service can impact other dependent ones, i.e., the propagation of disturbances between ICT-enabled grid services.

4.3 Operational State Model of the Power System

This section presents the finite state automaton model for a PS based on the ENTSO-E operational states, which is discussed in Sec. 2.4.2. The primary condition for the PS to be in Normal or Alert states is if all bus voltages (v), line loadings (l) and frequency (fr) are within their respective operational limits. While regulating bodies such as [69, 104] specify these limits in detail, this dissertation considers a simplified set of operational limits. The limits for v and l are assumed to be $\pm 5\%$ (i.e., 1 ± 0.05 p.u.) and $\leq 80\%$, respectively. For fr, a deviation of ± 50 mHz for the Normal state and ± 200 mHz for the Alert state are considered based on [69]. These limits can differ depending on the grid and voltage level and can be formalised using the following functions:

$$
f^{v,PS} = \begin{cases} 1 & 0.95 \leq v_b \leq 1.05, \ \forall b \in B \\ 0 & \text{otherwise.} \end{cases} \tag{4.21}
$$

$$
f^{l,PS} = \begin{cases} 1 & l_c \leq 0.80, \ \forall c \in C \\ 0 & \text{otherwise.} \end{cases} \tag{4.22}
$$

$$f_N^{fr,PS} = \begin{cases} 1 & 49.95 \leq fr \leq 50.05 \\ 0 & \text{otherwise.} \end{cases} \tag{4.23}$$

$$f_A^{fr,PS} = \begin{cases} 1 & 49.8 \leq fr < 49.95 \ \vee \ 50.05 < fr \leq 50.2 \\ 0 & \text{otherwise.} \end{cases} \tag{4.24}$$

Another condition for the PS to be in the Alert state is if there is at least one contingency in the contingency list, which cannot be remedied by the available remedial actions. This is determined by the contingency analysis, as described in Sec. 2.4.1. Since this analysis is a complex computational process with several system-specific information (e.g., current state, past disturbances, contingencies along with their probabilities), it is regarded as a black box for the modelling in this dissertation. $CA = 1$ implies a positive result of the contingency analysis, which would cause the PS to transition into the Alert state.

$$f^{CA,PS} = \begin{cases} 1 & CA = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{4.25}$$

The PS is in the Emergency state if the operational limits in Eqs. (4.21) - (4.24) are violated or if there is a loss of a high-level service. The latter captures the functional dependence of the PS on the ICT system, which, in this case, is represented by the state of the SE service.

$$f^{HLS,PS} = \begin{cases} 1 & s^{SE} = N \vee s^{SE} = L, \\ 0 & \text{otherwise.} \end{cases} \tag{4.26}$$

The PS is in the Blackout state if more than 50% of the buses lose their voltage, i.e., $\leq 0.6\,$p.u. (cf. Sec. 2.4.2). This can be formulated as

$$f^{lo,PS} = \begin{cases} 1 & 0.5|B| > |\{b \in B | v_b \leq 0.60\}| \\ 0 & \text{otherwise.} \end{cases} \tag{4.27}$$

Using the functions from Eqs. (4.21)-(4.27), the finite state automaton for PSs can be written as

$$A^{PS} = (S^{PS}, \Lambda^{PS}, s_0^{PS}, G^{PS}), \tag{4.28}$$

where

$$
\begin{aligned}
S^{PS} &= \{N, A, E, B\},\\
\Lambda^{PS} &= \{\lambda^{PS,NA}, \lambda^{PS,NE}, \lambda^{PS,AE}, \lambda^{PS,EB}, \lambda^{PS,AN}, \lambda^{PS,EN}, \lambda^{PS,BN}, \lambda^{PS,EA}\},\\
s_0^{PS} &= N,\\
G^{PS} &= \{g^{PS,NA}, g^{PS,NE}, g^{PS,AE}, g^{PS,EB}, g^{PS,AN}, g^{PS,EN}, g^{PS,BN}, g^{PS,EA}\},\\
g^{PS,NA} &:= f^{v,PS} \wedge f^{l,PS} \wedge f_A^{fr,PS} \wedge \neg f^{CA,PS} \wedge f^{HLS,PS},\\
g^{PS,NE} &:= \neg(f^{v,PS} \wedge f^{l,PS}) \vee \neg(f_N^{fr,PS} \wedge f_A^{fr,PS}) \vee \neg f^{HLS,PS} \wedge \neg f^{lo,PS},\\
g^{PS,AE} &:= \neg(f^{v,PS} \wedge f^{l,PS}) \vee \neg(f_N^{fr,PS} \wedge f_A^{fr,PS}) \vee \neg f^{HLS,PS} \wedge \neg f^{lo,PS},\\
g^{PS,EB} &:= f^{lo,PS},\\
g^{PS,AN} &:= f^{v,PS} \wedge f^{l,PS} \wedge f_N^{fr,PS} \wedge f^{CA,PS} \wedge f^{HLS,PS},\\
g^{PS,EN} &:= f^{v,PS} \wedge f^{l,PS} \wedge f_N^{fr,PS} \wedge f^{CA,PS} \wedge f^{HLS,PS},\\
g^{PS,BN} &:= f^{v,PS} \wedge f^{l,PS} \wedge f_N^{fr,PS} \wedge f^{CA,PS} \wedge f^{HLS,PS},\\
g^{PS,EA} &:= f^{v,PS} \wedge f^{l,PS} \wedge f^{HLS,PS} \wedge f_A^{fr,PS} \vee \neg f^{CA,PS}.
\end{aligned}
$$

Here, S^{PS} is the discrete states of PS, i.e. Normal (N), Alert (A), Emergency (E) and Blackout (B). The rest of the variables are as described in Eq. (4.12). Fig. 4.3 depicts A^{PS} with four discrete states and eight transitions as per [43]. This model can be used to analyse the impact of disturbances and remedial actions on the PS state. Transitions NA, NE, AE and EB represent state degradation, while AN, EA, EN and BN represent state recovery. The transition BN follows the restoration or black start procedure described in [111] with the restorative state in between, both of which are beyond the scope of this dissertation. Furthermore, since static steady-state modelling is considered, the temporal aspects of the PS state classification, including frequency, cannot be comprehensively investigated and, hence, are part of future work. Consequentially, Eqs. (4.23) and (4.24) are not used in the rest of the dissertation. Eq. (4.28), however, shows that the proposed model could be extended to include frequency.

4.4 Joint Operational State Model for CPESs

Fig. 4.4 shows the joint operational state model for CPES developed in this dissertation and comprises interconnected ICT and PS submodels. The former consists of the ICT model $\mathcal{G}^I$ and multiple finite state automata that determine the state of each grid service from Sec. 4.2. The latter consists of the PS model $\mathcal{G}^P$ and its automaton from Sec. 4.3. The dotted lines represent the interdependencies between the submodels.

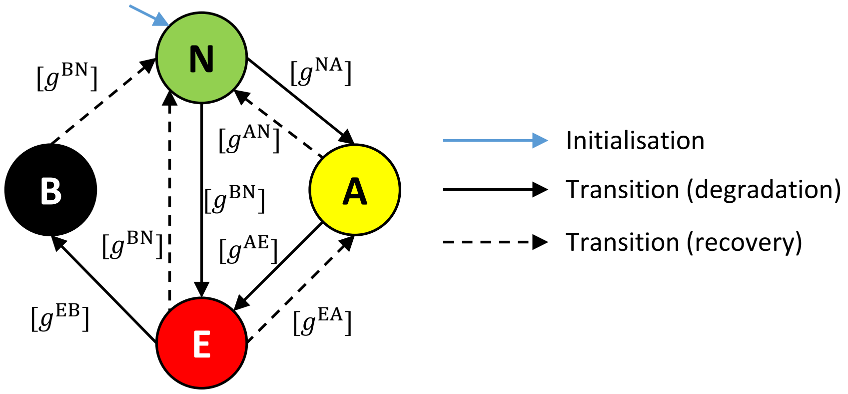


Fig. 4.3: Finite state automaton of a power system.

The PS submodel provides a set of unsupplied nodes (buses) to the ICT submodel. In return, it receives the state of each grid service as well as the available measurements and controllers. This captures structural as well as functional interdependencies between the submodels. In the PS submodel, a distinction is made between the global (or actual) view and the perceived view based on [25]. While the global view refers to the state of all PS components as they are in the field at a given moment, the perceived view refers to the state of PS components as depicted by the (potentially disturbed) ICT system at a given time. The perceived view is derived based on the states of the high-level services. The operational decisions based on the perceived view are modelled as optimisation. The resulting decisions are then mapped into the global PS view (as the decisions impact the actual grid) using power flow calculations.

The input to the overall model is a single or sequence of independent external disturbance from PS and ICT domains, based on which the properties of the corresponding submodels are modified, e.g., power line failures are modelled by suitably modifying $\mathcal{G}^P$ and server failure by removing the corresponding node from $\mathcal{G}^I$. State transitions in each submodel are triggered either by the external input disturbances or by a propagating disturbance from the other submodel, e.g., as shown in Eqs. (4.1) and (4.26). The output is the operational state trajectory of a CPES, which consists of states of PS and the ICT-enabled grid services.

Assuming that the ICT system has m grid services, let S^I be the set of the discrete states of the grid services, i.e., $S^I = \{s_1^{GS}, ..., s_m^{GS}\}$. Since the role of the ICT is to enable the grid services, S^I represents the state of the ICT system in CPES. Then, the joint operational state model of CPES can be written as the following n-tuple:

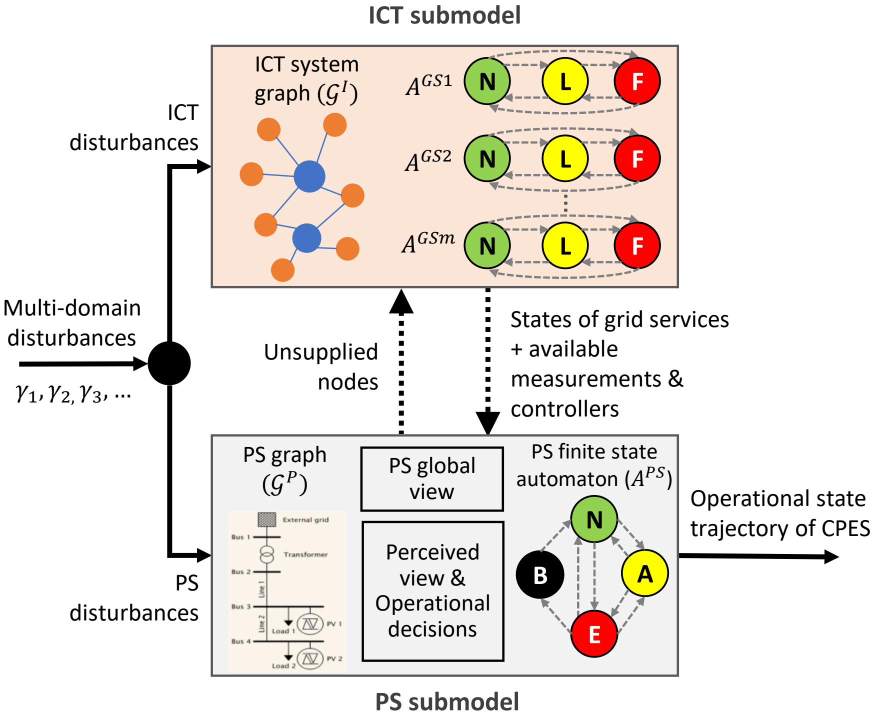


Fig. 4.4: Overview of the proposed joint operational state model for CPESs with power and ICT submodels.

$$A^C = (sys, S^C, X^C, \Lambda^C, G^C, \Gamma, Init, pf, u_1, u_2), \tag{4.29}$$

The explanation of variables in Eq. (4.29) are in Tab. 4.1. Fig. 4.5 shows the execution of A^C, which consists of the steps explained in the following sections.

4.4.1 Initialisation

The term sys consists of the PS and ICT system models constituting a CPES. Initialising sys involves initialising the PS $\mathcal{G}^P$ and the ICT system $\mathcal{G}^I$. The initial values of the continuous states X_0^C and discrete PS state S^{PS} can be determined using flow calculations based on the initial PS $\mathcal{G}_0^P$ and the PS automaton from Eq. (4.28), respectively. Note that the slack bus of $\mathcal{G}^P$ is initialised to 1 p.u.. The initial discrete state of ICT system S^I can be determined using the initial ICT graph model $\mathcal{G}_0^I$ and the automaton of the grid services (Eqs. (4.12), (4.19)). Using this, A^C can be initialised as $Init = \{S_0^C, X_0^C\}$. This represents an undisturbed CPES.

Tab. 4.1: Description of variables in joint operational state model in Eq. (4.29).

$sys = \mathcal{G}^P \cup \mathcal{G}^I$	Set of PS & ICT parameters
$S^C = S^{PS} \cup S^I$	Set of discrete PS & ICT (i.e., grid service) states
$X^C = \{V_b, L_c\}$	Set of continuous variables (bus voltages & line loadings)
$\Lambda^C = \Lambda^{PS} \cup \Lambda^I$	Set of PS & grid service state transitions
$G^C = G^{PS} \cup G^I$	Set of guard conditions for each $\lambda^C \in \Lambda^C$
$\Gamma = \{\gamma_1, \gamma_2, ...\}$	Set of independent PS & ICT input disturbances
$Init = \{S_0^C, X_0^C\}$	Set of initial values for S^C and X^C
pf	Power flow calculation describing the evolution of X^C
u_1	Function mapping each input $\gamma \in \Gamma$ onto sys
u_2	Function for activating a specific set of constraint

4.4.2 Introduction of External Disturbance

In this step, the next disturbance $\gamma \in \Gamma$ is mapped onto the CPES sys using the function u_1. For the first iteration, γ would correspond to the first disturbance. Γ can comprise both PS and ICT disturbances, and this step does not consider operational decisions. This disturbed CPES can be represented as $sys^+ = \mathcal{G}^{P+} \cup \mathcal{G}^{I+}$, where:

$$sys^+ = u_1(sys, \gamma) = \{Z * \zeta \mid Z \in sys, \zeta \in \gamma\} \tag{4.30}$$

Here, ζ indicates the change in the parameter $Z \in sys$ due to γ, and $*$ represents either the addition or multiplication operator depending on the nature of γ. In the case of disturbances like an increase/decrease in PS loads or ICT delays, ζ is a positive or negative value, Z will be P^D, Q^D (for loads) or δ (for delays), and $*$ will represent addition. However, in case of disturbances such as component failures, ζ is zero, Z will be ψ, and $*$ will represent multiplication. The impact of disturbances on PS and ICT systems can be determined as described in Secs. 4.2 and 4.3.

4.4.3 Perceived View

This step determines the perceived view of the potentially disturbed PS and ICT system. As mentioned earlier in this section, the perceived view refers to the state of PS components as depicted by the (potentially disturbed) ICT system at a given time and is derived based on high-level services. Fig. 4.6 shows the interaction between global and perceived views in the proposed model. The former refers to the physical CPES, and the latter is related to its situational awareness from the high-level services, which is based on the received measurements. While disturbances

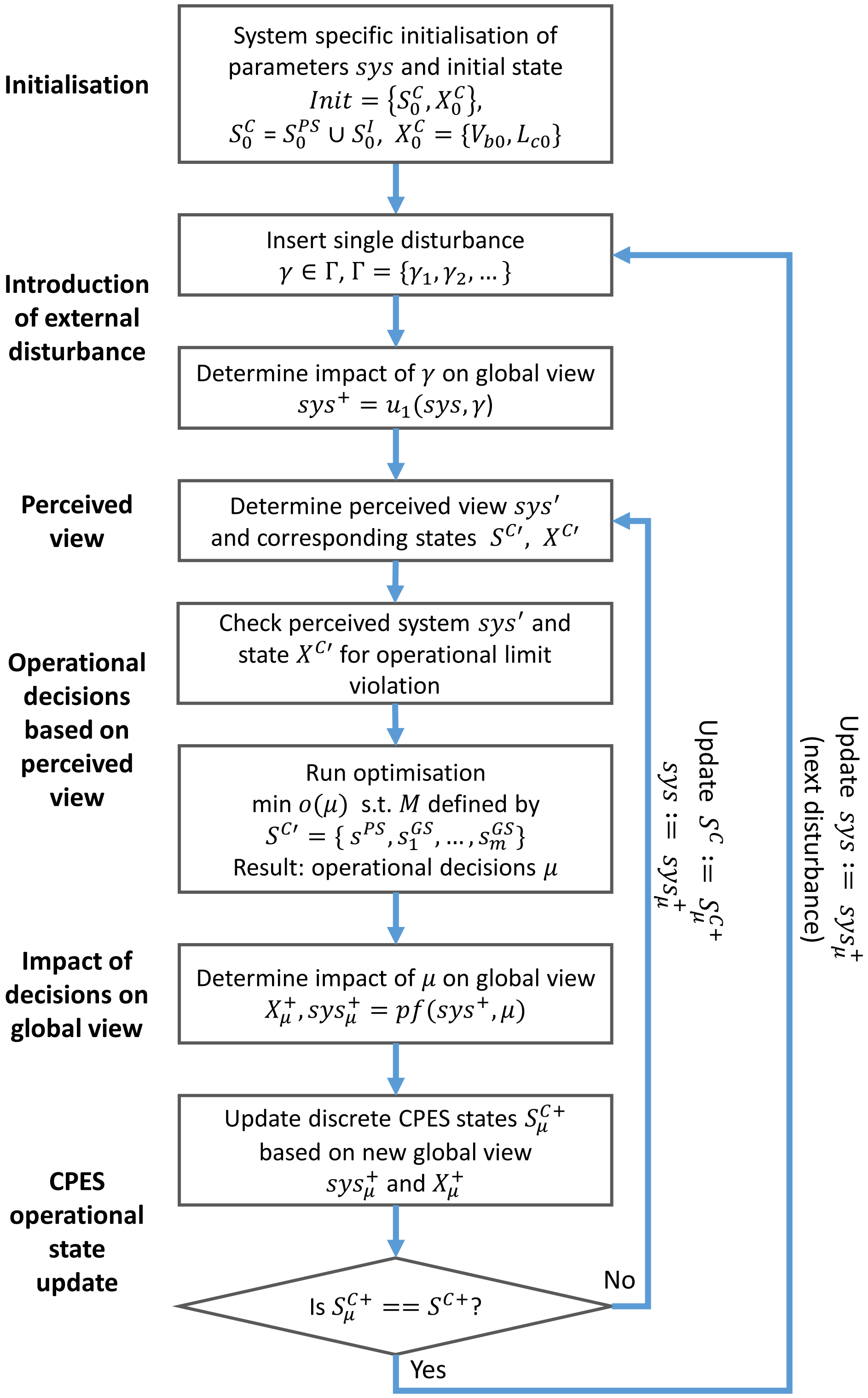


Fig. 4.5: Execution of the developed joint operational state model for CPES.

impact the global view, operational decisions are taken based on the perceived view, affecting the global view. Since centralised grid services are considered in this dissertation, the perceived view is from the control room's perspective. It consists of the perceived PS and ICT system sys' and the perceived continuous states $X^{C'}$, based on which the perceived discrete state $S^{C'} = S^{PS'} \cup S^{I'}$ are calculated.

The properties of the ICT system (cf. Sec. 4.1) influence the measurements and, consequentially, the high-level services. This can potentially cause the perceived view to differ from the global view. Consequently, certain PS disturbances can be hidden in the perceived view, as in the 2003 North American blackout (cf. Sec. 1.2). This is particularly relevant in the case of a disturbed ICT system $\mathcal{G}^{I+}$ (cf. Sec. 4.4.2). As shown in Sec. 4.2, the states of the grid services can be updated based on the graph $\mathcal{G}^{I+}$ and the respective finite state automaton. This results in the perceived discrete state of the ICT system $S^{I'}$. Note that certain ICT disturbances, such as stealthy cyber-attacks, could be challenging to detect. It is assumed that the control room can monitor the ICT components and their properties using network monitoring tools, as shown in [55].

In this dissertation, the perceived view of the PS is determined based on the SE service, which implies that the received measurements should satisfy the timeliness and correctness conditions in Eq. (4.8). Let $Z^{'} = \{Y', P', Q'\}$ be the measurements considered by the SE in the control room, where P' and Q' are the perceived aggregated power injections at the buses. Then, the SE service estimates the continuous state as $X^{C'} = \{V_b^{'}, L_c^{'}\}$, which represents the perceived continuous state. Here, $V_b^{'}$ is a set of complex voltage values with magnitudes and angles. The perceived discrete PS state $S^{PS'}$ can then be determined based on $X^{C'}$ using the PS automaton in Eq. (4.28).

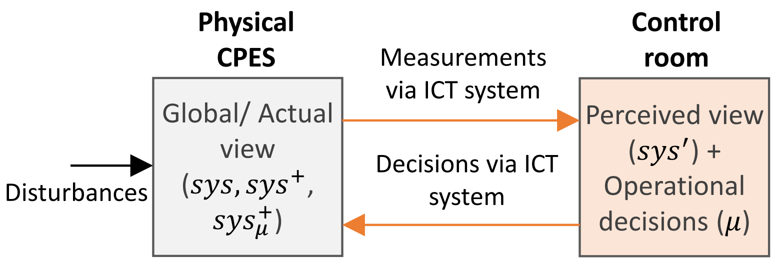


Fig. 4.6: Interaction between actual and perceived views.

4.4.4 Operational Decisions based on Perceived View

In this step, the operational decisions on the PS based on potential operational limit violations in the perceived view from Sec. 4.4.3 are determined. The result is the deployment of suitable remedial actions to counteract the disturbance γ and improve the PS discrete state S^{PS+}. The operational decisions are modelled as an optimal power flow, as shown in [112]. Generally, it can be written as the minimisation of the objective function $o(\mu)$:

$$\begin{aligned} \min_{\{\mu\}} \quad & o(\mu) \\ \text{subject to} \quad & l_e(\mu) \leq 0 \quad \text{and} \\ & l_i(\mu) = 0 \end{aligned} \tag{4.31}$$

Here, $\mu \subset sys'$ is the set of PS optimisation variables, i.e., P, Q, Y, that can be controlled from the control room. Generations and controllable loads are represented by P and Q, while switches and circuit breakers by Y. $o(\mu)$ can represent several possible objectives, such as the economy (e.g., finding a dispatch of DERs with the lowest costs) and stability (e.g., reducing loadings of power lines). $l_i(\mu)$ and $l_e(\mu)$ represent the inequality and equality constraints, respectively. Generally, the former includes capacities of PS components and the operational limits of buses, lines and other PS equipment, while the latter includes the power balance between generation and demand [112]. The selection of the constraints, however, depends on the perceived view, i.e., sys', $X^{C'}$ and $S^{C'}$. For a CPES with m grid services, the function u_2 suitably activates a specific set of constraints $\mathcal{L}_n \subset \mathcal{L}$ and can be generally defined as

$$u_2(sys', X^{C'}, S^{C'}) = \begin{cases} \mathcal{L}_1 \subset \mathcal{L} & \text{if } s_1^{GS} = N \wedge s^{PS} = A \Rightarrow \mu_1 \subset sys', \\ \mathcal{L}_2 \subset \mathcal{L} & \text{if } s_1^{GS} = L \wedge s^{PS} = A \Rightarrow \mu_2 \subset sys', \\ \mathcal{L}_3 \subset \mathcal{L} & \text{if } s_1^{GS} = F \wedge s^{PS} = A \Rightarrow \mu_3 \subset sys', \\ & \vdots \\ \mathcal{L}_{n-1} \subset \mathcal{L} & \text{if } s_m^{GS} = L \wedge s^{PS} = A \Rightarrow \mu_{n-1} \subset sys', \\ \mathcal{L}_n \subset \mathcal{L} & \text{if } s_m^{GS} = F \wedge s^{PS} = A \Rightarrow \mu_n \subset sys'. \end{cases} \tag{4.32}$$

This equation shows only an excerpt from the function u_2 with the PS in the Alert state and $\mu_1, \mu_2, ..., \mu_n$ represent different actuation commands from the control room. There exist multiple sets of constraints based on the discrete states of PS (s^{PS}) as well as the grid services (s^{GS}). This is relevant as certain grid services are only allowed in certain PS states, e.g., load shedding is permitted only when $s^{PS} = E$ (cf. Sec. 2.4). Eq. (4.32) can be adapted for specific grid services based on their respective automaton from Sec. 4.2. For the SE service, the control room has no situational awareness when $s^{SE} = F$. In this case, it sends a predefined command to the field controllers, switching them to the fallback mode, i.e., use local measurements. Using Eq. (4.32), the optimisation can be written in the following condensed form:

$$\begin{aligned} &\min_{\mu}\{o_s(\mu) \mid \mu \in M\} \text{ with} \\ &M = \{\mu \subset sys' \mid l_i(\mu) \leq 0, l_e(\mu) = 0, l_i, l_e \in \mathcal{L}\}. \end{aligned} \tag{4.33}$$

Here, M is the set of feasible solutions without constraint violations, and $\mathcal{L}$ is the set of all constraint functions corresponding to the states of PS and the grid services $s \in S^{C'}$. While the equality and inequality constraints corresponding to buses and lines are activated in all cases of u_2, the constraints corresponding to the grid services (especially the remedial actions), such as tap position t^T and P^G setpoints of DERs, are activated depending on the state of the PS and the corresponding grid service. This implies that each combination of discrete states has its constraint parameterisation. For example, as described in Sec. 3.4.3, the DERs controlled when the redispatch service in the Normal state ($s^{RD} = N$) is different from when it is in the Limited state ($s^{RD} = L$).

Eqs. (4.32) and (4.33) model the control room's response to the perceived view. For instance, if the goal is economic dispatch of the available DERs, the $o_s(\mu)$ can be a cost function. When a bus voltage limit violation is detected in the perceived view, the control room suitably deploys the VC service to adjust the P^G and Q^G of specific DERs and/or the transformer tap position t^T. Here, $P^G, Q^G, t^T \in \mu$ are constrained by the corresponding inequality constraint (l_i). If failures of DERs and OLTC are detected in sys', then the corresponding P^G, Q^G, and t^T are excluded from Eq. (4.32). If a remedial action has failed, all equipment solely controlled by that grid service will be excluded. Therefore, Eq. (4.32) captures the functional dependence, i.e., the impact of the operational states (or performance) of the ICT-enabled grid services on the PS. The result is a set of decisions μ, which are then transmitted to the corresponding OT devices.

4.4.5 Impact of Operational Decisions on Global View

In this step, the impact of decisions μ on the global CPES sys^+ is determined. This is calculated using power flow (pf) calculations, which modifies sys^+ based on μ, resulting in sys^+_μ. Here, sys^+_μ represents the global view impacted by the operational decisions μ. pf also yields the corresponding continuous states $X^{C+}_\mu = \{V^+_{b,\mu}, L^+_{c,\mu}\}$.

This can be written as $pf : (sys^{+}, \mu) \rightarrow (sys_{\mu}^{+}, X_{\mu}^{+})$. Activation of the control reserves as a change in P and Q of generators and controllable loads, while topology modifications can be mapped as changes in the corresponding entries in Y. The ICT nodes that have potentially lost power supply are then determined using $V_{b,\mu}^{+}$ and Eq. (4.1), based on which $\mathcal{G}^{I}$ is modified (i.e., structural dependence). This step is especially relevant when the perceived view differs from the global view, e.g., due to ICT disturbances. In this case, the decision μ may have an unwanted negative impact on the global CPES.

4.4.6 Operational State Update

In this step, the discrete state of the global CPES is updated as $S_{\mu}^{C+} = \{S_{\mu}^{PS+} \cup S_{\mu}^{I+}\}$, based on sys_{μ}^{+} and X_{μ}^{+} determined in the previous step. Similar to the initialisation in Sec. 4.4.1, $S_{\mu}^{PS'}$ is determined using Eq. (4.28) and $S_{\mu}^{I'}$ using Eqs. (4.12) and (4.19).

If $S_{\mu}^{C+} \neq S^{C}$, it indicates that the PS operational decision μ has propagated and impacted the ICT system via the structural dependence by causing certain ICT components to either gain (positive impact) or lose (negative impact) power supply. The resulting impact on the grid service and, consequentially, the PS should then be re-evaluated. To do so, the process in Fig. 4.5 is reiterated from Sec. 4.4.3, i.e., creating a new perceived view, with S_{μ}^{C+} and sys_{μ}^{+} as the new values of S^{C} and sys, respectively. This shows the ability of the model to capture the propagation of disturbances between power and ICT systems via interdependencies.

If $S_{\mu}^{C+} = S^{C}$, it indicates that there is no further propagation of the disturbance γ or decision μ between the power and ICT systems. Then, the process in Fig. 4.5 is reiterated from Sec. 4.4.2, i.e., the next disturbance from the sequence of input disturbance Γ is considered. The value of sys_{μ}^{+} is assigned as the new value of sys. The sequence of discrete states $S_{\mu}^{C'}$ constitutes the operational state trajectory of CPES corresponding to each $\gamma \in \Gamma$. Since Γ can be comprised of both PS and ICT disturbances (cf. Sec. 4.4.2), this shows the ability of the proposed model to analyse the impact of a sequence of multi-domain disturbances in terms of the operational state trajectory, also considering their propagation between the PS and ICT systems.

4.5 Chapter Summary

This chapter presents the artefact of RQ1, which aims to model the operational state trajectory of CPESs, considering the interdependencies between power and ICT systems. The highlights of this chapter are as follows:

- A formal description of CPESs is presented, with the power and ICT sub-systems modelled using property graphs. Components of both sub-systems and their linkages have been described by nodes, edges and their respective properties. The structural and functional interdependencies between the power and ICT systems have also been formalised using these properties.
- Using the ICT graph model, the operational states of ICT-enabled grid services from Chapter 3 have been formalised using finite state automata, with one automaton for each grid service. The automaton describes the three operational states (i.e., Normal, Limited and Failed), the conditions for state transitions and possible dependencies between the grid services. Subsequently, the model has been applied to state estimation and OLTC-based voltage control services.
- Based on the PS graph model, the PS operational states from Sec. 2.4 have also been formalised using a finite state automaton. The state transitions have been formulated based on properties such as bus voltages, line loading, contingency assessment and states of high-level services.
- A formal joint operational state model for CPESs has been developed using the automata of the power system and ICT-enabled grid services. Global and perceived views are differentiated because disturbances impact the global view, while operational decisions are taken based on the perceived view, affecting the global view. The operational decisions have been modelled using an optimal power flow. The developed model can take a sequence of multi-domain (power and ICT) disturbances as input and calculate the state trajectories of the PS and ICT-enabled grid services as output.

5 Joint Operational State Model for CPESs – Results & Discussion

This chapter presents the simulation setup and the results of the joint operational state model from Chapter 4. First, the architecture of the CPES under consideration is presented. This is followed by the simulation setup, which is used to validate the formal model. Finally, the results are presented and discussed. This chapter aims to demonstrate the artefact of RQ1 from Chapter 4, along with evaluating the corresponding functional and non-functional requirements. Note that parts of the contents of this chapter are published in [11].

5.1 System Architecture

The architecture of the CPES considered in this chapter consists of two aspects – the interconnected power and ICT systems and the ICT-enabled grid services.

5.1.1 Interconnected Power and ICT System Model

The PS considered here is the CIGRE MV benchmark grid shown in Fig. 5.1 [113]. Based on the modelling in Sec. 4.1, a static steady-state model of the PS is considered here. It has 15 buses (representing substations), two 110/20 kV transformers with 20 MVA rated power, and 13 loads. The 110 kV external grid is connected to bus-0 (slack bus), which is then connected to buses 1 and 12 via the transformers. The transformer $T1$ is equipped with an automatic OLTC with 10 tap steps of $\pm 1\%$ voltage ratio each on the secondary side (bus-1). The loads represent a mix of industrial as well as residential loads with a total peak demand of 46,125 kVA. Based on Sec. 4.3, the normal operational limits for bus voltages and line loadings are considered as 1 ± 0.05 p.u. and $\leq 80\%$, respectively. A violation of these limits will cause a state transition in the PS, as described in Sec. 4.3. For example, the PS degrades to the Emergency state in case of an over-/under-voltage and will further degrade to the Blackout state when more than 50% of all buses (in this case, more than 7 buses) have a voltage loss.

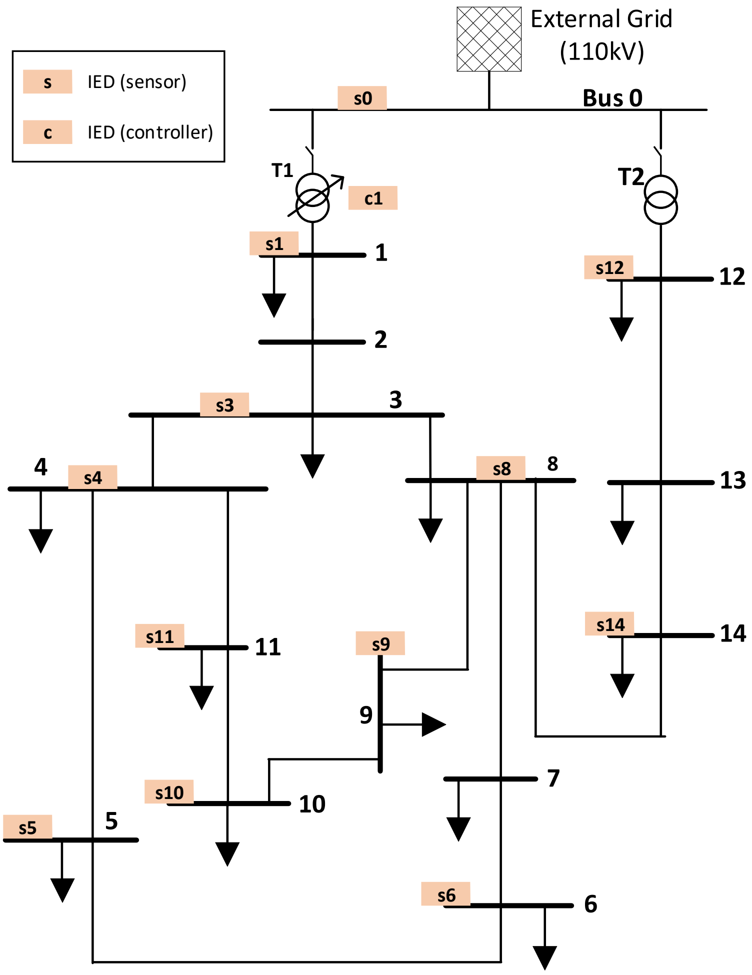


Fig. 5.1: Power system: CIGRE MV benchmark grid.

Although several benchmark power grids exist, there is currently a lack of standardised ICT systems corresponding to the power grids. Therefore, the ICT system used in this dissertation is designed based on the methodology in [114] and is presented in [11]. Fig. 5.2 shows the ICT system designed for the CIGRE MV grid. The ICT system is assumed to be dedicatedly used by the power grid. This is a valid assumption considering the rapid digitalisation of distribution grids [48]. IEDs for measurement are located at the buses and are named s_b, where b is the corresponding bus number. Since the CIGRE MV grid is a distribution grid, measurement IEDs are only placed at 12 buses, as shown in Fig. 5.1, representing observability of 80 %. The tap of the transformer $T1$ is controlled by IED c_1 associated with it. Measurement IEDs

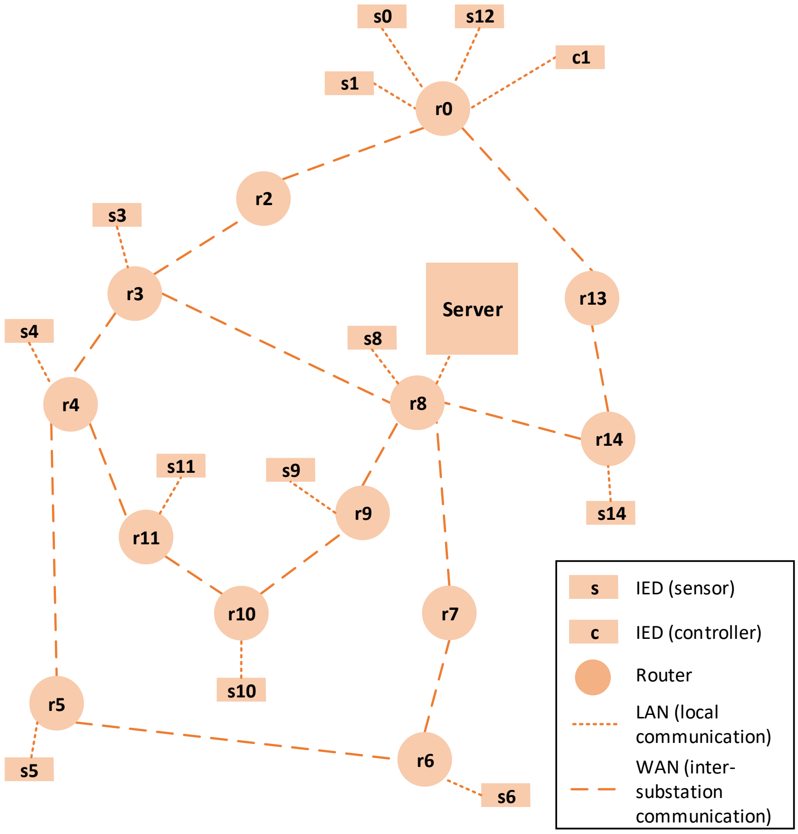


Fig. 5.2: ICT network for the CIGRE MV grid in Fig. 5.1.

s_b and the controller IED c_1 represent the OT part of the ICT system, and their properties are similar to those of nodes n_2 and n_1, respectively, in Fig. 4.1. Although a typical IED can perform both measurement and control, they are separated in this dissertation in order to analyse the difference between the loss of measurement data and actuation capability. In the rest of this chapter, the terms sensors and controllers refer to IEDs performing measurement and actuation, respectively, which are typically located at the bay level of the substation [115].

Each bus (or substation) is also equipped with a router named r_b. The IEDs (OT devices) in the substation communicate to the substation router via LAN. This represents intra-substation communication, shown using dotted lines in Fig. 5.2. The routers are then connected via the WAN, which represents inter-substation communication and is shown using dashed lines in Fig. 5.2. A WAN communication link is considered between two routers if power lines connect the corresponding buses. Buses 0, 1 and 12 are connected via the transformers, not power lines. This indicates that they are located in the same substation and are, therefore, associated with the same router r_0. Typical communication technologies used in LAN and WAN are already shown in Fig. 2.2. The routers and the communication links represent the IT network. The properties of the routers and links are similar to those of node n_3, edge e_1 and edge e_3 in Fig. 4.1. The links in this scenario represent wired communication, such as fibre optic and power line carrier communication. This could, however, be adapted to wireless communication, in which case, the links would represent the overlay for wireless technologies such as cellular or WiMAX.

The PS is operated from a central server, possibly located in a monitoring and control station, to which all sensor and controller IEDs communicate. Based on [83], the central server is assumed to be connected to the node with the highest betweenness centrality [1], in this case, the router at bus-8, as it is the most central node regarding data flows. This enables the assessment of the availability condition introduced in Sec. 3.1. For example, measurements from a sensor IED are said to be available only if the sensor IED is operational and has a valid communication path to the server. This can be calculated using Eq. (4.8).

Each bus provides power supply to the connected ICT components, and battery backup is not considered. Therefore, when a bus loses power, all the connected ICT components are considered unavailable. This represents a cascading disturbance and can be calculated using Eq. (4.1). Note that considering battery backup for several ICT components is costly, but it is a common measure to decouple the structural dependence of the ICT system on the interconnected PS [76].

5.1.2 ICT-enabled Grid Services

The ICT-enabled grid services considered are SE and VC, which are already discussed in Secs. 3.4 and 4.2. Their implementation based on the power and ICT systems in Figs. 5.1 and 5.2 is presented in this section.

The centralised SE service aims to provide estimated voltage magnitudes and angles devoid of telemetry errors, also for the buses from which measurements are unavailable, i.e., buses 2, 7 and 13 in Fig. 5.1. Bus measurements include active power and reactive power injections, whereas line measurements include active and reactive power flows from the sending end. For instance, sensor IED s_6 measures the power injection at bus-6 and the power flow between bus-6 and bus-7. The measurements are then transmitted to the server via the shortest path in the IT network. For instance, measurements from s_6 will be transmitted via the nodes

[1] In graph theory, betweenness centrality is a measure of centrality in a graph based on shortest paths.

r_6, r_7, r_8. In the case of an IT disturbance in this path, the measurements can be suitably rerouted, for example, via r_5. The server hosts the WLS algorithm, which processes the received measurements to calculate the SE results. The server also has pseudo-measurements for substituting corresponding field measurements when required. The operational states of the SE service can then be assessed using the model from Sec. 4.2.1.

The VC service aims to remedy voltage limit violations potentially caused by PS disturbances and is assumed to depend on SE results for situational awareness. When a bus voltage limit violation, i.e., $v_b > 1.05\,$p.u. or $v_b < 0.95\,$p.u., is detected in the SE results, setpoints are sent to c_1 to change the tap of $T1$, thereby modifying the voltage of the entire grid connected to the secondary side of T_1. The transfer of setpoints from the central server to c_1 is via the shortest path of the IT network. In this case, it could either be via the nodes r_8, r_3, r_2, r_0 or r_8, r_{14}, r_{13}, r_0. These setpoints are sent until the SE results indicate that all voltages are within their respective limits. In the absence of remote setpoints, for instance, due to IT disturbances, c_1 uses the measurement from local IED s_1. In this case, a tap change is performed only when s_1 indicates a voltage limit violation. The operational states of the VC service can then be assessed using the model from Sec. 4.2.2.

5.2 Simulation Setup for Validation

Validation is an essential step in any model development. In this dissertation, the formal model developed in Chapter 4 is validated by comparing its results with a simulation setup consisting of power and ICT systems. Based on [116], this serves as an input-output validation for the developed model. The developed simulation setup is presented in this section.

Fig. 5.3 illustrates the setup consisting of interconnected power and ICT system models, along with the two grid services. Its execution is described by Algorithm 1. The PS is modelled in steady-state in PandaPower [2] and the ICT network is modelled as a graph in NetworkX [3]. The choice of the simulations is motivated by their open-source nature, ease of usage and mutual compatibility. The data exchange between both simulators could be facilitated easily since both are Python-based libraries. The simulation setup is developed based on the formal model from Fig. 4.4, i.e., the input to the setup is a sequence of multi-domain independent disturbances, and the output is the operational states of PS and the two grid services.

[2] PandaPower: https://pandapower.readthedocs.io/en/v2.12.0/index.html# (Accessed: May 3, 2023)
[3] NetworkX: https://networkx.org/ (Accessed: May 3, 2023)

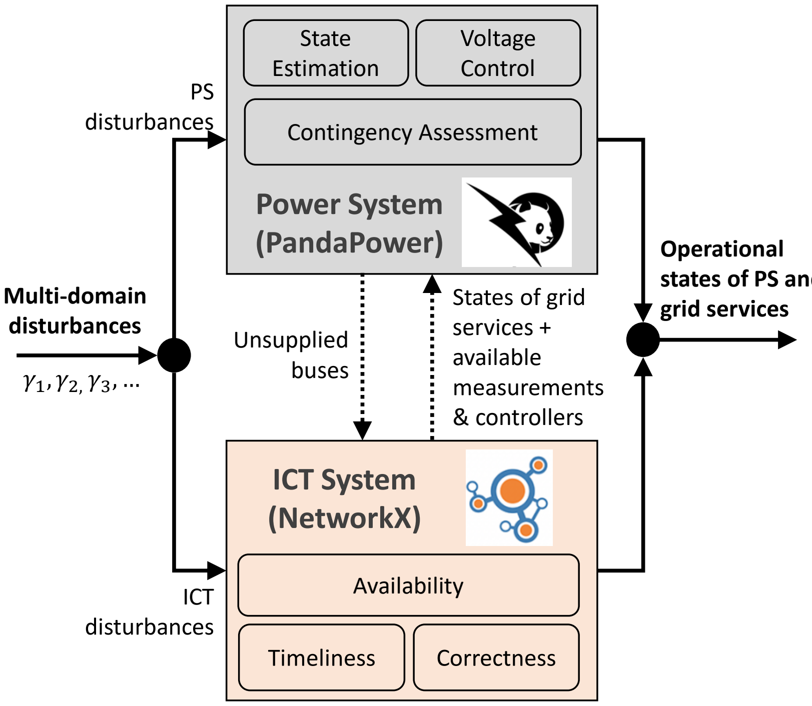


Fig. 5.3: Overview of the developed simulation setup for validation.

The PS simulation consists of the CIGRE MV grid shown in Fig. 5.1 and the two grid services. This contrasts with the formal model, where the grid services are part of the ICT system. This is because the PandaPower simulator has built-in modules for SE [4] and VC [5] services. The contingency analysis has also been considered in the PS simulation in order to assess the Alert state. As discussed in Sec. 2.4.1, this analysis identifies potential contingencies that would violate the operational limits despite utilising the available remedial actions, which in this case is only the VC service. The PS is in the Alert state when the contingency analysis yields a positive result. The contingency list here consists of all single power line failures. Each contingency in the list is simulated on a copy of the power grid in its current state, considering the current states of the two grid services. If the available remedial actions are not dependent on the SE service, the SE state need not be considered in the contingency analysis. Power flow calculations are used to assess the impact of PS disturbances (input) and calculate the list of unsupplied buses.

The ICT system model in NetworkX received the list of unsupplied nodes as input. The ICT simulation consists of the ICT network shown in Fig. 5.2. Graph theoretical

[4] PandaPower State Estimation:https://pandapower.readthedocs.io/en/v2.12.0/estimation.html (Accessed: May 3, 2023)
[5] PandaPower TrafoController: https://pandapower.readthedocs.io/en/v2.12.0/control/ controller.html#trafocontroller (Accessed: May 3, 2023)

Algorithm 1: Execution of Co-simulation Framework

Input: List of independent external disturbances: $\Gamma = \{\gamma_1, \gamma_2, \gamma_3, \dots\}$.
Result: Operational states of CPES: s^{PS}, s^{SE}, s^{VC}.
Data: Initial available measurements: Φ_0^ρ,
initial list of unsupplied buses: un,
initial operational states of CPES: $s_0^{PS}, s_0^{SE}, s_0^{VC}$.

1 **for** *disturbance* γ *in* Γ **do**
2   **if** γ *is a PS disturbance* **then**
3   modify Pandapower PS model based on γ
4   **else**
5   modify NetworkX ICT model based on γ
6   **end**
7   **if** γ *is the first disturbance in list* Γ **then**
8   Assign $s^{SE} \leftarrow s_0^{SE}, s^{VC} \leftarrow s_0^{VC}, \Phi^\rho \leftarrow \Phi_0^\rho$
9   **end**
10   **Run** *ps_simulation(*$s^{SE}, s^{VC}, \Phi^\rho$*)*:
11   Run SE in state s^{SE} using measurements Φ^ρ to estimate list of bus voltages $\hat{V}_b$
12   **while** *any* $\hat{v}_b$ *in* $\hat{V}_b$ *violates operational limits* **do**
13   Run VC in state s^{VC} to change transformer tap
14   Run SE in state s^{SE} and recalculate $\hat{V}_b$
15   **end**
16   Run powerflow to determine the updated list of unsupplied buses un' and
17   list of line loadings L_c
18   **return** $un', \hat{V}_b, L_c$
19   **Run** *ict_simulation(*un'*)*:
20   Update NetworkX ICT system model based on un'
21   Determine operational state of grid services s^{SE}, s^{VC}
22   Determine list of available measurements Φ^ρ
23   **return** $s^{SE}, s^{VC}, \Phi^\rho$
24   **Run** *cpes_state_assessment(* $\hat{V}_b, L_c, s^{SE}, s^{VC}$*)*:
25   Compare $\hat{V}_b, L_c$ to operational limits
26   Run contingency analysis with SE and VC services in s^{SE} and s^{VC} states
27   Determine state of PS s^{PS} using results of steps 25 and 26
28   **return** s^{PS}, s^{SE}, s^{VC}
29   **if** $un \neq un'$ **then**
30   Assign $un \leftarrow un'$
31   goto Step 10
32   **else**
33   goto Step 1
34   **end**
35 **end**

calculations are used to assess the impact of the ICT disturbances and the unsupplied buses received from the PS simulator. This can be used to calculate the availability, timeliness and correctness properties of the SE and VC services, which can then be used to determine their operational states as described in Sec. 3.4. Note that although the grid services themselves are implemented in Pandapower, their states are determined by the ICT simulator. Their states and available measurements and controllers are given as input to the PS simulator, which then varies the functionality of these grid services accordingly. The information exchange between the simulators captures the interdependencies between power and ICT systems.

5.3 Results & Discussion

This section presents the results of the formal model from Chapter 4. The aim of these scenarios is to show that the proposed model can analyse the propagation of multi-domain disturbances between power and ICT systems in a CPES using its operational state trajectory. In this case, the operational states of the CPES consist of the states of PS, SE and VC. Followed by a base scenario (Scenario 0) to show the impact of the normal operation of grid services, scenarios focusing on the two grid services individually are presented. The results from the formal model were then validated using the simulation setup from Sec. 5.2. In the following figures, the state of the CPES is denoted by S^C, which is updated either by the input disturbance γ or the operational decision μ (cf. Secs. 4.4.2 and 4.4.5). The arrows between the states denote the propagation of disturbances between power and ICT systems. The sequence of S^C forms the operational state trajectory of the CPES, which is computed until the condition in Sec. 4.4.6 is satisfied.

Tab. 5.1 shows the disturbances considered in the scenarios. They are chosen to represent a variety of disturbances from both PS and ICT domains and to demonstrate cascading and escalating modes of disturbance propagation. Sensor failures $(\gamma_{s3}, \gamma_{s11})$ may occur due to hardware or software problems, while link failure $(\gamma_{r0,c1})$ could be due to physical damage. The bus failure γ_{bus9} can be due to a short circuit fault at the bus, resulting in its isolation by the protection system. The step increase in reactive power consumption of loads, i.e., γ_{load10} and γ_{load1}, are designed such that they result in an under-voltage at the respective buses, thereby requiring the VC service for remedy. γ_{load10} decreases v_{10} from 0.978 p.u. to 0.940 p.u. and γ_{load11} decreases v_1 from 0.987 p.u. to 0.946 p.u.. Based on Sec. 4.4.1, the states of the PS and the two grid services are initialised as Normal.

Tab. 5.1: Description of disturbances considered in the simulation scenarios.

Disturbance	Domain	Description
γ_{s3}	ICT	Sensor IED $s3$ failure
γ_{s11}	ICT	Sensor IED $s11$ failure
$\gamma_{ro,c1}$	ICT	LAN link between router $r0$ & controller $c1$ fail
γ_{load10}	PS	Reactive (Q) load jump at bus-10
γ_{load1}	PS	Reactive (Q) load jump at bus-1
γ_{bus9}	PS	Bus-9 failure

The Failed state is not shown in the scenarios since its impact is fairly obvious in the considered CPES with two grid services. Disturbances causing the SE service to be in the Failed state (e.g. server failure, loss of too many field measurements) can cause the system operator to lose situational awareness of the corresponding PS, which, in turn, can hinder all central server-based operations [94]. When the VC service is in the Failed state, it cannot be used to remedy voltage limit violations.

5.3.1 Scenario 0: Base Scenario

Fig. 5.4 shows the CPES state trajectory (S^C) considering disturbances γ_{bus9} and γ_{load10}. It can be seen that the initial state S_0^C is Normal. The disturbance γ_{bus9} causes the state of PS to degrade to its Alert state (S_1^C) based on the contingency analysis. This means, considering the current state of the PS, there is at least one contingency, in this case, the failure of the power line between bus-4 and bus-11, that will cause an operational limit violation in the PS. Additionally, based on Eq. (4.1), γ_{bus9} also results in loss of power supply to the ICT components connected to bus-9, i.e. $s9$ and $r9$. This results in the loss of measurements from sensor $s9$ and shows how a PS disturbance can cascade and impact the ICT system via structural dependence. Despite this, it can be seen that the SE is still in its Normal state (S_1^C), indicating that the solvability condition could be satisfied using measurements from other sensors. This also shows the importance of redundant sensors in the design of the SE service to increase its robustness against loss of measurements [38]. When γ_{load10} occurs, the PS transitions to the Emergency state due to the voltage limit violation at bus-10 (S_2^C). This is captured in the SE results (i.e., the perceived view from Sec. 4.4.3) based on which suitable setpoints are sent from the server to $c1$ to facilitate a tap change (denoted by μ_{oltc}). This increases v_{10} from 0.940 p.u to 0.975 p.u, thereby remedying the under-voltage resulting from γ_{load10}. Consequentially, the PS returns to the Alert state (S_3^C). For the PS to return to the Normal state, the disturbances

γ_{bus9} should be cleared, and the bus should be repaired. Scenario 0 shows that the grid services in their Normal state can remedy the considered PS disturbances.

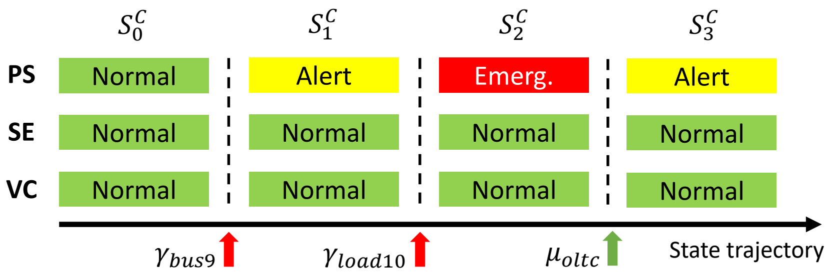


Fig. 5.4: CPES operational state trajectory for Scenario 0 (base scenario).

5.3.2 Scenario 1: States of Voltage Control Service

This scenario aims to demonstrate the disturbance propagation considering the operational states of the VC service. It consists of two sub-scenarios to show the different impacts of the Limited state of the grid service.

Fig. 5.5 shows the CPES state trajectory for Scenario 1A considering the disturbances $\gamma_{r0,c1}$, γ_{bus9} and γ_{load10}. The disturbance $\gamma_{r0,c1}$, which is a LAN link failure, causes the VC service to degrade to its Limited state (S_1^C) as it prevents setpoints from the server from reaching the controller $c1$. As discussed in Sec. 3.4.2, this results in the degradation of the VC service to its Limited state, where it acts based on local measurements, in this case, from sensor $s1$. Other disturbances that disrupt the data transfer between the server and $c1$, such as congestion in the WAN, will have the same consequence. Similar to Scenario 0 (cf. Sec 5.3.1), the disturbance γ_{bus9} causes the PS to transition to its Alert state (S_1^C), and the resulting loss of measurements from $s9$ does impact the state of the SE service. The under-voltage caused by γ_{load10} also causes the PS to degrade to the Emergency state (S_2^C). However, in contrast to Scenario 0, this under-voltage is not remedied by the VC service. The reason is that the grid service in the Limited state acts solely based on local measurements and, therefore, cannot detect the under-voltage at bus-10. If left unremedied, this could trigger protection systems, causing the loss of power supply to bus-10 as well as the components connected to it. This scenario demonstrates the ability of the proposed model to capture escalating disturbances, where the ICT disturbance $\gamma_{r0,c1}$ exacerbates the impact of an independent PS disturbance γ_{load10}. In Fig. 5.5, this is indicated by the arrow labelled 'esc.'. Furthermore, this demonstrates the propagation of disturbances due to functional dependencies between power and ICT systems via the remedial actions, which directly perform actuations on the PS.

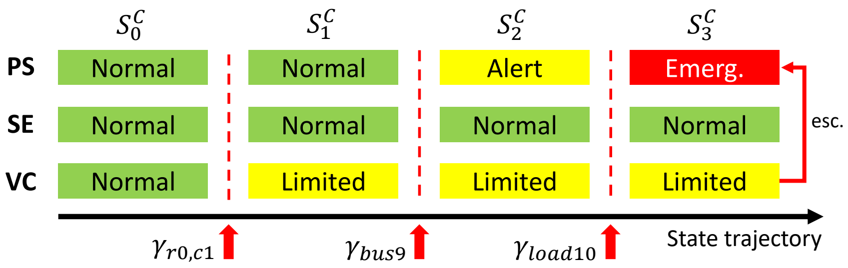


Fig. 5.5: CPES operational state trajectory for Scenario 1A. The Limited state of VC service has a negative impact on PS.

Fig. 5.6 shows the CPES state trajectory for Scenario 1B, which considers γ_{load1} instead of γ_{load10}. The impact of disturbances $\gamma_{r0,c1}$ and γ_{bus9} are similar that to that of Scenario 1A. This can be seen from the operational states S_1^C and S_2^C. The under-voltage caused by γ_{load1} transitions the PS to the Emergency state (S_3^C) due to the operational limit violation at bus-1. However, in contrast to Scenario 1A, this is remedied by the decision μ_{oltc} from the VC service, which increases v_1 from 0.946 p.u to 0.981 p.u., thereby restoring the PS to the Alert state (S_4^C). This is because the disturbance γ_{load1} is captured by the sensor $s1$ and is then communicated to the controller $c1$, which performs the tap change required to remedy the impact of γ_{load1}. In other words, in this scenario, the ICT disturbance $\gamma_{r0,c1}$ does not escalate the impact of the PS disturbance γ_{load1}. This shows that in alternative to Scenario 1A, the VC in its Limited state can also be used to remedy certain disturbances.

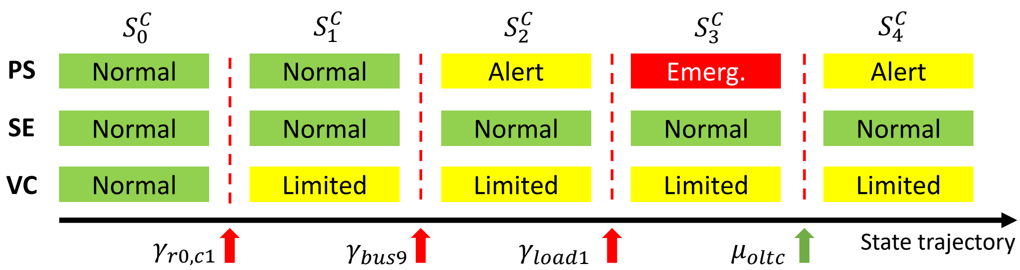


Fig. 5.6: CPES operational state trajectory for Scenario 1B The Limited state of VC service has a positive impact on PS.

These scenarios also show that the effectiveness of fallback measures while in the Limited state largely depends on the type of measure, the location and the nature of the disturbance. As discussed in [80], alternative fallback measures could be explored, such as using a combination of measurements from the secondary side (local) and voltage-wise the most critical bus (remote). Even then, the ability of the VC service to remedy the disturbance in its Limited state will be influenced by the location of the remote measurement and the disturbance. Therefore, one of the goals of system design should be to implement fallback measures that are efficient and flexible while keeping in mind the relevant set of disturbances.

5.3.3 Scenario 2: States of State Estimation Service

This scenario aims to demonstrate the disturbance propagation considering the operational states of the SE service. Similar to Scenario 1, this consists of two sub-scenarios to show the different impacts of the Limited state of the SE service.

Fig. 5.7 shows the CPES state trajectory for Scenario 2A considering the disturbances γ_{s11}, γ_{bus9} and γ_{load10}. Here, γ_{s11} results in the loss of measurements from sensor $s11$. The SE service, however, remains in its Normal state (S_1^C), indicating the importance of redundant measurements while designing the SE service. Similar to previous scenarios, the bus failure γ_{bus9} transitions the PS to its Alert state (S_2^C). However, in this scenario, the resulting cascade to the ICT system, i.e., loss of power supply to $s9$ and $r9$, degraded the SE service to its Limited state (indicated by the arrow labelled 'casc.' in Fig. 5.7). The SE service now has to use pseudo-measurements corresponding to either $s11$ or $s9$ to satisfy its solvability condition (cf. Eq.(3.1)). As discussed in Sec. 3.4.1, this increases the uncertainty in the SE results as pseudo-measurements are based on historical measurements, which, in this scenario, is before the occurrence of γ_{bus9}. The consequence of this can be seen after the occurrence of γ_{bus10} as the PS degrades to its Emergency state (S_3^C). This implies that the under-voltage caused by γ_{bus10} was not remedied by the VC service, even though it is in its Normal state. The reason is for this specific combination of disturbances and lost field measurements, the results of the SE service in its Limited state do not capture the under-voltage. As a result, no setpoints were sent to $c1$. This once again shows an escalating disturbance (indicated by the arrow labelled 'esc.' in Fig. 5.7), where γ_{s11} and γ_{bus9} worsen the impact of γ_{load10}. This scenario demonstrates disturbance propagation due to the functional dependencies between PS and ICT systems via the high-level services, which do not directly perform actuation on the interconnected PS. Furthermore, it also shows the relevance of the dependencies between the grid services.

Similar to Scenario 1B in Fig. 5.6, the Limited state of SE does not necessarily cause state degradation in the PS. This is shown by Scenario 2B in Fig. 5.8, where, instead of γ_{bus9}, γ_{s3} is considered between γ_{s11} and γ_{load10}. The impact of γ_{s11} (S_1^C) is the same as that of Scenario 2A. Although γ_{s3} still causes the state of SE to degrade to Limited (S_2^C) due to the use of pseudo-measurements corresponding to either $s11$ or $s3$, the VC service can remedy the under-voltage caused by γ_{load10}, i.e., increase v_{10}

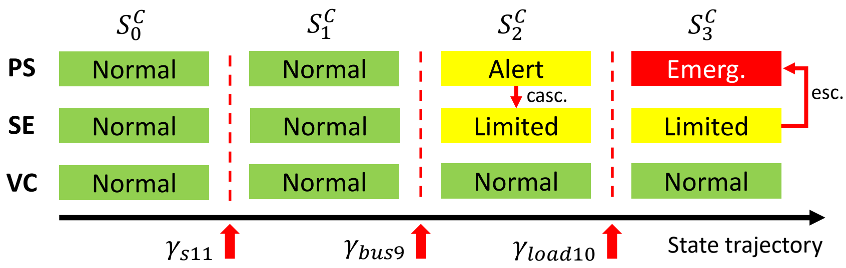


Fig. 5.7: CPES operational state trajectory for Scenario 2A. The Limited state of SE service has a negative impact on PS.

from 0.940 p.u. to 0.975 p.u.. As a result, the state of the PS is restored to Normal (S_4^C), indicating that the disturbance does not propagate. In contrast to Scenario 2A, this scenario shows that the SE results, even in the Limited state, can capture certain voltage limit violations. Based on this, setpoints were sent from the server to $c1$, facilitating suitable tap change to remedy the impact of γ_{load10}.

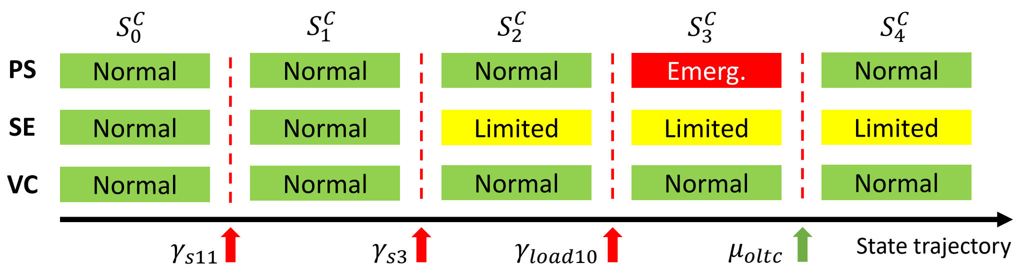


Fig. 5.8: CPES operational state trajectory for Scenario 2B. The Limited state of VC service has a positive impact on PS.

The effectiveness of fallback measures is largely influenced by their implementation [80]. In this regard, alternative methods for generating pseudo-measurements that do not solely rely on historical measurements, such as the ones shown in [98, 103], could provide different results. Furthermore, since the VC service depends on SE and not vice versa, a state degradation of the latter is more critical. Comparing scenarios 2A and 2B (as well as 1A and 1B), it is evident that the Limited state of a grid service does not necessarily imply that operational limit violations cannot be remedied; instead, it increases the risk of incorrect control actions in the PS. Therefore, the Limited state serves as a caution to the system operator about potentially bad decisions when using the corresponding grid service as well as other dependent services. In this regard, the proposed model can be used to test different fallback measures that enable the grid services to perform effectively in the presence of disturbances. It also allows the testing of robustness measures in the ICT system (e.g. redundancy, increased meshing), which enables the grid services to withstand the disturbances, thereby preventing the state degradation of the services in the first place.

5.4 Evaluation

This section evaluates the proposed model and the results based on the objectives of RQ1, which are presented in Sec. 1.5. This includes the functional requirements FR1, FR2 and FR3, as well as the non-functional requirements NFR1 and NFR2.

5.4.1 Functional Requirements

Based on the results from Sec. 5, it is evident that the developed model can successfully analyse the propagation of disturbances between power and ICT systems in a CPES. The resulting operational state trajectory has both state degradation (due to disturbances) and state recovery (due to remedial actions). This can be seen in scenarios 0, 1B and 2B, where disturbances such as $\gamma_{r0,c1}$ and γ_{load1} cause state degradation, and the operational decision μ_{oltc} resulted in state recovery. Based on this, it can be said that the developed model satisfies FR2 (analyse degradation and recovery using state trajectory).

Structural dependence is depicted in Scenario 2A, where the failure of a PS bus (γ_{bus9}) causes the interconnected ICT components to lose power supply, resulting in a state degradation of the SE service. This also shows that the proposed model can analyse cascading disturbances. However, Scenario 1A shows that the same disturbance γ_{bus9}, when coupled with other disturbances, does not degrade the state of SE service. This shows the benefit of the proposed model in analysing not only individual disturbances but also the sequence in which they occur. On the one hand, the functional dependence of PS on the ICT system is shown in scenarios 0, 1B and 2B, where the services remedy a PS operational limit violation. On the other hand, as discussed in Sec. 3.3, disturbances can also propagate via these dependencies. This can be seen in scenarios 1A and 2A, where the PS operational limit violation is not remedied due to a state degradation in the ICT-enabled grid services. Furthermore, these scenarios also depict escalating disturbances, where certain ICT disturbances exacerbate an independent PS disturbance. This shows that the proposed model can analyse functional dependencies as well as escalating disturbances. Therefore, the proposed model satisfies FR1 (consider structural and functional dependencies) and FR3 (investigate cascading and escalating disturbances). In the presented scenarios, it can be observed that functional dependence resulted in an escalating disturbance, while structural dependence resulted in a cascading disturbance.

5.4.2 Non-functional Requirement – Adaptability

Adaptability (NFR1) evaluates the ability of the proposed model to analyse different PS and ICT disturbances. As presented in Sec. 4.1, power and ICT systems are modelled as static property graphs. The input power and ICT disturbances are considered by suitably varying the properties of the graph model. Regarding PS disturbances, the model can consider failures of PS components such as generators, DERs, transformers, power lines, loads, and buses by removing the corresponding node/edge or by modifying the corresponding property in the PS graph $\mathcal{G}^P$. Variations in active and reactive powers of generators, DERs and loads can also be considered by modifying the properties d^B of PS nodes. ICT disturbances, as shown in Tab. 3.1, can be mapped onto one or more properties of the ICT graph $\mathcal{G}^I$, i.e., availability, timeliness and correctness. The model can consider failures of ICT components such as sensors, controllers, routers, links and servers by modifying the ψ property. Variation of timeliness can be mapped onto the δ property, and variation of correctness can be mapped onto the σ property of ICT nodes and edges. These properties are then used as guard conditions in automata to assess the operational states of ICT-enabled grid services. (cf. Sec. 4.2).

A limitation of the model is that it does not consider the dynamic or temporal aspects of power and ICT systems. Consequently, the model can only analyse the order of disturbances but not when they occur. The latter would give insights into the time spent by the CPES in each of the states S^C, which is essential for designing the timeliness of remedial actions. This also limits the application of the model to study frequency, voltage and rotor angle stabilities. Along similar lines, protocols and data flows are also abstracted in the ICT system model. Although the model allows preliminary analysis of timeliness and correctness using the graph properties δ and σ, it cannot comprehensively analyse data manipulations (typically done via the protocols [117]) and congestions (typically due to re-routing of data [93]). Note that the validation of the developed model with temporal aspects will require an improved simulation setup also with temporal aspects.

To summarise, the proposed model can analyse failures of PS and ICT components, as well as variations in PS loads. They are also shown by the scenarios in Sec. 5.3. However, it lacks the dynamic and data flow aspects and can only enable a preliminary analysis of timeliness and correctness.

5.4.3 Non-functional Requirement – Extensibility

Extensibility (NFR2) evaluates the ability of the proposed model to include additional grid services. It is especially relevant when using finite state automata as they are prone to state (combinatorial) explosion, i.e., the number of states grows exponentially as the number of system variables increase [118]. In the context of RQ1, this pertains to the number of ICT-enabled grid services, since the number of PS states remains the same irrespective of the PS size. As shown in Fig. 4.4, the proposed model does not aggregate the states of grid services into a unified set of states for the whole ICT system. This is because different services are required in different operational states of the PS (cf. Sec. 2.2), and aggregation is possible only if the priority of these grid services is known. Each grid service has three operational states, therefore, a CPES with m grid services will have $3 \times m$ states. Sec. 4.2.1 shows the integration of the SE service into the proposed model, which is then followed by its extension with the VC service in Sec. 4.2.2. It can be seen that extending the proposed model with an additional grid service would result in 3 more states, representing a linear increase. This contrasts 3^m states in the case of exponential increase.

To integrate additional grid services into the proposed model, their ICT requirements should be defined in terms of the three properties – availability, timeliness and correctness. Additionally, their dependencies on other grid services should be defined. For example, the properties of the VC service are defined in Eqs. (4.13)–(4.18), and its dependence on the SE service is defined in Eq. (4.15). These properties and dependencies can then be used to determine the operational state of the grid services, modelled using the finite state automata. In this regard, defining the properties and the operational states could be challenging for decentral and distributed grid services. The three operational states may be insufficient to fully capture their performance as they typically have multiple levels of degradation. Furthermore, the Limited state can encompass a wide variety of situations, i.e. everything from fully functional (Normal) to complete failure (Failed), making it challenging to fully capture the performance of decentral and distributed grid services. Investigating other architectures of grid services (cf. Sec. 2.2.2) is part of future work and may mandate finer granular operational states. In this regard, as shown in [38], the three ICT properties can also be extended to include additional grid service-specific aspects, such as unobservability risk (SE), convergence time (SE and redispatch), and Lagrange multiplier (optimal power flow based redispatch), which may be necessary to comprehensively describe their performance and the operational states.

5.5 Chapter Summary

This chapter presents the results, discussion and evaluation of the joint operational state model from Chapter 4 (artefact of RQ1). The highlights are as follows:

- A CPES architecture consisting of the CIGRE MV benchmark grid augmented with an ICT system has been described. The ICT system has been designed based on assumptions from literature since there is a lack of standardised ICT systems for power grids. This CPES architecture also incorporates state estimation and voltage control services.
- A simulation setup consisting of Pandapower and NetworkX for modelling power and ICT systems, respectively, has been developed. Subsequently, this setup has been used to validate the results from the joint operational state model via input-output validation.
- The developed operational state model has been shown to be capable of analysing different power and ICT disturbances by suitably varying the properties of the graph model. Since the states of the grid services are not aggregated, the developed model is extensible in terms of including additional grid services without state explosion.
- Five scenarios have been simulated to show the propagation of power and ICT systems. The focus has been on analysing the impact of the power and ICT disturbances on the states of state estimation and voltage control services and, consequentially, on the power system state. The main findings are as follows:
  - The Limited state of the grid services does not necessarily have a negative impact on the interconnected power system; instead, it increases the risk of incorrect control actions in the power system.
  - Although the state estimation does not directly actuate any power system equipment, a state degradation in this service can indirectly impact the operation of the power system via the grid services that depend on it, which in this case is the voltage control. This shows the necessity of considering dependencies between the grid services in the planning and operation of CPESs.
- The identified functional requirements (FR1, FR2, FR3) and non-functional requirements (NFR1 and NFR2) for the developed joint operational state model have been shown to be fulfilled, indicating the successful answering of RQ1.

6 Assessing Resilience of ICT-enabled Grid Services

This chapter presents the methodology and the metrics developed in this dissertation to assess the resilience of grid services. It builds on the formal operational state model from Chapter 4. This chapter contributes towards RQ2 of this dissertation, and parts of this chapter have been published in [40].

6.1 Mapping Operational States to Resilience

Fig. 6.1 depicts the three operational states of an ICT-enabled grid service, namely Normal N, Limited L and Failed F. The state transitions occur due to the events, i.e., disturbances or recovery actions, which can be given as input to automata models from Sec. 4.2. Disturbances can degrade the operational state, resulting in the transitions NF, NL and LF, whereas recovery actions can improve the state, resulting in the transitions LN, FN and FL. Depending on the ICT system and the grid services, certain disturbances and recovery actions may not necessarily result in a state change. These are represented by the self-transitions NN, LL and FF.

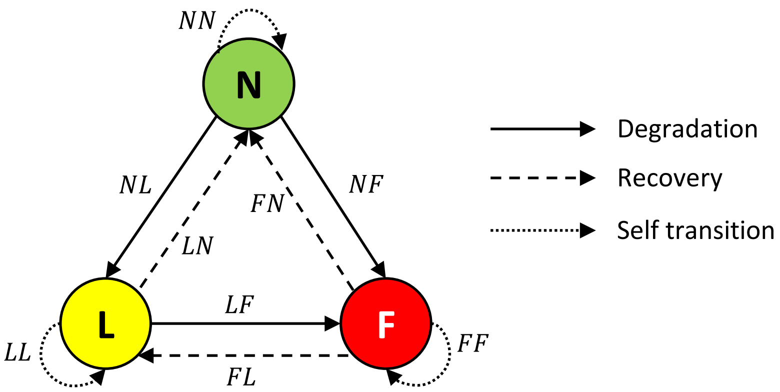


Fig. 6.1: Operational states and transitions of an ICT-enabled grid service.

As discussed in Sec. 2.7.2, the authors of [19] use the PS operational states to measure its performance. This idea is extended in this dissertation to ICT-enabled grid services. Fig. 6.2 shows the mapping of the developed operational states of a grid service to the concept of resilience. It can be seen that L and F states correspond to partial and complete performance degradation, respectively. Disturbances affecting critical and non-critical components can cause NF and NL transitions, respectively. Along similar lines, repairs of critical and non-critical components can cause FN and FL transitions. Since disturbances are uncontrollable and inevitable, these states can repeat throughout the lifetime of a grid service. Furthermore, due to the inclusion of the time dimension in Fig. 6.2 when compared to Fig. 6.1, the self-transitions are across a time span. This can be seen in the NN and LL transitions and is elaborated further in Sec 6.2. Based on this, the transitions among the operational states can be mapped to the four phases of resilience as follows:

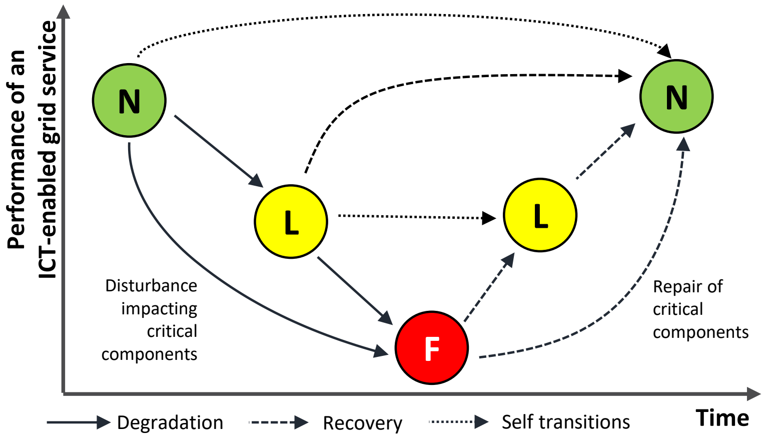


Fig. 6.2: Mapping operational states of an ICT-enabled grid service to the resilience curve.

- *Robustness* can be captured by NN, implying that the input event (disturbance or recovery action) does not result in performance degradation and the grid service stays in the N state. This is typically due to disturbances affecting components that are redundant to the grid service.
- *Absorption* can be captured by NL, implying that the input event has caused a performance degradation in the grid service, but the service has not failed. This is typically due to disturbances affecting components that are not critical to the grid service.
- *Stabilisation* can be captured by LL, which shows the ability of the grid service to maintain itself in a degraded L state without failing. This phase is due to the fallback measures in the grid services (cf. Sec. 3.2).
- *Recovery* can be captured by LN, implying that the grid service is restored to normal performance. This is typically done via recovery actions on the ICT

components (e.g., repairing components, rebooting servers, rerouting data flow), which the grid service depends on.

It can be seen that the phases of resilience can be mapped to the transitions within as well as between the N and L states. The resilience of a grid service can then be assessed based on how often each phase occurs in the operational state trajectory.

6.2 Proposed Methodology

The proposed methodology aims to assess the resilience of each grid service in the ICT system in order to support the choice of ICT design options. Fig. 6.3 depicts the proposed methodology. The input is ICT network information consisting of ICT components, their interconnections (or topology), and their failure and repair rates. While ICT components and topology are from the ICT graph $\mathcal{G}^I$ (cf. Sec. 4.1), the failure and repair rates can be acquired from utility data as shown in [25, 89]. The following sections discuss the different blocks of Fig. 6.3.

6.2.1 Generate Input Events

The finite state automata from Sec. 4.2 can determine the operational state of grid services for specific input events, i.e., disturbances and recovery actions, in the ICT system. To assess the performance and, consequently, the resilience of grid services, a wide range of input events should be considered as resilience is not only about individual disturbances but also about a range of disturbances and recovery actions (cf. Sec. 2.7.2). In other words, for a given ICT system, the input events should be generated in a generalised manner considering the typical events the system will encounter during its lifetime. This is essential as the results are intended to support the design of ICT systems. In this regard, a probabilistic approach is required as disturbances are stochastic in nature. Based on [25, 19], the sequential Monte Carlo (SMC) method is used in this dissertation. It is a systematic approach that simulates the behaviour of a system as a sequence of random events that build upon each other as the system progresses through time. The SMC method can assess the operational state of each grid service at any desirable time using the state of the individual ICT components, which are considered input events.

The SMC method requires a component behaviour model that determines the state of each ICT component and the duration for which the component stays in each

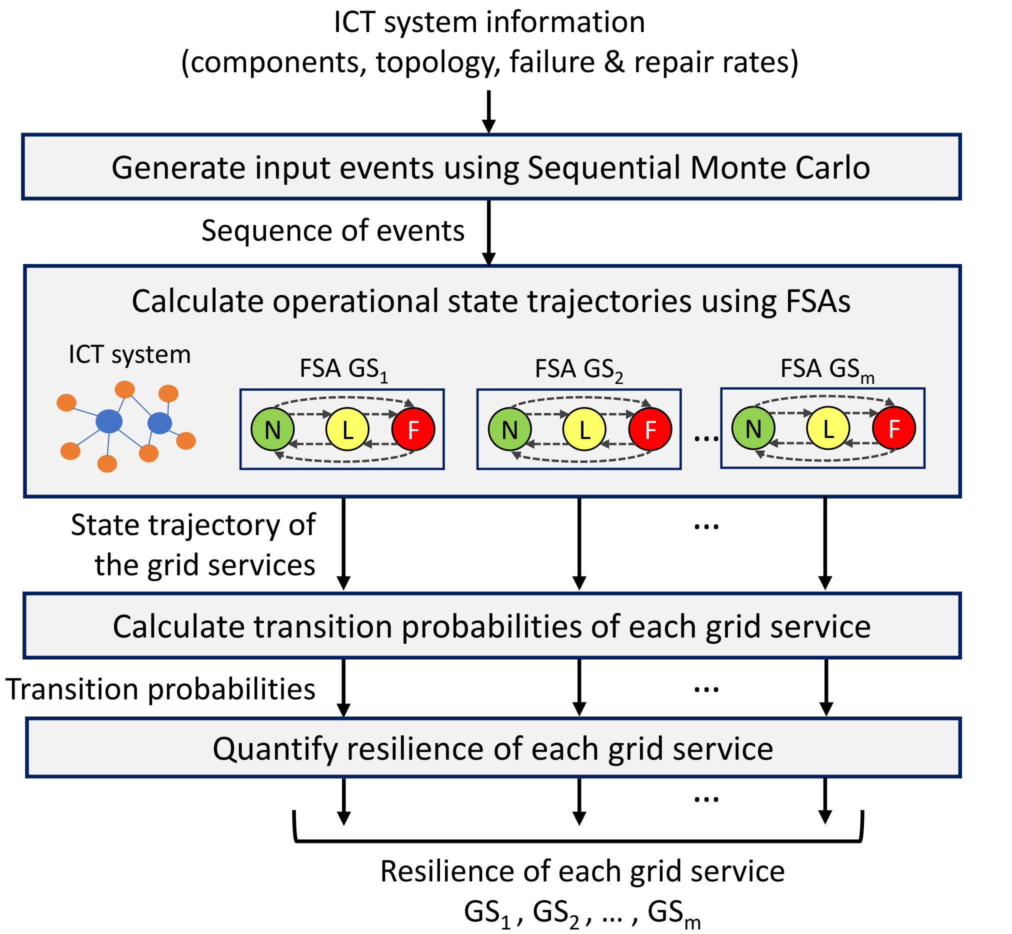
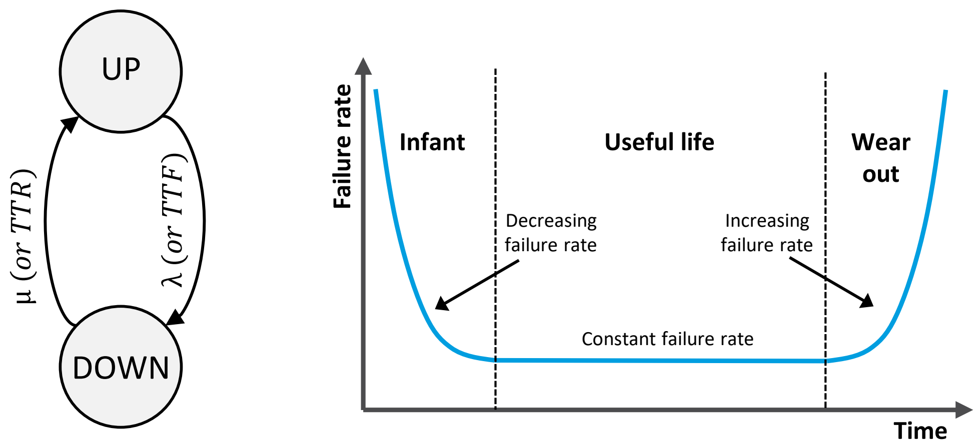


Fig. 6.3: Proposed methodology to assess the resilience of ICT-enabled grid services. FSA denotes finite state automaton.

state. As discussed in Sec. 2.6.1, ICT components can be represented by a two-state model as shown in Fig. 6.4a, where λ and μ are the failure and repair rates of the component. According to this model, a component transitions between fully functional (UP) and out-of-service (DOWN) states, with the rates determining the frequency of transitions. The time the component stays in the UP and DOWN states is called time to fail (TTF) and time to repair (TTR), respectively. In this dissertation, ICT components are assumed to operate in their *useful life*. This is because components are typically used only in this phase as their failure rate changes drastically outside this phase [119]. Fig. 6.4b depicts the lifetime of an exemplary component and shows that in contrast to the infant and wear-out phases, the *useful life* has a constant failure rate. Note that the drastic increase in the failure rate of a component in its infant and wear-out phases can be mitigated by carrying out field prototype tests and maintenance, respectively [119].



(a) Two-state model of a component [25].

(b) Useful life of a component [119].

Fig. 6.4: Modelling the behaviour of an ICT component.

The exponential distribution model can now be used as it accurately models the behaviour of components in this phase [25]. Accordingly, the TTF and TTR for an ICT component c can be calculated as:

$$TTF^c = \frac{-ln(U_1)}{\lambda^c}, \qquad TTR^c = \frac{-ln(U_2)}{\mu^c}. \tag{6.1}$$

Here, λ^c and μ^c are the failure and repair rates of the component c, and U_1 and U_2 are two uniform random numbers in the interval $(0, 1]$. Note that λ^c and μ^c are constant during the *useful life* of c. An operating or UP–DOWN sequence of a component c can now be generated by alternatively sampling values of TTF^c and TTR^c using Eq. (6.1). This can then be extended to all components of the

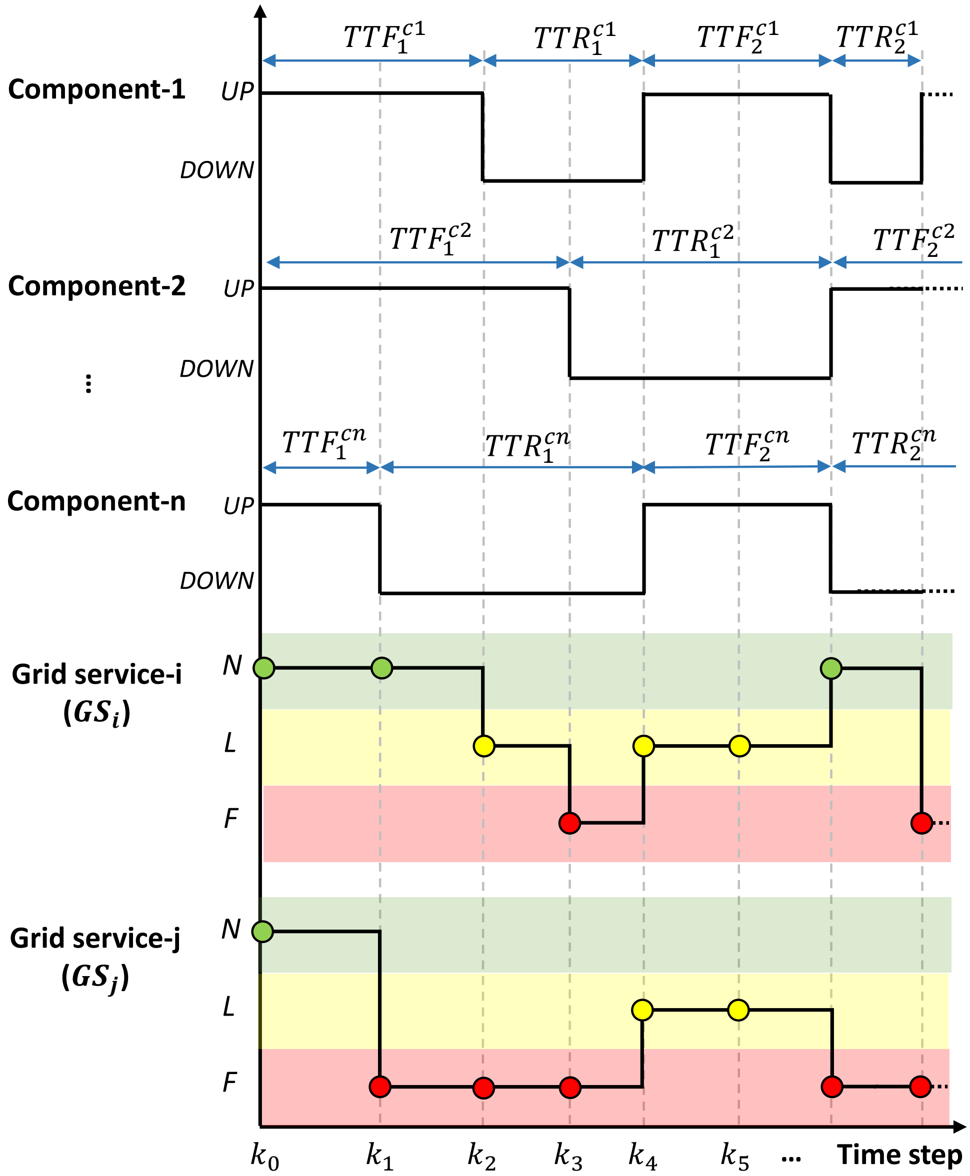


Fig. 6.5: Exemplary sequence of inputs of three ICT components and state trajectories of two grid services.

ICT system by considering their respective failure and repair rates. All components are initially assumed to be in the UP state, implying that the ICT system has no inherent disturbances. The top three curves of Fig. 6.5 show operating sequences of three exemplary ICT components. The values of TTF and TTR in the figure are different from each other as they are calculated using the random numbers U_1 and U_2. This method generates different combinations of failure and repair sequences, all of which are input events to the proposed methodology.

6.2.2 Calculate Operational State Trajectories

At each time step k, the set of states of all ICT components is given as an input to the ICT submodel in Fig. 4.4, which consists of the ICT graph $\mathcal{G}^I$ and finite state automata of m grid services. The graph $\mathcal{G}^I$ and its properties are modified based on the states of components, resulting in transitions in the finite state automata if the corresponding guard conditions are met (cf. Sec. 4.2). When repeated for several time steps, this results in a sequence of operational states, i.e. the state trajectory, for each of the m grid services. As shown in Fig. 6.5, each grid service has its own trajectory from the corresponding automaton.

The last two curves of Fig. 6.5 show the operational state trajectories of exemplary grid services GS_i and GS_j. The state of both GS_i and GS_j at k_0 is N, since all components are initially UP. The state of GS_i is N at k_1 as well, indicating an NN transition. This implies that the service GS_i is robust to the input at k_1, which in this case is the failure of component-n (third curve in Fig. 6.5). However, at the same time step, the service GS_j is in the F state, indicating that the component-n is critical for GS_j. The resulting state trajectories have both state degradations (e.g., NL from k_1 to k_2 for GS_i) as well as state recoveries (e.g., FL from k_3 to k_4 for GS_j). It is evident that the SMC method can model the impact of simultaneous component failures and repairs on the grid services. For example, components 1 and n are DOWN at k_2 and are simultaneously repaired at k_4. The service GS_i degrades slower and recovers quicker than GS_j. While GS_i transitions back to L state at time step k_4, GS_j remains in F state for several time steps. Furthermore, GS_j appears to be more sensitive to the state of component-n because when component-n fails, GS_j transitions to F irrespective of the states of the other components. An example of this is the OLTC controller, which is critical for the VC service (cf. Sec. 3.4.2).

Due to the discrete-event nature of the ICT system (cf. Chapter 4), the state and transitions of a grid service are also discrete, i.e., transitions occur instantly at time steps without slopes, unlike the bathtub curve in Fig. 1.1. Due to the same reason, the horizontal axis of Fig. 6.5 has time steps (instead of continuous time), which is decided by the rates λ^c and μ^c in Eq. (6.1). Also, as already shown in Fig. 6.2, the self transitions occur across time steps, e.g., GS_j remains in F state from k_1 to k_4 indicating two FF transitions. Furthermore, since the grid services transition between discrete operational states, the vertical axis of Fig. 6.5 corresponding to the two services has no depth, i.e., only the colour and the location of the circles are relevant, but not their position within the shaded area.

6.2.3 Calculate Transition Probabilibities

From the state trajectory of each grid service, the probabilities p of the nine transitions shown in Fig. 6.1 can be computed. By definition of the automaton model from Sec. 4.2, these nine transitions are exhaustive for a grid service, and therefore, the sum of these nine transition probabilities should be one, i.e.,

$$\sum p^{xy} = 1, \forall x, y \in \{N, L, F\} \tag{6.2}$$

These probabilities are calculated at each time step k as the SMC is simulated in increasing time steps. The stochasticity of the SMC, introduced due to Eq. (6.1), mandates a stopping condition that determines the number of time steps required to achieve the desired level of confidence in the results, which in this case are the transition probabilities. If simulated for too few time steps, the sample mean will not fully capture the underlying distribution, yielding unrepresentative results [120]. Simulating for too many time steps, on the other hand, would consume unnecessary computational resources. The convergence condition used in this dissertation is based on the absolute error of transition probabilities and can be written as

$$Z \cdot \frac{S_k^p}{\sqrt{k}} < 0.01. \tag{6.3}$$

Here, k is the total number of samples (or time steps), S_k^p is the variance of the k samples of a transition probability p, and Z is the standard normal value for the required confidence. For a confidence level of 95%, the value of Z is 1.96. The term $S_k^p/\sqrt{k}$ denotes the absolute difference, i.e., error, between the true mean of the underlying distribution and the mean of k samples. The SMC simulation is stopped when the absolute error of all transition probabilities for each grid service considered satisfies Eq. (6.3). In other words, the nine transition probabilities of the grid services are computed using their respective state trajectories until the time step k, at which the absolute error is less than 1%.

6.2.4 Metrics to Quantify Resilience of Grid Services

As discussed in Sec. 2.7.2, metrics are essential to quantify the resilience of the grid services in an ICT system. In this dissertation, metrics are derived using the aforementioned probabilities of transitions between the operational states. This is because, as explained in Sec. 6.1, these transition probabilities can be mapped onto the phases of resilience.

The metrics to capture the four phases of resilience (cf. Fig. 1.1) can be defined as:

$$R^H = p^{NN}, \tag{6.4}$$
$$R^A = p^{NL}, \tag{6.5}$$
$$R^S = p^{LL}, \tag{6.6}$$
$$R^R = p^{LN}. \tag{6.7}$$

Here, R^H, R^A, R^S, and R^R are the metrics that capture robustness (or hardening), absorption, stabilisation and recovery, respectively. The different values of p represent the corresponding transition probabilities, e.g., p^{NN} denotes the probability of NN transition, capturing robustness, and p^{LN} denotes the probability of LN transition, capturing recovery. The following metric R, which quantifies the resilience of a grid service, can now be defined using Eqs. (6.4) - (6.7).

$$R = e\,(R^H + R^A + R^S + R^R), \tag{6.8}$$

$$\text{where, } e = \begin{cases} 0 & (R^A > 0 \vee R^R > 0) \wedge R^A \times R^R = 0, \\ 1 & \text{otherwise.} \end{cases} \tag{6.9}$$

In this equation, the coefficient e ensures that the operational state trajectory of the grid service has both absorption and recovery, as they are mandatory phases from a resilience viewpoint. This is because a resilient service can absorb a disturbance and instantly recover from it, making the stabilisation phase optional. The value of e is zero when the trajectory does not have an absorption or a recovery phase. Since the metric R is calculated based on dependent probabilities (Eq. (6.2)), its domain is $[0, 1]$, and the resulting value is dimensionless. $R = 1$ indicates the highest probability of resilient behaviour of a grid service with its state trajectory consisting only of transition between and within N and L states, i.e., robustness, absorption, stabilisation and recovery. On the other hand, $R = 0$ indicates that the probability of resilient behaviour is zero, implying that the service is not resilient. $0 < R < 1$ indicates that the service has some probability of resilient behaviour. This means that its trajectory enters the F state at least once but also has at least one absorption and one recovery phase, which need not necessarily be consecutive. In addition to answering whether a grid service is resilient or not, the R metric also answers *how much* is the resilience of a grid service.

Eq. (6.8) shows that the resilience of a grid service depends only on p^{NN}, p^{NL}, p^{LL} and p^{LN}, i.e., the probabilities of transitions within and between N and L states. The reason is that transitions to the F state, as shown in Fig. 1.1, are considered non-resilient behaviour. The transitions to and within the F state, however, give certain valuable insights into specific behaviours of a grid service. For example, a disturbance causing a NF transition can be regarded as a high-impact event as it causes the grid service to instantly fail without entering the L state (e.g., server crash for the SE service). The FF transition captures the inability of a grid service to exit the F state, which hints at the required repair effort to recover the grid service from this state. Evidently, integrating these transitions into the metric will result in a better and more holistic resilience quantification of a grid service. Accordingly, the two following metrics are defined.

$$R^F = p^{NF} + p^{LF} + p^{FF} \tag{6.10}$$

$$\hat{R}^R = \hat{R}^{R,N} + \hat{R}^{R,L} + R^R \tag{6.11}$$

$$\text{where, } \hat{R}^{R,N} = p^{FN} \text{ and } \hat{R}^{R,L} = p^{FL}$$

Here, R^F is the failure metric (or the failure probability) that captures the (dis)ability of a grid service to enter and stay in the F state, and $\hat{R}^R$ is the extended recovery metric, which, in addition to R^R (Eq. (6.7)), also includes the recovery transition from the F state. Considering this, a metric R^{MOP}, which measures the performance of a grid service from a resilience viewpoint, can be defined as:

$$R^{MOP} = w^N (R^H + R^R + \hat{R}^{R,N}) + w^L (R^A + R^S + \hat{R}^{R,L}) - w^F (R^F) \tag{6.12}$$

Here, $w^N, w^L, w^F \in [0, 1]$ are the weights of the transitions to N, L and F states, respectively and can be used to weigh the contribution of each state to the overall performance of a grid service. Typically, $w^N > w^L$ since a grid service is preferred to be in the N state over L. Since a failure is an undesired behaviour from the resilience viewpoint, the performance metric R^{MOP} is penalised by the failure metric R^F. As a result, the domain of R^{MOP} is $[-1, 1]$ (maximum value of R^F is 1), and its value is dimensionless. Note that a higher value of all metrics, except R^F, indicates a better performance of the corresponding grid service.

Although the metric R in Eq. (6.8) captures resilience as discussed in 2.7, several state trajectories can have an R value of one. Examples include (i) a service that stays in the N state with only NN transitions, (ii) a service that oscillates between N and L states, and (iii) a service that enters L, stays there for a long time with several LL transitions and then recovers to N state. The reason is, according to Sec. 2.7.1, all these three behaviours are considered to be resilient. This makes it challenging to compare the grid services solely based on the R metric. In such cases, the metric R^{MOP} from Eq. (6.12) can be used along with R to assess the performance of a grid service. Therefore, the resilience and the performance of individual grid services can be quantified using Eqs. (6.8) and (6.12). Furthermore, the developed metrics are modular, i.e., the phases can be analysed individually as well as in combination with others to quantify the overall resilience of a grid service.

As discussed in Sec. 2.7.2, some literature view robustness as a phase of resilience, while others do not. In the latter case, Eqs. (6.8) and (6.12) can be adapted by removing the R^H (robustness metric) term. Then, the other metrics have to be scaled accordingly for R and R^{MOP} to have the same domain, i.e., $[0, 1]$ and $[-1, 1]$, respectively. In contrast to the unbounded metrics in the literature, the proposed metrics are bounded, which makes them easy to comprehend. Therefore, they can be used to compare the resilience of different grid service architectures and design choices, e.g., central vs distributed. This can support ICT system design with the aim of improving the resilience of the grid services it enables.

Note that one of the most popular approaches in the literature when dealing with transition probabilities is to calculate steady-state probabilities by constructing a discrete-time Markov chain (DTMC) [25]. Steady-state probability pertains to the long-term probability that a system will be in each state, which can then be used for reliability calculations. This is, however, not used in this dissertation as both states and transitions are relevant for resilience. For example, as described in Sec. 6.1, a LN transition is considered as a part of resilience but not FN, even though both transitions result in the N state. The steady-state probability only captures the probability of being in the states and not the transitions.

6.3 Illustrative Example

Fig. 6.6 illustrates the proposed metrics using six exemplary operational state trajectories of grid services GS_1 to GS_6. These trajectories are designed to illustrate certain possible results from the metrics. The SMC simulation is assumed to have converged within six steps in all these cases. The corresponding R and R^{MOP} values are shown in the figure. These calculations consider exemplary weights of $w^N = 1$, $w^L = 0.5$ and $w^F = 1$. As a result, $R^{MOP} = 1$ indicates that the service remains in the N state (best possible performance). If $0 < R^{MOP} < 1$, the grid service is in the N and L states more than the F state. However, $R^{MOP} < 0$ indicates that the service is expected to enter in F state frequently (R^F is greater than the sum of the other terms in Eq. (6.12)), despite the repairs considered in the input events.

The trajectories of GS_1 and GS_2 exhibit a 100% probability of resilient behaviour, i.e., $R = 1$. While GS_1 never degrades, GS_2 has both absorption and recovery

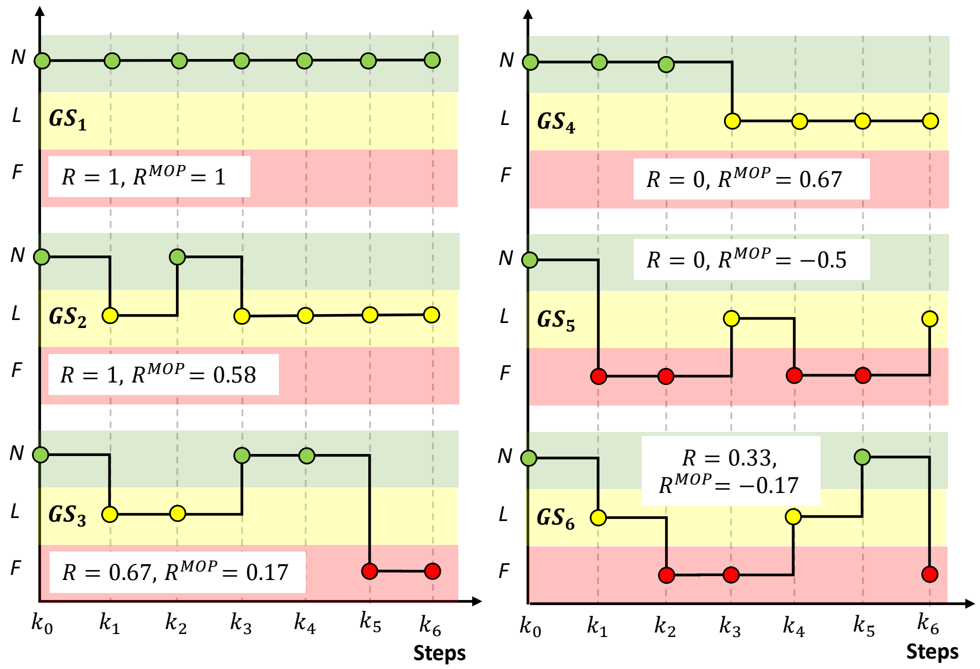


Fig. 6.6: Exemplary state trajectories of six grid services to illustrate the proposed metrics.

phases without entering the F state. However, the latter has a worse performance, i.e., lower R^{MOP}, as it enters the L state more than GS_1.

The trajectories of GS_4 and GS_5 exhibit zero probability of resilient behaviour, i.e., $R = 0$. The service GS_4 has absorption at k_3 but never recovers from the L state, whereas GS_5 fails often with neither absorption nor recovery. In such cases, the R^{MOP} metric can be used to compare and identify the better performance, which would be GS_4 because of fewer transitions to F state. This also indicates that it would be easier to improve the resilience of GS_4 when compared to GS_5.

From the trajectory of GS_3 and GS_6, it can be seen that both grid services have a positive probability of resilient behaviour despite entering the F state multiple times. However, the R^{MOP} of GS_6 is negative, while that of GS_3 is positive because the former has more transitions to the F state. This indicates that GS_3 has a better performance than GS_6.

Overall, while GS_1 depicts the ideal grid service from a resilient viewpoint, GS_2 is the second best considering both resilience probability R and performance R^{MOP}. Due to the broad and rapidly changing disturbance landscape in ICT systems, designing grid services such as GS_1 would be impractical in real systems. Although GS_4 has a higher R^{MOP} than GS_2 and GS_3, GS_4 is considered worse from a resilience viewpoint because it has zero resilient behaviour probability ($R = 0$). However, from a purely operational states perspective, GS_4 exhibits the second-best performance. It can be seen that the aggregated metrics abstract the contribution of the individual phases but can enable the comparison of the resilience of ICT-enabled grid services. Note that changing the weights would result in different values of R^{MOP}.

6.4 Chapter Summary

This chapter presents the artefact of RQ2, which aims to quantify the resilience of ICT-enabled grid services in CPESs. The highlights of this chapter are as follows:

- The concept of the resilience of ICT-enabled grid services has been proposed, where the transitions between the three operational states (Normal, Limited and Failed) have been mapped to phases of resilience. While certain transitions (e.g., Normal to Limited) are deemed as resilient behaviour, others are not (e.g., Normal to Failed).
- A methodology to assess the resilience of grid services has been developed using sequential Monte Carlo simulations, incorporating the ICT graph and finite state automata models from Chapter 4. The behaviour of ICT components has been modelled using an exponential distribution model assuming that they are operating in their *useful life*. Subsequently, this has been used to simulate typical events (failures and repairs) that the ICT components can encounter during their lifetime.
- Two dimensionless metrics to quantify resilience have been developed based on the probability of the nine state transitions.
  - The metric R quantifies the probability of resilient behaviour along with the four constituting phases, namely, robustness, absorption, stabilisation and recovery.
  - The metric R^{MOP} measures the performance of a grid service, including the Failed state. In this metric, the contribution of each operational state to the overall performance can be weighed.
- These metrics have been illustrated using six exemplary operational state trajectories, based on which the developed methodology can quantify their resilience. The illustration shows that the proposed metrics can compare the resilience and performance of different grid services.

7 Resilience of ICT-enabled Grid Services – Results & Discussion

This chapter presents the simulation results of the method and metrics to quantify the resilience of ICT-enabled grid services from Chapter 6, which is the artefact of RQ2. This chapter also demonstrates the artefact and evaluates the corresponding functional and non-functional requirements. Note that parts of the contents of this chapter are published in [40].

7.1 Scenario Design

The simulation scenario includes an ICT network with SE and redispatch services. A detailed description of these grid services and their operational states is presented in Secs. 3.4.1 and 3.4.3, respectively. This section presents their state classification adapted to the SMC simulation of the proposed resilience assessment methodology from Chapter 6. Since the RQ2 of this dissertation focuses only on the ICT aspects, the simulation of the grid services presented in this chapter is from an ICT viewpoint and abstracts the power grid aspects. This is also because only the operational states and transitions of a grid service are relevant to its resilience assessment.

7.1.1 State Estimation Service

Fig. 7.1 shows the process to assess the operational state of a SE service, denoted as s^{SE}. This process is executed at each time step k of the SMC simulation. Since a central WLS implementation is considered, the unavailability of a suitable server causes the SE service to transition to its F state unless for a backup or a redundant server. If at least one server is available, the solvability condition from Eq. (3.1) is checked with the field measurements available at that time step at the server. If this condition is satisfied, the state of SE service is N. If not, suitable pseudo-measurements are used, and the condition is rechecked. If the solvability is satisfied using pseudo-measurements, the state of SE service is L; else, the state of SE service is F. The solvability condition can also be violated if the required pseudo-measurements are unavailable or too many field measurements are lost, thereby requiring too many pseudo-measurements. A threshold $\Phi^{PM,th}$ is defined for the maximum number of pseudo-measurements that could be used in each run of SE, which happens at each time step k. Since pseudo-measurements are based on historical data, using too many pseudo-measurements will cause a large difference between the SE results and the actual PS state. This threshold $\Phi^{PM,th}$ is usually defined by the system operator based on the observability of the grid and the acceptable level of uncertainity [94]. This process, when repeated until the SMC convergence (cf. Sec. 6.2.3), results in the operating state trajectory of the SE service.

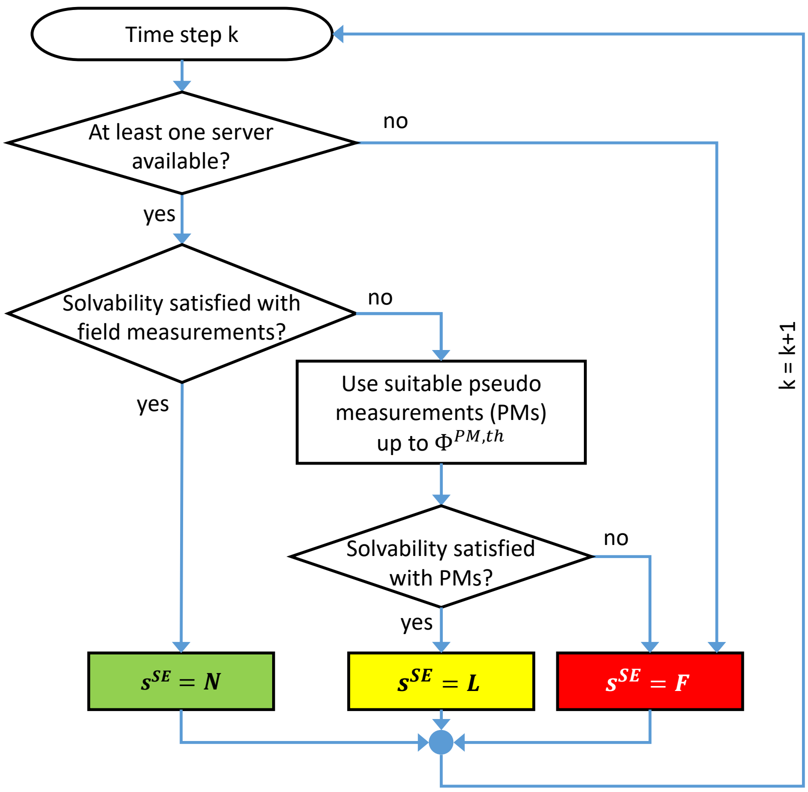


Fig. 7.1: Flowchat showing operational state assessment of state estimation service. PMs stands for pseudo-measurements.

7.1.2 DER Redispatch Service

Fig. 7.2 shows the process to assess the operational state of the redispatch service, denoted as s^{RD}. This process is also executed at each time step k of the SMC simulation. The redispatch service is only deployed if an operational limit violation is detected based on the SE results. Since the focus here is on the resilience of the redispatch service from an ICT point of view, certain simplifications are made on the PS side. An exemplary central redispatch is considered with the goal of meeting a flexibility target (f^T) using the total flexibilities of the available DERs (f^A). All DERs are assumed to offer equal flexibility, in this case, only active power, at the same cost and are abstracted based on their respective DER controllers. At each time step k, the value of f^T is chosen randomly between zero and maximum flexibility in the grid to simulate the remedying of different operational limit violations. Here, small values of f^T correspond to small operational limit violations. Each DER has a binary property $\sigma^{\eta,k}$ representing its uncertainty (correctness) at time step k. A DER-η can only guarantee its flexibility at k if $\sigma^{\eta,k} = 1$. As discussed in Sec. 3.4.3, this property differentiates the N and L states of the redispatch service. Furthermore, the attribute $p^{DER,\sigma}$ denotes the probability of uncertain DERs, which determines the number of uncertain DERs at each time step and is kept constant ($p^{DER,\sigma} = 0.3$) across all time steps. This implies that, at each k, 30% of DERs (chosen randomly) will be uncertain with their respective $\sigma^{\eta,k}$ set to zero.

Since a central redispatch is considered, the unavailability of a suitable server causes the grid service to transition to its F state (similar to SE in Fig. 7.1) unless for a backup or a redundant server. If at least one server is available, the state of the SE service s^{SE} is checked. Since the redispatch service depends on the SE service for detecting the operational limit violations, the redispatch service will transition the F state when $s^{SE} = F$. Note that this is true only for central redispatch from the control room and could be different for other architectures as shown in [57]. If $s^{SE} \neq F$, the values of f^T and $p^{DER,\sigma}$ are chosen as mentioned above. The total flexibility available is then calculated based on the DERs, which are reachable from the server. While f^A denotes the available flexibility using all reachable DERs, $f^{A,\sigma}$ denotes the available flexibility using only the reachable and guaranteed DERs, i.e., the DERs with $\sigma^{\eta,k} = 1$. ICT disturbances impacting the DER controllers or the IT network can impact the values of f^A and $f^{A,\sigma}$. The state of the redispatch service s^{RD} is N if the target f^T could be met using only guaranteed DERs and is L if meeting f^T requires at least one uncertain DER. Similar to the case of pseudo-measurements for the SE service, the threshold $\sigma^{\eta,th}$ indicates the maximum number of uncertain DERs that could be used. The redispatch service is in its F state if the

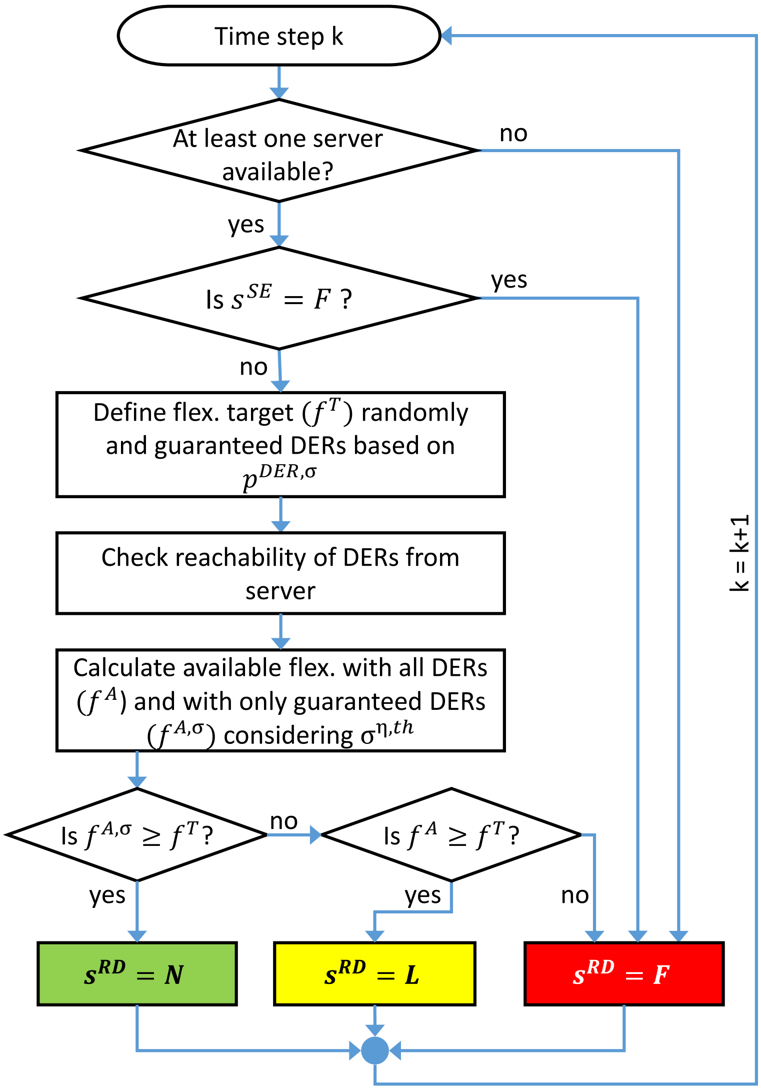


Fig. 7.2: Flowchat showing operational state assessment of DER redispatch service.

target cannot be met with the available flexibilities, considering both guaranteed and uncertain DERs up to $\sigma^{\eta,th}$. This process, when repeated until the SMC convergence (cf. Sec. 6.2.3), results in the operating state trajectory of the redispatch service.

7.1.3 Design of ICT Systems

Fig. 7.3 shows two ICT system designs $D1$ and $D2$, both with SE and redispatch services, for the CIGRE MV benchmark power grid and follows the description in Sec. 5.1.1. Since there is a lack of standard ICT system designs for CPESs, these designs represent two possibilities considering the increasing penetration of ICT in distribution grids and are based on [11, 48]. The components considered are sensor IEDs, controller IEDs, servers, ICT nodes (representing routers), LAN links (intra-substation) and WAN links (inter-substation). The ICT nodes are associated with the PS buses and are numbered accordingly. In design $D1$, 8.1 and 8.2 represent redundant nodes for the servers, both of which are located at the same bus. Note that, similar to Sec. 5.1.1, the terms sensors and controllers refer to the IEDs performing sensing and actuation, respectively.

The design of the ICT system, which includes the design of the grid services, influences the performance and, consequentially, the resilience of the grid services. Tab. 7.1 summarises the factors differentiating designs $D1$ and $D2$. They are chosen to include hardware-based factors (e.g., observability, number of DERs, meshing, redundancy) as well as software-based (or algorithmic) factors (e.g., thresholds for pseudo-measurements and uncertain DERs). While observability and pseudo-measurement threshold pertain to the SE service, the number of DERs and uncertain DERs threshold pertain to the redispatch service. Network topology and server redundancy are general design factors for all grid services in the ICT system. Although several other factors exist for designing ICT systems with grid services (examples in Sec. 2.2.2), the simulations in this section consider the ones in Tab. 7.1. This is because the goal is to show the ability of the proposed methodology and metrics to assess the resilience of grid services considering different ICT designs and not to design the most resilient ICT system with the grid services. Analysis of further design factors is part of future work. The design factors considered are as follows:

Observability: This is the percentage ratio of the number of sensors to buses. While the power grid has 15 buses, the ICT system design $D1$ has 13 sensors (87 % observability), and $D2$ has 10 sensors (66 % observability). The location of sensors in $D1$ and $D2$ is shown in Fig. 7.3.

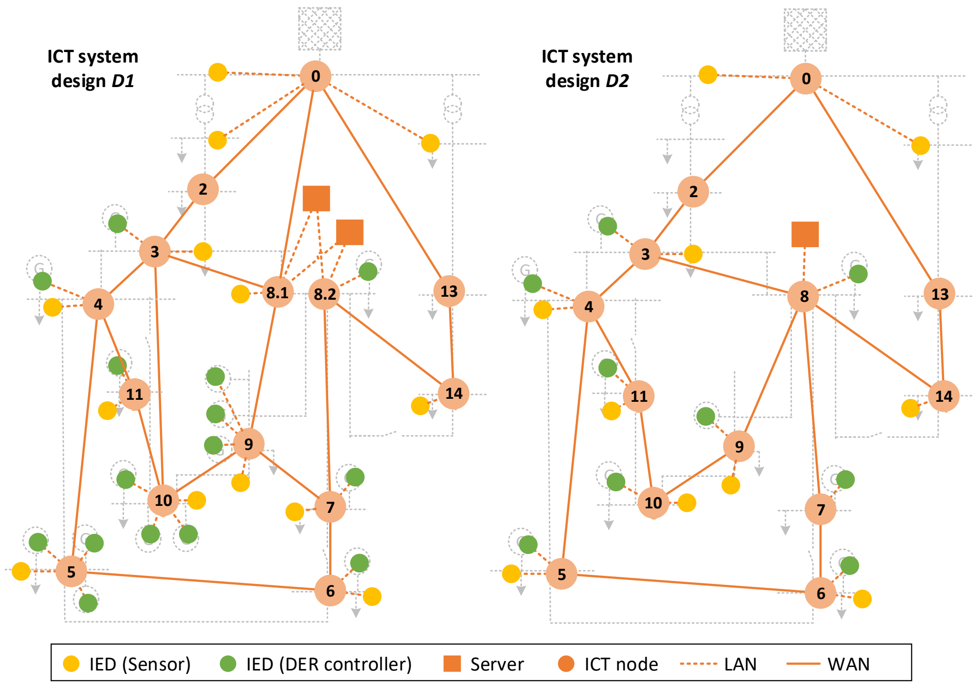


Fig. 7.3: ICT system designs D1 and D2 for the CIGRE MV grid, which is shown in grey background.

Pseudo-measurement threshold ($\Phi^{PM,th}$): Pseudo-measurements can be used when the solvability condition cannot be satisfied using field measurements. $\Phi^{PM,th}$ dictates the maximum number of pseudo-measurements that can be used. Designs $D1$ and $D2$ can use up to 15% and 50% of pseudo-measurements, respectively. This corresponds to two sensors (15% of 13 sensors), i.e., buses 8 and 14 for $D1$ and five sensors (50% of 10 sensors), i.e., buses 3, 5, 9, 10 and 14 for $D2$.

Number of DERs: The redispatch service uses the flexibility of DERs to meet the target f^T. To compare the resilience of the service between the two ICT system designs, the total available flexibility in both designs is capped at $3079\,\text{kW}$ as per [113]. Since the DERs are assumed to have the same flexibility (cf. Sec. 7.1.2), the 9 DERs of $D1$ are each $342.1\,\text{kW}$ and the 15 DERs of $D2$ are each $205.3\,\text{kW}$.

Uncertain DERs threshold ($\sigma^{\eta,th}$): This is a percentage of the number of uncertain DERs to the total number of DERs used. Uncertain DERs are used when the target f^T cannot be met using guaranteed DERs. While design $D2$ can use up to 50% uncertain DERs to meet f^T, $D1$ can only use up to 10%.

Server redundancy: As shown in Figs. 7.1 and 7.2, a server failure will cause both grid services to fail. While design $D1$ has redundant servers as well as ICT nodes

Tab. 7.1: Factors differentiating the two ICT system designs.

	Factors	System *D1*	System *D2*
SE	Observability	87%	66%
	Pseudo-measurement threshold ($\Phi^{PM,th}$)	2 (buses 8,14)	4 (buses 3,5, 9, 10,14)
Redispatch	Number of DERs	15	9
	Uncertain DERs threshold ($\sigma^{\eta,th}$)	20%	50%
All	Server redundancy	yes	no
	Network topology	Same as $D2$ with links between 0-8.1, 3-10, 7-9	Based on PS topology

and links to which the servers are connected, design $D2$ has a single server, i.e., a single point of failure.

Network Topology: This represents the meshing (or connectivity) between the ICT nodes via WAN and LAN links. While design $D2$ follows the same topology as the PS (based on Sec. 5.1.1), $D1$ is more meshed and has additional links between nodes 0-8.1, 3-10, and 7-9.

In addition to ICT system designs, the SMC method requires the failure rate λ^c and repair rate μ^c for ICT components (cf. Eq. (6.1)). For simplicity, based on [25], uniform values of $\lambda^c = 0.009\,h^{-1}$ and $\mu^c = 0.2\,h^{-1}$ are assumed for all the ICT components in Fig. 7.3. This assumption could, however, easily be removed by using suitable rates from the literature in Sec. 2.7.2 and is recommended for future work. Using these rates, the input events can be generated as explained in Sec.6.2.1 of the proposed methodology. It is to be noted that the failure of components can happen due to various possible disturbances (cf. Tab. 3.1).

7.2 Results & Discussion

This section presents the results of the resilience assessment methodology from Chapter 6 considering the designs $D1$ and $D2$. The aim is to show that the methodology can quantify the resilience of grid services considering different ICT design factors. Similar to the results of RQ1 in Chapter 5, the ICT designs and the operational states of the grid services are modelled and simulated as property graphs in NetworkX[1]. Based on the input events, the SMC method converged in 14,900 and 11,108 steps

[1] NetworkX: https://networkx.org/ (Accessed: May 3, 2023)

for $D1$ and $D2$, respectively. This is because $D1$ has more ICT components than $D2$, which implies that $D1$ has more variability in the input events due to the increased number of operating sequences (cf. Sec. 6.2.2). The resulting state trajectories of SE and redispatch services are then used to compute their respective transition probabilities as shown in Sec. 6.2.3. Their resilience and performance can then be calculated using the metrics in Sec. 6.2.4.

Fig. 7.4 shows the phases of the resilience of SE and redispatch services, including the transitions to and from the F state. The values are computed using Eqs. (6.4) - (6.7), (6.10) and (6.11). Therefore, the values of R^H, R^A, R^S, R^F, $\hat{R}^R$ adds up to one (the value of R^R is included in that of $\hat{R}^R$). The aim is to compare the resilience of SE and redispatch services between the ICT designs and not between the grid services themselves. The results show that for both grid services, design $D1$ is more robust (higher R^H) compared to $D2$, meaning that the services in $D1$ have more resistance to degradation from the N state. This can be attributed to the hardware-based design factors. The higher observability enables the SE service to withstand an increased number of sensor failures, whereas the more the number of DERs, the more robust the redispatch service is to their failure (assuming that the DERs have the same flexibility). Server redundancy benefits both grid services since they both have a centralised architecture and, therefore, require the server (cf. Figs. 7.1 and 7.2). With more meshing, sensors and DER controllers have more communication paths to the server, which increases their robustness against IT (WAN and LAN) disturbances.

On the other hand, design $D2$ has higher values of absorption (R^A) and stabilisation (R^S) metrics than design $D1$. In the case of SE, a higher pseudo-measurement threshold allows $D2$ to use more pseudo-measurements to further compensate for the loss of field measurements caused either by the failure of sensors themself or the communication path between a sensor and the server. In the case of the redispatch service, a higher uncertain DER threshold has a similar impact, but considering the failure of DER controllers instead of sensors. In both cases, the corresponding grid service transitions to and stays in the L state instead of failing (cf. Secs. 3.4.1 and 3.4.3). It can also be observed that the hardware-based factors improve robustness, while the software (or algorithmic) factors improve absorption and stabilisation.

The design $D1$ has a marginally lower failure metric (R^F) for both grid services than $D2$, indicating that $D1$ enters the F state less often. This can be attributed to server redundancy, which is a critical component for both grid services as they transition to the F state in the case of server failure. The extended recovery metric ($\hat{R}^R$) of both

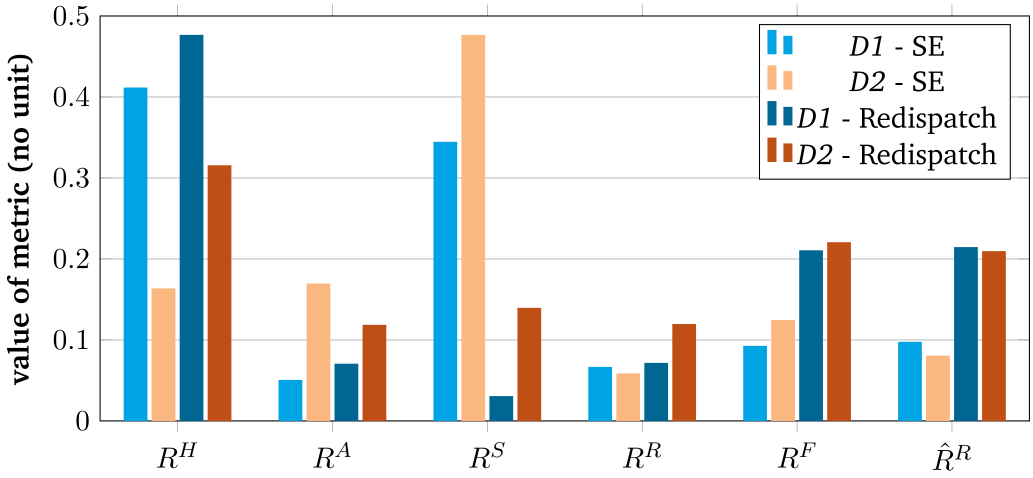


Fig. 7.4: Metrics showing phases of the resilience of SE and redispatch services for both ICT system designs.

designs is greater than the respective recovery metrics (R^R) as the former includes the latter (cf. Eq. (6.11)). The results also show that while the grid services in $D2$ have more transitions between N and L states (degradation NL and recovery LN), the grid services in $D1$ have more transitions within the N state (NN). These results show that the proposed methodology and metrics can quantify the impact of ICT design factors on individual phases of the resilience of ICT-enabled grid services, including the transitions related to F state. Using these results, relevant factors that improve the favourable phases of resilience while lowering unfavourable ones (i.e., R^F) could be analysed and implemented.

Tab. 7.2 presents the probabilities of resilient behaviour R (Eq. (6.8)) and the corresponding performance R^{MOP} (Eq. (6.12)) of SE and redispatch services for both ICT system designs. Here, R^{MOP} was calculated considering weights of $w^N = 1$, $w^L = 0.5$ and $w^F = 1$. The values of R and R^{MOP} aggregate the phases from Fig. 7.4. It can be seen that both designs have similar values of R for both grid services. This indicates that the decrease of R^H in design $D2$ is nearly compensated by the increase in R^A and R^S. However, there is a larger difference in R^{MOP}, which can be attributed to the lower weightage of L state (compared to N) and the penalisation of F state. Although a comparison between the grid services is futile, the resilience and the performance metrics of redispatch are lower than that of SE because the redispatch service depends on SE but not vice-versa (cf. Fig. 7.2). This means that the metrics of the redispatch service are also affected by the failure of the SE service.

The results also show that design $D1$, due to higher R and R^{MOP}, is better for the SE service, whereas design $D2$ is better for the redispatch service. This indicates that an ICT system design suitable for one grid service need not necessarily be ideal for another, i.e., there is no one-size-fits-all design for ICT systems, and the resilience (and performance) of all grid services should be considered while designing ICT systems. In such cases, the criticality of the grid services, if known, can be used to decide between ICT system designs. Since SE impacts all control room-based grid services, it is more critical than redispatch; hence, design $D1$ is preferred. Additionally, these metrics are also lower than the maximum possible value of 1 (cf. Sec. 6.3), indicating a possibility for improvement (redispatch more than SE) in the designs and the implementations of the grid services. While the aim here is to assess and compare the resilience of grid services, designing the most resilient grid service is part of the future work.

Tab. 7.2: Resilience and performance of SE and redispatch services for designs $D1$ and $D2$.

Grid Service	**ICT System Design**	**R (no unit)** Eq. (6.8)	**R^{MOP} (no unit)** Eq. (6.12)
SE	*D1*	0.871	0.605
	D2	0.866	0.436
Redispatch	*D1*	0.637	0.382
	D2	0.691	0.410

Furthermore, cost is an essential factor against which resilience has to be weighed while designing ICT systems [17]. Factors such as observability, number of DERs, redundancy and meshing in the presented designs will require more hardware. Although design $D1$ is more resilient than $D2$ for the SE service, $D1$ will be more expensive due to increased hardware components. Software-based factors such as pseudo-measurement threshold and uncertain DERs threshold tend to be cheaper than hardware as they can be achieved by modifications in the algorithm of the grid services [101].

Although improving resilience often increases the design cost, a system with lower resilience has a higher risk of failure caused by disturbances. This higher risk can lead to higher operational costs due to potential damages and compensation, which is challenging to measure due to the large number of actors involved and the complex nature of the system [85]. Thus, the proposed methodology and metrics can serve as one of the aspects of system design. As already shown in the results of RQ1 (cf. Chapter 5), this is relevant because improving the resilience of grid services can improve the resilience of the interconnected PS.

7.3 Evaluation

This section evaluates the proposed methodology and metrics based on the objectives of RQ2, which are presented in Sec. 1.5. This includes the functional requirements FR4 and FR5, as well as the non-functional requirements NFR3 and NFR4.

7.3.1 Functional Requirements

The results in Sec. 7.2, particularly the R^{MOP} metric, show that the developed methodology and metrics can quantify the performance of the ICT-enabled grid services. This is done using the (weighted) discrete operational states and transitions while also considering the dependencies between the grid services. Therefore, it can be concluded that the developed methodology and metrics satisfy FR4 (quantifying the performance of grid services). Although these operational states capture the performance of a grid service, they are discrete and, therefore, aggregate a wide range of situations. For example, as discussed in Sec. 5.4.3, the Limited state encompasses all situations between fully functional (Normal) to complete failure (Failed). Different weights could then be assigned to a Limited state close to the border to Normal versus a Limited state close to the border to Failed. This can also indicate the ease of recovery of the grid service from an operational point of view. Including finger granular states into the R^{MOP} metrics can enable it to measure the depth of degradation and is a promising part of future research.

The results in Sec. 7.2 also show that developed methodology can measure the resilience (Eq. (6.8)) and its constituting phases (Eqs. (6.4) - (6.7)) of a grid service considering different design factors. This can be used to identify weaker phases and implement specific measures to boost them. For example, the redispatch service in design $D1$ has a low stabilisation metric (cf. Fig. 7.4) and can benefit from an increased uncertain DERs threshold. Although not a part of traditional resilience, the failure and extended recovery metrics (Eqs. (6.10) - (6.11)) capture the transitions to and from the Failed state, which can be used to assess the impact of critical component failures, e.g., server and critical sensors. Based on this, it can be concluded that the developed methodology and metrics satisfy FR5 (measure the phases of resilience for different ICT designs). A limitation of this resilience assessment is the lack of temporal aspects, which is due to the limitation of the operational state model from RQ1 (cf. Sec. 5.4.2). Consequentially, the metrics capture only the state transitions but not the speed of transitions. The integration of temporal aspects into the operational state model and the proposed resilience metrics is also part of future work.

7.3.2 Non-functional Requirement – Scalability

Scalability (NFR4) evaluates the ability of the proposed methodology to consider ICT systems of various sizes. The proposed method in Sec. 6.2.1 uses SMC simulation to generate the operating (UP–DOWN) sequences of each ICT component, which are randomly sampled based on their respective behaviour model. This is required to determine the state trajectories of the grid services. Fig. 6.5 shows that the number of operating sequences increases with the number of components in the ICT system. Consequently, at each time step k, the automata has to process more combinations of component states. This increases the randomness in the SMC simulations, which can affect its convergence. This section aims to determine the impact of the number of components (size) in the ICT system on the convergence of the proposed methodology. To do so, three ICT networks of varying sizes (i.e., the number of nodes) are considered: (i) ICT system for IEEE 4 bus grid [2], (ii) ICT system for CIGRE 14 bus MV grid from Sec. 7.1.3, and (iii) ICT system for IEEE 30 bus grid [3]. These ICT systems have 24, 79 and 151 components, respectively, and are all designed based on the considerations in Sec. 5.1. While ICT systems i and iii are shown in Fig. 7.5, ICT system ii is shown in Fig. 7.3 (design $D2$ but with full observability).

As discussed in Sec. 6.2.1, the SMC inputs can model single as well as simultaneous failures of ICT components via their operating sequences. Fig. 7.6 shows the distribution of simultaneous component failures for the three ICT systems. For instance, 1 indicates a single component failure and 5 indicates that 5 components fail simultaneously. It can be seen that the number of simultaneous component failures increases with the size of the ICT system with 2, 5 and 7 as the modes (most occurrences) of ICT systems i, ii and iii, respectively. The three systems have a maximum of 7 (2 occurrences), 12 (1 occurrence) and 16 (3 occurrences) simultaneous component failures. These are, however, not visible in the figure due to the scale of the y-axis. This shows that the more ICT components, the more component failure combinations are considered inputs to the SMC simulation. This also gives insights into how the SMC method samples the underlying distribution, which consists of the ICT component behaviour models.

[2] Case 4gs grid: https://pandapower.readthedocs.io/en/v2.13.1/networks/power_system_test_cases.html (Accessed: Feb 12, 2032)

[3] IEEE 30 bus grid: https://icseg.iti.illinois.edu/ieee-30-bus-system# (Accessed: Feb 12, 2032)

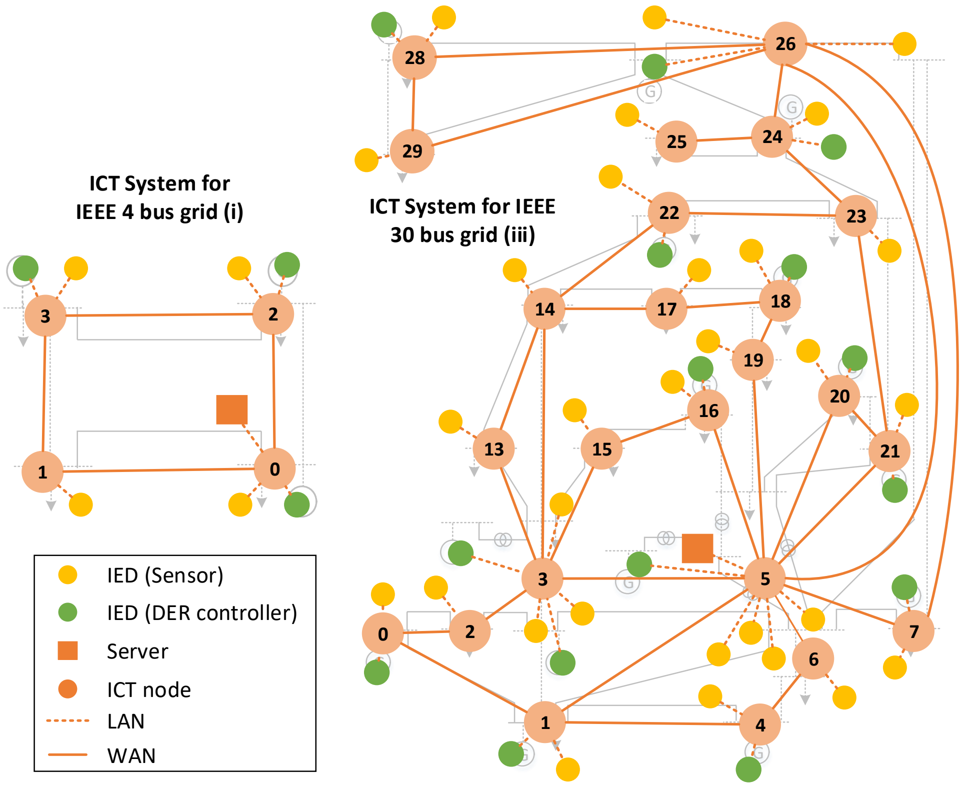


Fig. 7.5: ICT systems for (i) IEEE 4 bus grid and (iii) IEEE 30 bus grid.

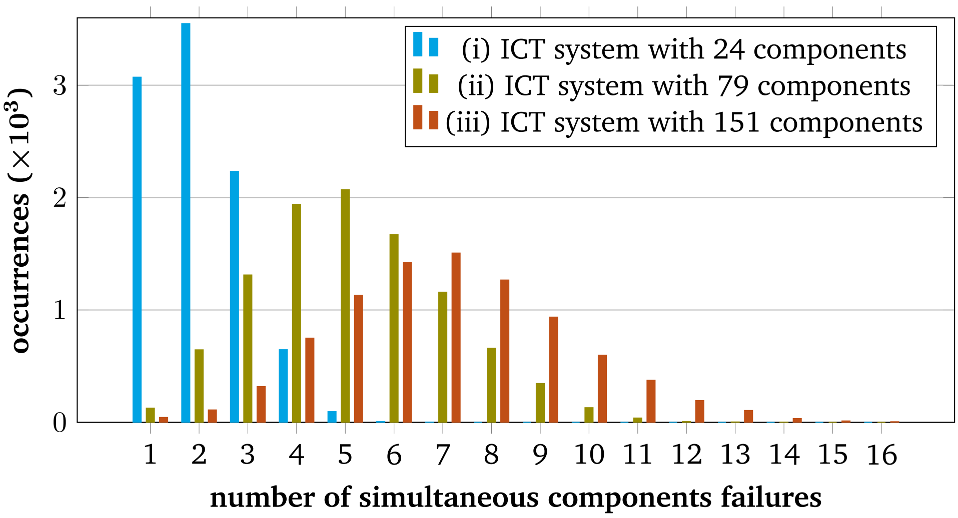


Fig. 7.6: Number of simultaneous component failures from the SMC simulation.

Tab. 7.3 shows the convergence of the proposed methodology for the three ICT systems. The simulations were done on a laptop with an 11th Gen Intel i5-1135G7 processor running at 2.40 GHz using 16 GB of RAM with the Windows 10 operating system. It can be seen that, although the larger ICT systems have more randomness (discussed above), the SMC simulation converges in a similar number of steps. This implies that the number of steps for SMC convergence is independent of the size of the ICT system. The table also shows the execution times for each part of the proposed methodology in Fig. 6.3. Contrary to the number of steps, the total simulation time increases linearly with the ICT system size. This is because more ICT components increase the number of operating cycling (the input) as well as the graph-based calculations in the automata to assess the states of grid services (cf. Sec. 4.2). This is evident from the increase in the time to generate inputs and calculate the state trajectories, with the latter contributing to nearly 99% of the total simulation time. The time taken to quantify resilience is negligible since it involves only simple arithmetic operations (cf. Sec. 6.2.4).

Tab. 7.3: Convergence of proposed methodology for ICT systems of different sizes.

		ICT for IEEE 4 bus (i)	ICT for CIGRE 15 bus (ii)	ICT for IEEE 30 bus (iii)
Number of ICT components		24	79	151
Steps for SMC convergence		10500	11108	10800
Time (s)	Generate inputs	9.25	25.7	74.37
	Calc. trajectories	1237.73	3544.18	4363.22
	Quantify resilience	0.039	0.049	0.045
	Total sim. time	1247.02	3569.93	4437.64

Model Observation: The reason why the number of steps for SMC convergence is independent of ICT network size can be explained by simulating and observing a simple yet representative model. Let $A = \{a_1, a_2, ..., a_m\}$ and $B = \{b_1, b_2, ..., b_n\}$ be two sets of sizes m and n, respectively, with $m \gg n$. A function f is defined to randomly map each element in A to an element in B, i.e. $\forall a \in A, f(a) = b \in B$. Fig. 7.7 depicts the two sets and the mapping function f (black arrows). This function essentially represents the Monte-Carlo selection and is then simulated until the same convergence condition in Eq. (6.3) is satisfied. The transition probabilities are calculated between the elements of set B. The simulation is then repeated for different values of m and n. The results in Tab. 7.4 show that the number of steps for convergence depends on the size of the target set B, i.e., n, and is independent of the size of the source set A, i.e., m. This is because the mapping function f flattens the complexity of set A based on the size of B. For example, if $n = m/2$, then the complexity of A is decreased by half as, on average, two elements in A would be mapped to an element in B. If $n = 1$, then the complexity of A is completely flatted to 1 as all its elements will be mapped to the same element in B.

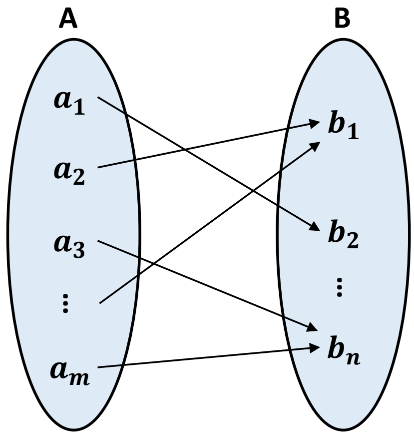


Fig. 7.7: Exemplary mapping between sets A and B with m and n elements.

Tab. 7.4: Variation of SMC convergence for different m and n.

Size of A (m)	Size of B (n)		
	$n = 3$	$n = 4$	$n = 5$
$m = 10^8$	3400	5500	7710
$m = 10^{10}$	3120	5900	7740
$m = 10^{12}$	3160	5840	8220

For the proposed methodology, the number of combinations of ICT component states at each time step is analogous to the size of A, and the number of operational states of a grid service is analogous to the size of B with $n = 3$, i.e., the finite state automaton maps the combination of operating sequences onto one of three states (cf. Fig. 6.5). Although the number of possible combinations of component states increases with the size of the ICT network, its complexity is flattered as they are mapped onto one of the three operational states. This flatting is, however, acceptable since the states of the grid services capture the aspects relevant to system operation (cf. Chapter 3). Furthermore, the results in Tab. 7.3 show that some complexity manifests as the linear increase in the simulation time. Although these simulation times can potentially be improved by optimising the code, their relative differences would still hold. A drawback of this flattering is the loss of traceability, i.e., a state transition cannot be traced to the causing events. In this regard, the properties of the grid services, namely, availability, timeliness and correctness, could give some insights into the causing events (cf. Fig. 3.2). Detailed analysis of traceability based on these properties is considered to be future work.

7.3.3 Non-functional Requirement – Comparability

Comparability (NFR4) evaluates the ability of the proposed methodology and metrics to enable a comparison between different ICT system designs. Due to the rapid digitalisation and advancements in ICT technologies, several options exist to design

ICT-enabled grid services. Some of them are discussed in Chapter 2 and in Sec. 7.1.3. Fig. 7.8 shows the experiments performed to evaluate comparability. They aim to evaluate the ability of the proposed methodology to analyse and compare the influence of an individual as well as a combination of ICT design factors in terms of the resilience of the grid services. The former serves as a sensitivity analysis of a grid service to individual design factors, whereas the latter can be used to compare overall ICT system designs. While the influence of a combination of design factors is already discussed in Sec. 7.2, the influence of individual design factors, particularly, pseudo-measurement threshold ($\Phi^{PM,th}$) and server redundancy on the SE service are analysed in this section.

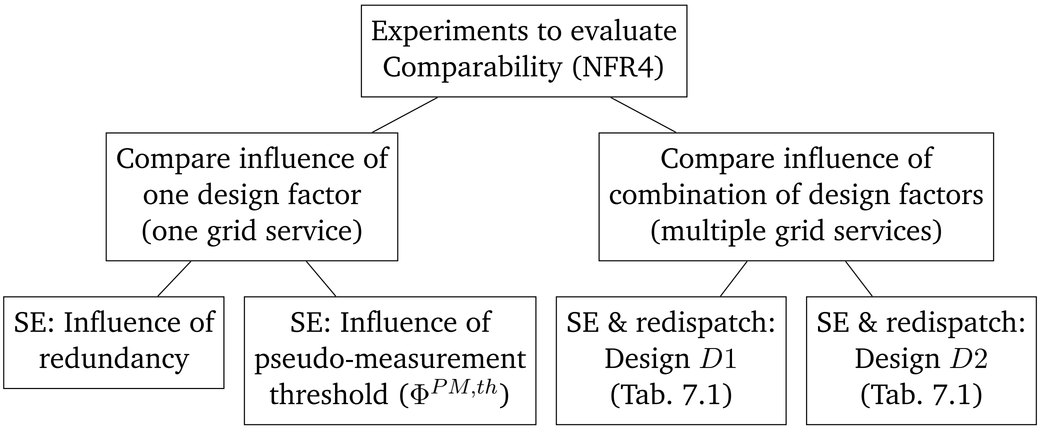


Fig. 7.8: Experiements to evaluate comparability (NFR4).

Fig. 7.10 shows the influence of server redundancy on the individual phases and the aggregated resilience of SE service. These results were obtained with ICT design $D1$ from Fig. 7.3 considering $\Phi^{PM,th} = 3$ and the redundancy archetypes shown in Fig. 7.9. Here, *partial* refers to only redundant servers, whereas *full* refers to redundant servers, ICT nodes and LAN links. It can be seen that the metric R^H increases with redundancy while the metric R^F decreases. The reason is that, with more redundancy, the SE service has more robustness and, therefore, has more occurrences of N state because of NN transitions. This can also be seen in Fig. 7.11, where the occurrence of N and F states increase and decrease, respectively, with increasing redundancy. This correspondingly increases the R and R^{MOP} metrics. Since the server is a critical component for the SE service, *full* redundancy results in a high resilience value with $R = 0.91$. Furthermore, the metrics R^A and R^S, and the occurrence of L state are nearly constant as redundancy does not impact absorption, stabilisation and consequentially, the transitions to L state. As expected, the SE service has a nearly constant stabilisation index (R^S) of around 0.42 across the archetypes, which is similar to the corresponding value in Fig. 7.12 with $\Phi^{PM,th} = 3$.

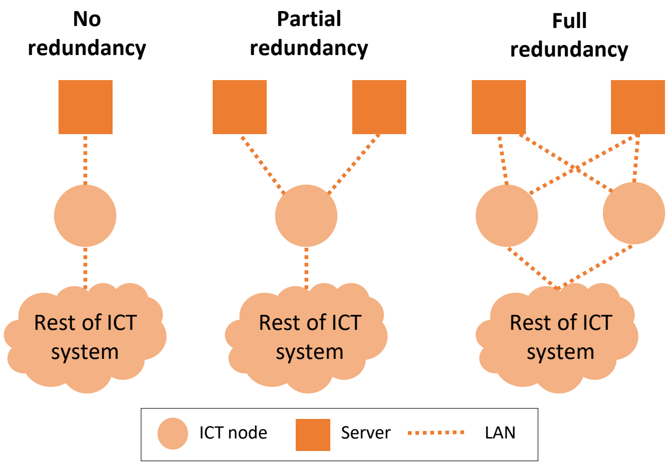


Fig. 7.9: Variations of server redundancy to evaluate comparability.

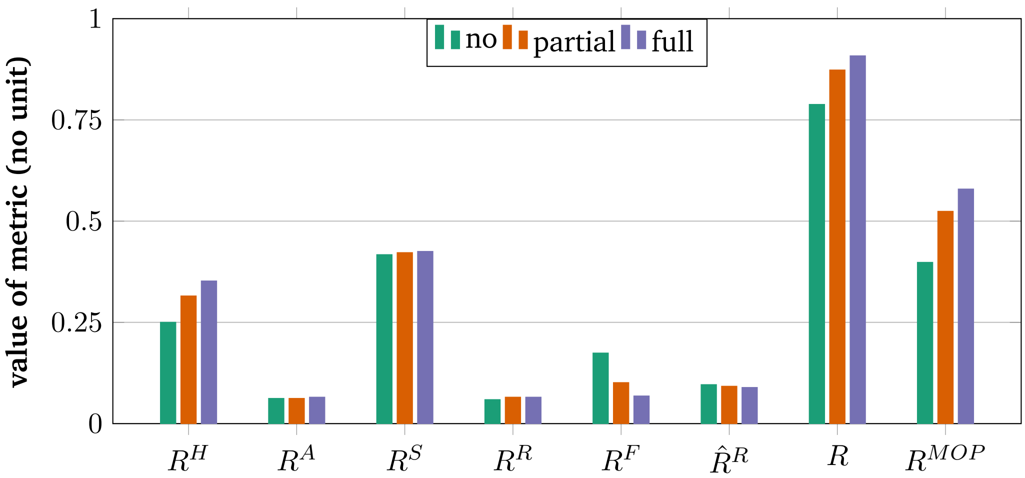


Fig. 7.10: State estimation: Influence of redundancy on resilience metrics.

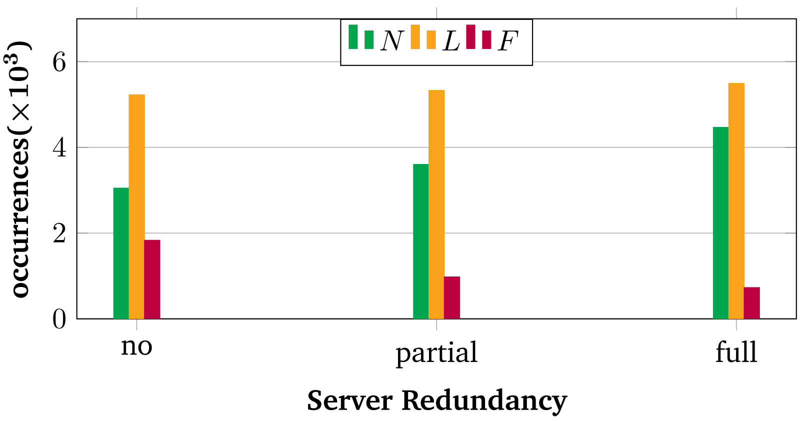


Fig. 7.11: State estimation: Occurrences of states for the three redundancy archetypes.

Fig. 7.12 shows the influence of pseudo-measurement threshold $\Phi^{PM,th}$ on the individual phases and the aggregated resilience of SE service. These results were obtained considering the ICT design $D1$ in Fig. 7.3 but without redundancy (i.e., *no redundancy* from Fig. 7.9). Note that $\Phi^{PM,th} = 6$ correspond to using around 50% pseudo-measurements. When $\Phi^{PM,th} = 0$, the service cannot use pseudo-measurements at all and, therefore, has neither absorption nor stabilisation, i.e. $R^A = R^S = 0$. This results in zero probability of resilient behaviour with $R = 0$ and a negative performance with $R^{MOP} = -0.38$. The reason can be seen in Fig. 7.13, which shows the number of occurrences of the three operational states. When $\Phi^{PM,th} = 0$, the F state occurs nearly twice as much as the N state with no occurrence of the L state. While the metric R^S increases with the pseudo-measurement threshold, the metric R^F decreases. This is because the SE service, with more pseudo-measurements, has more stabilisation in the L state and, therefore, fewer transitions to the F state. This can also be observed in Fig. 7.13, where the occurrence of L state increases with the pseudo-measurement threshold, while the occurrence of F state decreases. As a result, the R and R^{MOP} metrics also increase correspondingly. The metric R^H and the occurrences of the N state are nearly constant, indicating that pseudo-measurements do not impact robustness as well as the transitions to the N state.

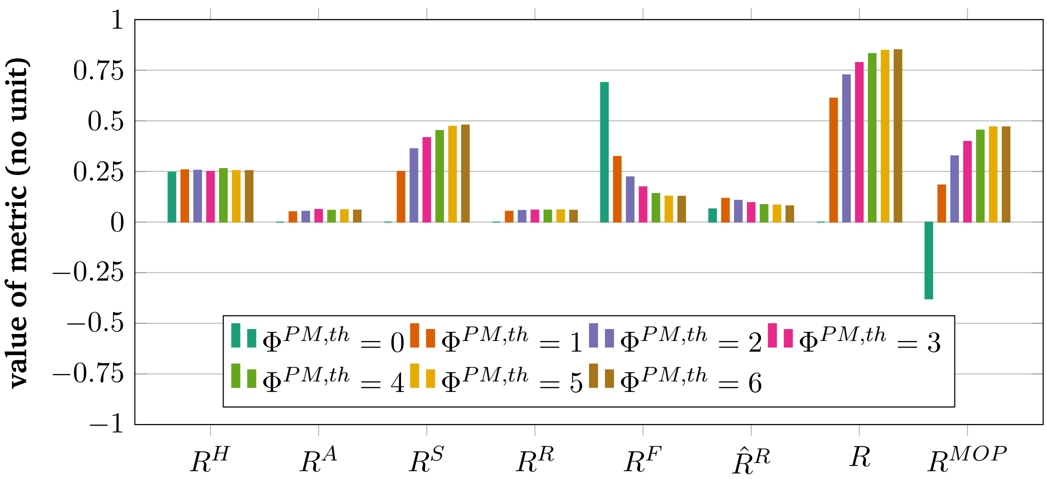


Fig. 7.12: State estimation: Influence of pseudo-measurement threshold ($\Phi^{PM,th}$) on resilience metrics.

The benefits of increasing the pseudo-measurement threshold, in terms of R^S, R and R^{MOP}, are, however, only marginal beyond $\Phi^{PM,th} = 4$. The reason is evident from Tab. 7.5, which shows the normalised percentages of the number of pseudo-measurements used in the simulations for each pseudo-measurement threshold. For example, when $\Phi^{PM,th} = 2$ (maximum of 2 pseudo-measurements can be

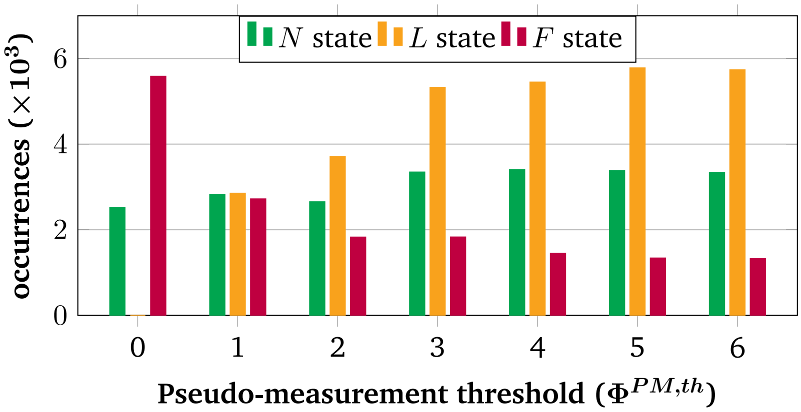


Fig. 7.13: State estimation: Occurrences of states for pseudo-measurement threshold variation.

used), 39.8% and 23.5% of runs used 1 and 2 pseudo-measurements respectively, whereas 36.8% of the runs did not use any pseudo-measurements (because the solvability condition could be satisfied with only field measurements). Note that the runs which resulted in the F state are not counted. It can be seen that only a small percentage of SMC steps (5%) require the use of four or more pseudo-measurements. This behaviour could be attributed to the selected failure and repair rates in Sec. 7.1.3, in a way that disturbances, which cause loss of field measurements such that four or more pseudo-measurements are required, are rare. This shows that more pseudo-measurements are not necessarily better as the benefits of using more pseudo-measurements saturate while at the same time introducing more uncertainty in the SE results (cf. Sec. 3.4.1). This also shows the need to consider the resilience of individual grid services while designing ICT systems. Note that these results are specific to this ICT system and grid service architecture, and using different ones could yield different results.

Tab. 7.5: State estimation: Number of pseudo-measurements used for each pseudo-measurement threshold. The entries are percentages based on the total number of steps for each threshold.

No. of pseudo-measurements used	Pseudo-measurement threshold ($\Phi^{PM,th}$)					
	1	2	3	4	5	6
0	37.1%	36.8%	36.7%	37.2%	37.4%	36.6%
1	62.9%	39.8%	40.4%	39.5%	39.7%	40.4%
2	-	23.5%	11.4%	11.5%	11.8%	11.7%
3	-	-	11.5%	6.6%	5.7%	5.9%
4	-	-	-	5.2%	3.2%	3.2 %
5	-	-	-	-	2.2%	1.3%
6	-	-	-	-	-	0.9%

The comparison of ICT system designs $D1$ and $D2$ considering SE and redispatch services showed that different designs could suit different grid services. The results also compared several design factors, including both general and service-specific ones. The proposed metrics are shown to be capable of assessing the influence of these design factors on the specific phases of resilience. Based on the analysis of the pseudo-measurement threshold, redundancy and the comparison between designs $D1$ and $D2$, it can be concluded that the proposed methodology and metrics can compare different ICT design factors based on the resilience of the ICT-enabled grid services. It can also be used to analyse the sensitivity of the phases of resilience to different (individual as well as combination) design factors.

7.4 Chapter Summary

This chapter presents the results, discussion and evaluation of the proposed methodology and metrics from Chapter 6 (artefact of RQ2). The highlights are as follows:

- A simulation scenario consisting of two ICT system designs for the CIGRE 14 bus benchmark grid with state estimation and DER redispatch services has been described. The grid services have been modelled from an ICT system viewpoint while abstracting the power system aspects. The ICT system designs have been chosen to include both hardware- and software-based design factors.
- The simulation results demonstrate that the proposed methodology can assess and compare the resilience of grid services between the system designs. The metrics quantify the individual phases as well as the aggregated resilience. The results show that there is not necessarily a one-size-fits-all design for ICT systems, and the resilience of each grid service should be considered while designing ICT systems.
- The methodology has been shown to be scalable with respect to the size of the ICT network. Specifically, the convergence of the sequential Monte Carlo simulation has been found to be independent of the number of components in the ICT system (larger networks have more components, resulting in a larger sample space). The reason is that the states of components have been mapped onto one of the three operational states, which restricted the overall complexity.
- The methodology has been shown to compare the influence of individual as well as a combination of design factors on the resilience of ICT-enabled grid

services. Subsequently, the metrics have been shown to capture the impact of various design factors on the individual phases of resilience, which can then be used for designing ICT systems.

- The functional (FR4, FR5) and non-functional (NFR3, NFR4) requirements for the resilience assessment methodology have been shown to be fulfilled, indicating the successful answering of RQ2. The NFRs have been evaluated quantitatively using simulations with different sizes of ICT networks and design factors.

8 Conclusion and Outlook

This chapter presents the conclusions and outlook of this dissertation. First, a summary of the scientific contributions and their applications are presented in Sec. 8.1. This is followed by the limitations of this dissertation and potential future research in Sec. 8.2.

8.1 Summary

ICT systems are an essential part of modern CPESs as they bring in the automation required for the grid services, which aid in the operation of the interconnected power system. Although these grid services have been a part of traditional power systems, the introduction of ICT systems has enhanced their capabilities in monitoring, communication and control. There exists a strong interdependence between the power and ICT systems, which increases their complexity, leading to new disturbances that can potentially harm the overall CPES. These disturbances can originate from both power and ICT systems and can propagate across the system's boundary to impact the connected system. As a safety-critical infrastructure, CPESs should be designed to survive such disturbances and reliably supply electricity to their customers. Due to the rapid advancements in ICT technologies and the novelty of CPESs, system operators also have fewer experiences in dealing with such disturbances. Therefore, these complex modes of disturbance propagation challenge the traditional paradigm, where power systems are designed to withstand only a pre-defined set of severe disturbances. Resilient systems are required, which, in addition to known disturbances, can also handle new and unforeseen ones. In this regard, this dissertation has two research questions, which result in the two developed artefacts, i.e., the scientific contributions. While RQ1 focus on the joint operational state of CPESs, considering the interdependencies between power and ICT systems, RQ2 focus on quantifying the resilience of the ICT system in CPESs with a focus on the grid services.

8.1.1 Artefact – Joint Operational State Model

The first artefact is a model to investigate the propagation of disturbances via the interdependencies between power and ICT systems. Property graphs have been used to model both systems as they enable the mapping of different power and ICT disturbances by suitably modifying the properties of the graph. Operational states, which capture the performance of the respective system, have been used to determine the impact of these disturbances. While the power system operational states are well-established in the literature, there is a lack of operational states for ICT systems. Therefore, a novel operational state model for the ICT system has been developed in this dissertation. The focus has primarily been on the performance of ICT-enabled grid services, which constitute the dependence of the power system on the ICT system and, therefore, can map the impact of ICT disturbances on the operation of power systems. Three properties of the ICT system, namely, availability of components, timeliness of data transfer and correctness of data, have been identified in order to define the operational states of the grid services. These properties and the states have been subsequently formalised using finite state automata due to their capability to model discrete states and their transitions. The combination of the operational state models of ICT-enabled grid services and the power system yielded the joint operational state model for CPES, which is the artefact corresponding to RQ1 of this dissertation.

The developed model can take sequences of multi-domain disturbances as input and analyse their propagation as a sequence of operational states, which is the output. The property graph model of CPESs has been shown to incorporate different power and ICT disturbances (NFR1). Next, the resulting sequence of operational states has been shown to have both degradation and recovery transitions (FR2). Using different simulation scenarios, the model has subsequently been demonstrated to capture the two types of disturbance propagation: cascading and escalating (FR3). It can, therefore, be used to trace and study the complex modes of disturbance propagation in a CPES. Furthermore, the developed model could capture structural and functional dependencies between the power and ICT systems (FR1). Structural dependence has been represented by the provision of electricity to ICT components, while functional dependence has been by the operational states of grid services. In contrast to the current literature, these operational states can model the performance of individual grid services and their dependence on the other grid services. The states are shown to be general in the sense that they can be used to model different grid services as well as enable the extension of the developed model to include additional grid services (NFR2). The developed model can be used to analyse the impact of different grid services and their architectures on the interconnected power system, given different power and ICT disturbances. This can be used to gain novel insights into the interdependencies between power and ICT systems, which can be used for designing modern CPESs. Since the artefact has been shown to satisfy all the specified requirements (cf. Sec. 5.4), it can be concluded that the RQ1 of this dissertation has been successfully answered.

8.1.2 Artefact – Resilience Assessment Methodology

The second artefact is a novel methodology to quantify the resilience of ICT-enabled grid services in CPESs. In contrast to the current literature on ICT resilience, which is limited only to its infrastructural aspects and data transfer, this dissertation considers the performance of the grid services, which is quantified using the aforementioned operational states. This is relevant as these grid services directly impact the short-term resilience of the interconnected power system by either mitigating the impact of a disturbance or recovering the power system after a disturbance. The resilience of grid services is measured considering a wide range of events (e.g., disturbances and repair actions) that the ICT system may encounter during its lifetime, which is simulated using the sequential Monte Carlo method combined with component behaviour models. This provides a systematic approach to simulate the realistic behaviour of an ICT system as a sequence of events that build upon each other as the system progresses through time. These events are fed to the finite state automata of the grid services, which then assesses their corresponding operational states. Based on the resulting state transitions, two metrics (R and R^{MOP}) are developed to quantify the resilience of the respective grid services. This methodology and metrics to quantify and assess the resilience of ICT-enabled grid services are the artefacts corresponding to RQ2 of this dissertation. The first metric R has been shown to, for the first time in literature, quantify not only the probability of resilient behaviour of a grid service but also its constituting phases, namely, robustness, absorption, stabilisation and recovery (FR5). The second metric R^{MOP} has been shown to measure the performance of the grid service from a resilience perspective (FR4). These metrics are modular, i.e., the phases of resilience could be quantified individually, and their contribution (or weight) to the aggregated metrics could be adjusted. Using three ICT systems of different sizes, the proposed methodology has been shown to be scalable with respect to the number of ICT components (NFR3). Specifically, the convergence of the Monte Carlo Simulation was found to be independent of the number of components in the system. The methodology has also been shown to enable a comparison of different ICT system design factors in terms of the resilience of the grid services. In this regard, the sensitivity of grid services to individual as well as combination of design factors, could be calculated and compared based on both R and R^{MOP} (NFR4). The results show that an ICT design suitable for one grid service need not necessarily be suitable for another and that the resilience of all grid services should be considered while designing ICT systems. Therefore, the proposed methodology and metrics can be used to design resilient ICT systems in CPES. This is essential because enhancing the resilience of the ICT system and its grid services will enhance the resilience of the interdependent power system and, consequentially, the whole CPES. Since this artefact has been shown to satisfy all the specified requirements (cf. Sec. 7.3), it can be concluded that the RQ2 of this dissertation has also been successfully answered.

8.2 Limitations and Future Work

Although some of the limitations of the developed artefacts have already been discussed in the respective evaluations, i.e., Secs. 5.4 and 7.3, this section summarises the limitations along with suggestions to address them.

The operational states are the foundation for both the developed artefacts. Each state, by definition, is intended to provide situational awareness to the operator about the essential aspects required to operate the underlying system. In this regard, a balance is needed between simplicity (i.e., the states should be easy to understand and use) and capturing complexity (i.e., the states should represent the phenomena under interest). While the power system states are well established in the literature, the three operational states of grid services defined based on the three ICT properties are a novel contribution of this dissertation. They are, however, only evaluated considering grid services with centralised architectures. Evaluating their applicability to grid services with distributed architectures and on different hierarchies (e.g., field, substation and control room) is a crucial next step, especially considering the rising prominence of multi-agent systems and distributed grid operation [60]. This not only requires further properties to describe the performance of a grid service but also finer granular operational states to adequately capture their performance. In this regard, the first ideas for applying the developed operational states for a distributed grid service, such as state estimation, have been discussed in[121], with additional properties such as rate of convergence, unobservability risk and quality in bad data detectors. Since distributed architectures typically have multiple levels of degradation, finer granular operational states can assess not only the state but also how deep the grid service is in that state, e.g., a grid service in Limited but near the border to Normal is better than Limited but near the border to Failed. This may then influence the recovery actions mandated by the operator to improve the operational state. The developed operational state model is based on the three ICT properties: availability, timeliness and correctness. However, only availability is investigated in the presented simulation results. As discussed in Sec. 5.4.2, the model does not consider temporal aspects, which limits its application to analyse dynamics of power and ICT systems. For power systems, the time spent in insecure states has dangers such as component damage due to overloads in the Emergency state and financial loss in the Blackout state. Power system dynamics can be modelled by including the differential-algebraic equations corresponding to the dynamic phenomena of interest, e.g., frequency and voltage stability [43]. The finite state automaton model should then be extended to a hybrid automaton, capable of representing the time spent by the system in each operational state. For instance, temporal aspects of the ICT system can be considered by incorporating queuing models (e.g., M/M/1 model [122]) into the property graph model. This would allow the model to consider dynamic data flows and analyse phenomena such as congestion and package loss, which are essential phenomena in ICT systems.

There exists a fundamental difference between availability and timeliness on one hand and correctness on the other. While the former can be measured, for instance, by pinging (or using a component's heartbeats) and comparing timestamps, respectively [42], data correctness cannot be directly measured due to the absence of ground truth (i.e., actual value). This implies that data correctness can only be estimated and is relevant considering the rise of cyber threats in CPESs. Since CPESs span large geographical areas, data transfer from source to destination typically passes through several intermediate nodes, all of which can be potential entry points for attackers. In this regard, trust in power system network assessment (PSNA-trust) is a promising approach for estimating data correctness using the trustworthiness of the involved ICT components. The authors in [55, 99] present the PSNA-Trust approach, where trust is computed based on static information about involved components and live health monitoring systems. The integration of PSNA-Trust into the operational states will enable the estimation of data correctness, particularly in the case of cyber threats, which are not considered in this dissertation. First ideas on this topic have already been outlined in [41].

A prevalent aspect of resilience in the literature is the behaviour of a system under the so-called unknown events, which refers to new, unplanned or low-probable events. In addition to bouncing back without collapsing, a resilient system should be capable of learning and improving after facing such disturbances. The sequential Monte Carlo method in this dissertation generates events based on a given probabilistic distribution, which are then used to calculate the proposed resilience metrics. This has two limitations from the perspective of resilience. First, events with a low probability of occurrence are hardly chosen, implying that the resulting metrics do not capture the impact of low-probable events on the system. Second, there is a lack of probabilistic distributions to represent the behaviour of ICT components in CPESs (especially regarding timeliness and correctness) due to their continuously evolving nature. In this regard, other methods to generate events, such as using artificial intelligence [123], risk-based approaches [124, 125], optimisation-based approaches [27] and even based on expert knowledge [21], which do not rely on probabilities could be explored as a part of future work. Using such methods could enable the generation of events required to evaluate the proposed resilience metrics considering the timeliness and correctness properties of the ICT system.

The developed resilience assessment methodology and metrics are currently applied only to the ICT system and the grid services with the consideration that improving the resilience of the grid services will benefit the operation of the interconnected power system. A natural future step is to extend the developed methodology to assess the resilience of power systems. Like the grid services, the operational states of a power system can be used to quantify its performance. In this regard, metrics such as loads at risk, operational limit violations and loads lost can be calculated for each operational state. Extending the developed methodology to consider the resilience of power systems will enable its usage for the holistic design of resilient CPESs.

Acronyms

BAN	Building area network
BDEW	German association of energy and water industries
CL	Contingency list
CPES	Cyber-physical energy system
DER	Distributed energy resource
ENTSO-E	European network of transmission system operators for electricity
ESYS	German energy systems of the future
FAN	Field area network
FSA	Finite state automaton
ICT	Information and communication technology
IED	Intelligent electronic device
IT	Information technology
MOP	Measure of performance
MV	Medium voltage
OLTC	On-load tap changer
OT	Operational technology
PLC	Power line carrier communication
PM	Pseudo-measurement
PMU	Phasor measurement unit
PS	Power system
PSNA	Power system network assessment
RA	Remedial action

RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SE	State estimation
SMC	Sequential monte carlo
SPS	Special protection scheme
TTF	Time to fail
TTR	Time to repair
VC	Voltage control
WAN	Wide area network
WLS	Weighted least square

List of Figures

List of Tables

Own Publications

[8] **Anand Narayan**, Batoul Hage Hassan, Shadi Attarha, et al. "Grid function virtualization for reliable provision of services in cyber-physical energy systems". In: *2020 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE. 2020, pp. 1–5 (cit. on pp. 2, 12, 16, 18, 43).

[9] **Anand Narayan**. "Interdependent ICT and Power System State Classification for ICT-reliant Energy Systems". In: *Abstracts from the 8th DACH+ Conference on Energy Informatics*. DACH+ Conference on Energy Informatics. Springer, Sept. 2019 (cit. on pp. 2, 12).

[11] **Anand Narayan**, Marcel Klaes, Sebastian Lehnhoff, and Christian Rehtanz. "Analyzing the Propagation of Disturbances in CPES considering the States of ICT-enabled Grid Services". In: *2021 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE. 2021, pp. 522–529 (cit. on pp. 2, 12, 22, 43, 52, 81, 82, 117).

[34] Marcel Klaes, **Anand Narayan**, Amit Dilip Patil, et al. "State description of Cyber-Physical Energy Systems". In: *Energy Informatics* 3.1 (2020), pp. 1–19 (cit. on pp. 8, 12, 18, 27, 34, 43, 45).

[36] **Anand Narayan**, Marcel Klaes, Davood Babazadeh, Sebastian Lehnhoff, and Christian Rehtanz. "First approach for a multi-dimensional state classification for ICT-reliant energy systems". In: *International ETG-Congress 2019; ETG Symposium*. VDE. 2019, pp. 1–6 (cit. on pp. 12, 46).

[37] **Anand Narayan**, Carsten Krueger, Andre Goering, et al. "Towards future SCADA systems for ICT-reliant energy systems". In: *International ETG-Congress 2019; ETG Symposium*. VDE. 2019, pp. 1–7 (cit. on pp. 12, 22).

[38] Batoul Hage Hassan, **Anand Narayan**, Davood Babazadeh, Marcel Klaes, and Sebastian Lehnhoff. "Performance assessment of state estimation in cyber-physical energy systems". In: *2021 IEEE Madrid PowerTech*. IEEE. 2021, pp. 1–6 (cit. on pp. 12, 19, 43, 89, 96).

[39] Jonas Haack, **Anand Narayan**, Amit Dilip Patil, et al. "A Hybrid Model for Analysing Disturbance Propagation in Cyber-Physical Energy Systems". In: *Electric Power Systems Research* 212 (2022), p. 108356 (cit. on pp. 12, 57).

[40] **Anand Narayan**, Michael Brand, and Lehnhoff. "Quantifying the Resilience of ICT-enabled Grid Services in Cyber-Physical Energy System". In: *Energy Informatics* 6, Suppl 1.23 (2023) (cit. on pp. 12, 99, 113).

[41] Michael Brand, **Anand Narayan**, and Sebastian Lehnhoff. "Applying Trust for Operational States of ICT-Enabled Power Grid Services". In: *ACM Trans. Auton. Adapt. Syst.* (Apr. 2024). Just Accepted (cit. on pp. 12, 45, 139).

[42] Carsten Krüger, **Anand Narayan**, Felipe Castro, et al. “Real-time test platform for enabling grid service virtualisation in cyber physical energy system”. In: *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. Vol. 1. IEEE. 2020, pp. 109–116 (cit. on pp. 12, 17, 22, 43, 61, 139).

Bibliography

[1] Marilyn A Brown and Shan Zhou. "Sustainable Smart Grids, Emergence of a Policy Framework". In: *Electrical Transmission Systems and Smart Grids: Selected Entries from the Encyclopedia of Sustainability Science and Technology*. Springer, 2012, pp. 271–318 (cit. on p. 1).

[2] International Energy Agency: IEA. "World energy outlook 2022". In: IEA Paris, France. 2022 (cit. on p. 1).

[3] Xinghuo Yu and Yusheng Xue. "Smart grids: A cyber–physical systems perspective". In: *Proceedings of the IEEE* 104.5 (2016), pp. 1058–1070 (cit. on pp. 1, 2, 17).

[4] *EU Directive 2019/944: Common rules for the internal market for electricity, 2019*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0944. Accessed: July 16, 2023 (cit. on p. 1).

[5] Theis B. Rasmussen, Guangya Yang, Arne H. Nielsen, and Zhaoyang Dong. "A review of cyber-physical energy system security assessment". In: *2017 IEEE Manchester PowerTech* (2017), pp. 1–6 (cit. on pp. 1, 4).

[6] *Towards Smarter Grids: ENTSO-E Position Paper on Developing TSO and DSO Roles for the Benefit of Consumers, 2015*. https://www.entsoe.eu/2015/03/04/towards_smarter_grids_entso-e_position_paper_on_developing_tso_and_dso_roles_for_the_benefit_of_consumers/. Accessed: Apr 4, 2023 (cit. on p. 1).

[7] Radhakisan Baheti and Helen Gill. "Cyber-physical systems". In: *The impact of control technology* 12.1 (2011), pp. 161–166 (cit. on p. 2).

[10] Inger Anne Tøndel, Jørn Foros, Stine Skaufel Kilskar, Per Hokstad, and Martin Gilje Jaatun. "Interdependencies and reliability in the combined ICT and power system: An overview of current research". In: *Applied computing and informatics* 14.1 (2018), pp. 17–27 (cit. on pp. 2, 4, 8, 30).

[12] NERC. "Technical Analysis of the August 14, 2003 Blackout: What Happened, Why, and What Did We Learn? Report to the NERC Board of Trustees by the NERC Steering Group". In: *System* (2004), pp. 1–119 (cit. on pp. 3, 5–7).

[13] Thomas Schossig and Walter Schossig. "Disturbances and blackouts—Lessons learned to master the Energy Turnaround". In: *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*. IET. 2014, pp. 1–6 (cit. on p. 3).

[14] David E Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies". In: *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. IEEE. 2017, pp. 1–8 (cit. on p. 3).

[15] Yuan-Kang Wu, Shih Ming Chang, and Yi-Liang Hu. "Literature review of power system blackouts". In: *Energy Procedia* 141 (2017), pp. 428–431 (cit. on p. 4).

[16] Mathaios Panteli, Peter A Crossley, Daniel S Kirschen, and Dejan J Sobajic. "Assessing the impact of insufficient situation awareness on power system operation". In: *IEEE Transactions on power systems* 28.3 (2013), pp. 2967–2977 (cit. on pp. 4, 6, 18, 24, 28, 30).

[17] AM IEEE PES Task Force: Stanković, KL Tomsovic, F De Caro, et al. "Methods for analysis and quantification of power system resilience". In: *IEEE Transactions on Power Systems* (2022) (cit. on pp. 4, 37–39, 122).

[18] Mohamed El-shimy. "Dynamic security of interconnected electric power systems". In: *LAP Lambert Academic Publishing* (2015) (cit. on pp. 4, 26).

[19] Mathaios Panteli and Pierluigi Mancarella. "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events". In: *IEEE Systems Journal* 11.3 (2015), pp. 1733–1742 (cit. on pp. 4, 38–42, 99, 101).

[20] Reza Arghandeh, Alexandra Von Meier, Laura Mehrmanesh, and Lamine Mili. "On the definition of cyber-physical resilience in power systems". In: *Renewable and Sustainable Energy Reviews* 58 (2016), pp. 1060–1069 (cit. on pp. 4, 24, 25, 37, 39).

[21] acatech/Leopoldina/Akademienunion(Eds.) *The resilience of digitalised energy systems. Options for reducing blackout risks (Series on Science-based Policy Advice)*. Apr. 2021 (cit. on pp. 4, 5, 37–39, 140).

[22] Glenn A Fink, Richard L Griswold, and Zachary W Beech. "Quantifying cyber-resilience against resource-exhaustion attacks". In: *2014 7th International Symposium on Resilient Control Systems (ISRCS)*. IEEE. 2014, pp. 1–8 (cit. on p. 5).

[23] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation, Article 18: Classification of System States*. `http://data.europa.eu/eli/reg/2017/1485/oj`. Accessed: Feb 6, 2023 (cit. on pp. 5, 8, 27, 29).

[24] Daniel Kirschen and Francois Bouffard. "Keeping the lights on and the information flowing". In: *IEEE Power and Energy magazine* 7.1 (2009), pp. 50–60 (cit. on pp. 6, 32–34).

[25] Mathaios Panteli and Daniel S Kirschen. "Assessing the effect of failures in the information and communication infrastructure on power system reliability". In: *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE. 2011, pp. 1–7 (cit. on pp. 6, 32–34, 71, 101, 103, 109, 119).

[26] Jean-Claude Laprie, Karama Kanoun, and Mohamed Kaâniche. "Modelling interdependencies between the electricity and information infrastructures". In: *Conference on computer safety, reliability, and security*. Springer. 2007, pp. 54–67 (cit. on pp. 6, 30, 32–34).

[27] Bassam Moussa, Parisa Akaber, Mourad Debbabi, and Chadi Assi. “Critical links identification for selective outages in interdependent power-communication networks”. In: *IEEE Transactions on Industrial Informatics* 14.2 (2017), pp. 472–483 (cit. on pp. 6, 32, 35, 36, 140).

[28] Rezoan A Shuvro, Zhuoyao Wangt, Pankaz Das, Mahshid R Naeini, and Majeed M Hayat. “Modeling cascading-failures in power grids including communication and human operator impacts”. In: *2017 IEEE Green Energy and Smart Systems Conference (IGESSC)*. IEEE. 2017, pp. 1–6 (cit. on pp. 6, 32, 35, 36).

[29] Marzieh Parandehgheibi, Konstantin Turitsyn, and Eytan Modiano. “Modeling the impact of communication loss on the power grid under emergency control”. In: *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. 2015, pp. 356–361 (cit. on pp. 6, 32, 35, 36).

[30] Amit Dilip Patil, Jonas Haack, Martin Braun, and Hermann de Meer. “Modeling interconnected ICT and power systems for resilience analysis”. In: *Energy Informatics* 3.1 (2020), pp. 1–20 (cit. on pp. 6, 32, 36, 39, 40).

[31] Cen Nan and Giovanni Sansavini. “A quantitative method for assessing resilience of interdependent infrastructures”. In: *Reliability Engineering & System Safety* 157 (2017), pp. 35–53 (cit. on pp. 7, 38–40).

[32] Paul Smith, David Hutchison, James PG Sterbenz, et al. “Network resilience: a systematic approach”. In: *IEEE Communications Magazine* 49.7 (2011), pp. 88–97 (cit. on pp. 7, 39, 40).

[33] Xin Liu, Bo Chen, Chen Chen, and Dong Jin. “Electric power grid resilience with interdependencies between power and communication networks–a review”. In: *IET Smart Grid* 3.2 (2020), pp. 182–193 (cit. on pp. 7, 39, 41).

[35] K Pfeffers, Tuure Tuunanen, Charles E Gengler, et al. “The design science research process: A model for producing and presenting information systems research”. In: *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006), Claremont, CA, USA*. 2006, pp. 83–106 (cit. on p. 10).

[43] Prabha Kundur, Neal J Balu, and Mark G Lauby. *Power system stability and control*. Vol. 7. McGraw-hill New York, 1994 (cit. on pp. 14, 17, 26, 51–53, 58, 70, 139).

[44] M.S. Thomas and J.D. McDonald. *Power System SCADA and Smart Grids*. CRC Press, 2017 (cit. on pp. 14, 20).

[45] Vladimir Terzija, Gustavo Valverde, Deyu Cai, et al. “Wide-area monitoring, protection, and control of future electric power networks”. In: *Proceedings of the IEEE* 99.1 (2010), pp. 80–93 (cit. on p. 15).

[46] *Operational Technology Cybersecurity for Energy Systems*. `https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems`. Accessed: Feb 1, 2023 (cit. on p. 15).

[47] *Gartner Glossary - Information Technology (IT)*. https://www.gartner.com/en/information-technology/glossary/it-information-technology. Accessed: Feb 1, 2023 (cit. on p. 15).

[48] Murat Kuzlu, Manisa Pipattanasomporn, and Saifur Rahman. "Communication network requirements for major smart grid applications in HAN, NAN and WAN". In: *Computer Networks* 67 (2014), pp. 74–88 (cit. on pp. 15, 16, 44, 50, 82, 117).

[49] Frauke Oest and Sebastian Lehnhoff. "Constraint-based Modeling of Smart Grid Services in ICT-Reliant Power Systems". In: *ENERGY 2022, The Twelfth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*. IARIA XPS Press, 2022, pp. 15–21 (cit. on pp. 16, 19, 43).

[50] Prashant Kansal and Anjan Bose. "Bandwidth and latency requirements for smart transmission grid applications". In: *IEEE Transactions on Smart Grid* 3.3 (2012), pp. 1344–1352 (cit. on p. 16).

[51] Rahul Jain, Eitan Altman, Ekram Hossain, et al. "Guest editorial: The economics of communication networks and systems". In: *IEEE Journal on Selected Areas in Communications* 30.11 (2012), pp. 2089–2092 (cit. on p. 18).

[52] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation*. http://data.europa.eu/eli/reg/2017/1485/oj. Accessed: Feb 6, 2023 (cit. on p. 18).

[53] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation, Article 24: Availability of means, tools and facilities*. http://data.europa.eu/eli/reg/2017/1485/oj. Accessed: Feb 6, 2023 (cit. on p. 19).

[54] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation, Article 22: Categories of remedial actions*. http://data.europa.eu/eli/reg/2017/1485/oj. Accessed: Feb 6, 2023 (cit. on p. 19).

[55] Michael Brand, Shoaib Ansari, Felipe Castro, et al. "A Framework for the Integration of ICT-relevant Data in Power System Applications". In: *2019 IEEE Milan PowerTech*. IEEE. 2019, pp. 1–6 (cit. on pp. 19, 44, 62, 75, 139).

[56] Friederike Wenderoth, Elisabeth Drayer, Robert Schmoll, Michael Niedermeier, and Martin Braun. "Architectural and functional classification of smart grid solutions". In: *Energy Informatics* 2 (2019), pp. 1–13 (cit. on p. 19).

[57] Kyriaki E Antoniadou-Plytaria, Iasonas N Kouveliotis-Lysikatos, Pavlos S Georgilakis, and Nikos D Hatziargyriou. "Distributed and decentralized voltage control of smart distribution networks: Models, methods, and future research". In: *IEEE Transactions on smart grid* 8.6 (2017), pp. 2999–3008 (cit. on pp. 20, 22, 115).

[58] Lena Robitzky, Sven C Müller, Stefan Dalhues, Ulf Häger, and Christian Rehtanz. "Agent-based redispatch for real-time overload relief in electrical transmission systems". In: *2015 IEEE Power & Energy Society General Meeting*. IEEE. 2015, pp. 1–5 (cit. on p. 21).

[59] Larah Brüning Ascari, Nastasha Salame da Silva, and Antonio Simões Costa. "Hierarchical State Estimation Architecture Based on State & Topology Coestimation Performed at Substation Level". In: *Journal of Control, Automation and Electrical Systems* 32.6 (2021), pp. 1603–1616 (cit. on p. 21).

[60] Astrid Nieße and Martin Tröschel. "Controlled self-organization in smart grids". In: *2016 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE. 2016, pp. 1–6 (cit. on pp. 22, 138).

[61] Batoul Hage Hassan, Anand Narayan, Michael Brand, and Sebastian Lehnhoff. "Virtualization for performance guarantees of state estimation in cyber-physical energy systems". In: *Energy Informatics* 5.1 (2022), pp. 1–12 (cit. on p. 22).

[62] Algirdas Avizienis, J-C Laprie, Brian Randell, and Carl Landwehr. "Basic concepts and taxonomy of dependable and secure computing". In: *IEEE transactions on dependable and secure computing* 1.1 (2004), pp. 11–33 (cit. on pp. 23, 24).

[63] Bart W Tuinema, JL Rueda Torres, A Stefanov, F Gonzalez-Longatt, and MAMM van der Meijden. *Probabilistic Reliability Analysis of Power Systems*. Springer, 2020 (cit. on p. 23).

[64] UG Knight. "Disturbances in Power Systems and their Effects". In: *Power Systems in Emergencies: From Contingency Planning to Crisis Management* (2001), pp. 7–34 (cit. on pp. 23, 25).

[65] *European Union (EU) Operations Annual Reports - Incident Classification Scale (ICS), 2021*. https://www.entsoe.eu/network_codes/sys-ops/annual-reports/. Accessed: Feb 1, 2023 (cit. on p. 24).

[66] Jonas Wäfler and Poul E Heegaard. "Interdependency modelling in smart grid and the influence of ICT on dependability". In: *Meeting of the European Network of Universities and Companies in Information and Communication Engineering*. Springer. 2013, pp. 185–196 (cit. on pp. 24, 32–34).

[67] E Ahlers, Y Aniol, and B Scholz. "BDEW Roadmap—Realistic Steps for the Implementation of Smart Grids in Germany". In: *BDEW Bundesverband der Energie-und Wasserwirtschaft eV, Berlin* (2013) (cit. on p. 25).

[68] Elisabeth Drayer, Jan Hegeman, Marc Lazarus, Raphaël Caire, and Martin Braun. "Agent-based distribution grid operation based on a traffic light concept". In: *CIRED 2015-The 23nd International Conference on Electricity Distribution*. 2015 (cit. on p. 25).

[69] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation, Article 25: Operational Security Limits*. http://data.europa.eu/eli/reg/2017/1485/oj. Accessed: Feb 6, 2023 (cit. on pp. 27, 51, 68).

[70] *Electronic Data Interchange (EDI) Library: IEC 62325 - Coordinated Capacity Calculation - Contingency List, Remedial Actions And Additional Constraints (CRAC)*. https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/. Accessed: May 22, 2023 (cit. on p. 28).

[71] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation, Article 33: Contingency Lists*. http://data.europa.eu/eli/reg/2017/1485/oj. Accessed: Feb 20, 2023 (cit. on p. 28).

[72] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation, Chapter 5: Contingency Analysis and dandling*. http://data.europa.eu/eli/reg/2017/1485/oj. Accessed: Feb 20, 2023 (cit. on p. 28).

[73] *Under voltage [27]/Over voltage [59] Relay*. https://electengmaterials.com/under-voltage-27-over-voltage-59-relay/. Accessed: Sept 1, 2023 (cit. on pp. 29, 59).

[74] Steven M Rinaldi, James P Peerenboom, and Terrence K Kelly. "Identifying, understanding, and analyzing critical infrastructure interdependencies". In: *IEEE control systems magazine* 21.6 (2001), pp. 11–25 (cit. on p. 30).

[75] Per Hokstad, Ingrid B Utne, and Jørn Vatn. *Risk and interdependencies in critical infrastructures*. Springer, 2012 (cit. on p. 30).

[76] Jonas Wäfler and Poul E Heegaard. "Interdependency in smart grid recovery". In: *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. IEEE. 2015, pp. 201–207 (cit. on pp. 32, 33, 84).

[77] James PG Sterbenz, David Hutchison, Egemen K Çetinkaya, et al. "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines". In: *Computer networks* 54.8 (2010), pp. 1245–1265 (cit. on pp. 32–34, 38, 40, 46).

[78] Daniel Schacht, Dirk Lehmann, Hendrik Vennegeerts, Simon Krahl, and Albert Moser. "Modelling of interactions between power system and communication systems for the evaluation of reliability". In: *2016 Power Systems Computation Conference (PSCC)*. IEEE. 2016, pp. 1–7 (cit. on pp. 32, 33).

[79] Jonas Wäfler and Poul E Heegaard. "A combined structural and dynamic modelling approach for dependability analysis in smart grid". In: *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. ACM. 2013, pp. 660–665 (cit. on pp. 32, 34).

[80] Kristof Kamps, Fabian Möhrke, Markus Zdrallek, and Michael Schwan. "Modeling of smart grid technologies for reliability calculations of distribution grids". In: *2018 Power Systems Computation Conference (PSCC)*. IEEE. 2018, pp. 1–7 (cit. on pp. 32, 34, 52, 91, 93).

[81] Kristof Kamps, Fabian Möhrke, Karl Friedrich Schäfer, et al. "Modelling and risk assessment of special protection schemes in transmission systems". In: *2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. IEEE. 2020, pp. 1–6 (cit. on pp. 32, 34).

[82] Jose Sanchez Torres, Raphael Caire, and Nouredine Hadjsaid. "Towards a Complex Networks Modeling of Interdependent Critical Infrastructures". In: *Workshop Interdisciplinaire sur la Sécurité Globale-WISG 2013*. 2013 (cit. on pp. 32, 35, 36).

[83] Dung T. Nguyen, Yilin Shen, and My T. Thai. "Detecting critical nodes in interdependent power networks for vulnerability assessment". In: *IEEE Transactions on Smart Grid* 4.1 (2013), pp. 151–159 (cit. on pp. 32, 35, 36, 84).

[84] Mahshid Rahnamay-Naeini, Zhuoyao Wang, Andrea Mammoli, and Majeed M Hayat. "Impacts of control and communication system vulnerabilities on power systems under contingencies". In: *2012 IEEE Power and Energy Society General Meeting*. IEEE. 2012, pp. 1–7 (cit. on pp. 32, 35, 36).

[85] Narayan Bhusal, Michael Abdelmalak, Md Kamruzzaman, and Mohammed Benidris. "Power system resilience: Current practices, challenges, and future directions". In: *IEEE Access* 8 (2020), pp. 18064–18086 (cit. on pp. 37–39, 41, 122).

[86] Mathaios Panteli and Pierluigi Mancarella. "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience". In: *IEEE Power and Energy Magazine* 13.3 (2015), pp. 58–66 (cit. on pp. 37, 39, 41).

[87] Suhail Afzal, Hazlie Mokhlis, Hazlee Azil Illias, Nurulafiqah Nadzirah Mansor, and Hussain Shareef. "State-of-the-art review on power system resilience and assessment techniques". In: *IET Generation, Transmission & Distribution* 14.25 (2020), pp. 6107–6121 (cit. on p. 38).

[88] Martin Braun, Christian Hachmann, and Jonas Haack. "Blackouts, restoration, and islanding: a system resilience perspective". In: *IEEE Power and Energy Magazine* 18.4 (2020), pp. 54–63 (cit. on p. 39).

[89] Carrington Nichelle'Le K, Ian Dobson, and Zhaoyu Wang. "Extracting resilience metrics from distribution utility data using outage and restore process statistics". In: *IEEE Transactions on Power Systems* 36.6 (2021), pp. 5814–5823 (cit. on pp. 39, 40, 101).

[90] Zhaohong Bie, Yanling Lin, Gengfeng Li, and Furong Li. "Battling the extreme: A study on the power system resilience". In: *Proceedings of the IEEE* 105.7 (2017), pp. 1253–1266 (cit. on pp. 39, 40).

[91] Linas Martišauskas, Juozas Augutis, Ričardas Krikštolaitis, et al. "A framework to assess the resilience of energy systems based on quantitative indicators". In: *Energies* 15.11 (2022), p. 4040 (cit. on p. 39).

[92] Rohan Samarajiva and Shazna Zuhyle. "The resilience of ICT infrastructure and its role during disasters". In: (2013) (cit. on pp. 39, 40).

[93] Chuanxiong Guo, Lihua Yuan, Dong Xiang, et al. "Pingmesh: A large-scale system for data center network latency measurement and analysis". In: *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*. 2015, pp. 139–152 (cit. on pp. 44, 95).

[94] Ali Abur and Antonio Gomez Exposito. *Power system state estimation: theory and implementation*. CRC press, 2004 (cit. on pp. 44, 45, 49–51, 89, 114).

[95] Uros Kerin, Chris Heyde, Rainer Krebs, and Edwin Lerch. "Real-time dynamic security assessment of power grids". In: *The European Physical Journal Special Topics* 223.12 (2014), pp. 2503–2516 (cit. on pp. 44, 52, 53, 58).

[96] CM Hird, H Leite, N Jenkins, and H Li. “Network voltage controller for distributed generation”. In: *IEE Proceedings-Generation, Transmission and Distribution* 151.2 (2004), pp. 150–156 (cit. on p. 45).

[97] Frhat Aeiad, Wenzhong Gao, and James Momoh. “Bad data detection for smart grid state estimation”. In: *2016 North American Power Symposium (NAPS)*. IEEE. 2016, pp. 1–6 (cit. on p. 45).

[98] Hesam Khazraj, Filipe Miguel Faria da Silva, and Claus Leth Bak. “Bad data detection and identification for state estimation: An enhanced strategy”. In: *CIGRÉ Symposium 2017*. CIGRE (International Council on Large Electric Systems). 2017 (cit. on pp. 45, 93).

[99] Michael Brand, Davood Babazadeh, and Sebastian Lehnhoff. “Trust in Power System State Variables based on Trust in Measurements”. In: *2021 IEEE Madrid PowerTech*. IEEE. 2021, pp. 1–6 (cit. on pp. 45, 139).

[100] Rajkumar Palaniappan, Björn Bauernschmitt, Dominik Hilbrich, and Christian Rehtanz. “An intelligent measurement and control device for active distribution grids”. In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. IEEE. 2020, pp. 975–979 (cit. on p. 48).

[101] Kaveh Dehghanpour, Zhaoyu Wang, Jianhui Wang, Yuxuan Yuan, and Fankun Bu. “A survey on state estimation techniques and challenges in smart distribution systems”. In: *IEEE Transactions on Smart Grid* 10.2 (2018), pp. 2312–2322 (cit. on pp. 50, 122).

[102] Robert Lukomski and Kazimierz Wilkosz. “Methods of measurement placement design for power system state estimation”. In: *AT&P journal* Plus 2 (2008), pp. 75–79 (cit. on p. 50).

[103] Gergő Bendegúz Békési, Lilla Barancsuk, István Táczi, and Bálint Hartmann. “Benchmarking Various Pseudo-Measurement Data Generation Techniques in a Low-Voltage State Estimation Pilot Environment”. In: *Applied Sciences* 12.6 (2022), p. 3187 (cit. on pp. 50, 93).

[104] *DKE: Characteristics of voltage in public electricity supply networks; German version, DIN EN 50160: 2020-11*. `https://www.dke.de/de/normen-standards/dokument?id=7171257&type=dke%7Cdokument`. Accessed: Nov 24, 2023 (cit. on pp. 51, 68).

[105] FNN. *Voltage Regulating Distribution Transformer (VRDT) – Use in Grid Planning and Operation*. Tech. rep. Accessed: March 10, 2023. Forum Netztechnik / Netzbetrieb im VDE (FNN), 2016 (cit. on p. 51).

[106] Rajkumar Palaniappan, Dominik Hilbrich, Björn Bauernschmitt, and Christian Rehtanz. “Co-ordinated voltage regulation using distributed measurement acquisition devices with a real-time model of the Cigré low-voltage benchmark grid”. In: *IET Generation, Transmission & Distribution* 13.5 (2019), pp. 710–716 (cit. on p. 52).

[107] Marcel Klaes, Jannik Zwartscholten, Anand Narayan, Sebastian Lehnhoff, and Christian Rehtanz. “Impact of ICT Latency, Data Loss and Data Corruption on Active Distribution Network Control”. In: *IEEE Access* (2023) (cit. on pp. 53–55).

[108] Shemsedin Nursebo Salih and Peiyuan Chen. “On coordinated control of OLTC and reactive power compensation for voltage regulation in distribution systems with wind power”. In: *IEEE Transactions on Power Systems* 31.5 (2015), pp. 4026–4035 (cit. on p. 53).

[109] Renzo Angles. “The Property Graph Database Model.” In: *AMW*. 2018 (cit. on p. 57).

[110] VS Alagar, K Periyasamy, VS Alagar, and K Periyasamy. “Extended finite state machine”. In: *Specification of software systems* (2011), pp. 105–128 (cit. on p. 62).

[111] *European Union (EU) Commission Regulation 2017/2196 - Establishing a Network Code on Electricity Emergency and Restoration*. `http://data.europa.eu/eli/reg/2017/2196/oj`. Accessed: May 7, 2021 (cit. on p. 70).

[112] Bernard Knueven, James Ostrowski, and Jean-Paul Watson. “On mixed-integer programming formulations for the unit commitment problem”. In: *INFORMS Journal on Computing* 32.4 (2020), pp. 857–876 (cit. on p. 76).

[113] Conseil international des grands réseaux électriques. Comité d’études C6. *Benchmark systems for network integration of renewable and distributed energy resources*. Cigré, 2014 (cit. on pp. 81, 118).

[114] Yiming Wu, Lars Nordström, and David E Bakken. “Effects of bursty event traffic on synchrophasor delays in IEEE C37.118, IEC61850, and IEC60870”. In: *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. 2015, pp. 478–484 (cit. on p. 82).

[115] JP Iloh and Okeke Shedrach. “Communication technologies evolutionary trends in substation automation”. In: *International Conference on Power Engineering-13 (ICOPE-13)*. 2013, p. 3 (cit. on p. 83).

[116] Kishor S Trivedi and Andrea Bobbio. *Reliability and availability engineering: Modeling, analysis, and applications*. Cambridge University Press, 2017 (cit. on p. 85).

[117] Kaustav Chatterjee, V Padmini, and SA Khaparde. “Review of cyber attacks on power system operations”. In: *2017 IEEE Region 10 Symposium (TENSYMP)*. IEEE. 2017, pp. 1–6 (cit. on p. 95).

[118] Edmund M Clarke, William Klieber, Miloš Nováček, and Paolo Zuliani. “Model checking and the state explosion problem”. In: *Tools for Practical Software Verification: LASER, International Summer School 2011, Elba Island, Italy, Revised Tutorial Lectures* (2012), pp. 1–30 (cit. on p. 96).

[119] Yongheng Yang, Huai Wang, Ariya Sangwongwanich, and Frede Blaabjerg. “Design for reliability of power electronic systems”. In: *Power electronics handbook*. Elsevier, 2018, pp. 1423–1440 (cit. on p. 103).

[120] Martin Bicher, Matthias Wastian, Dominik Brunmeir, and Niki Popper. “Review on Monte Carlo Simulation Stopping Rules: How Many Samples Are Really Enough?” In: *Simulation Notes Europe (SNE)* 32.1 (2022), pp. 1–8 (cit. on p. 106).

[121] Batoul Hage Hassan, Anand Narayan, Michael Brand, and Sebastian Lehnhoff. "Modeling of Resilient State Estimation in Cyber-physical Energy Systems". In: *Abstracts of the 12th DACH+ Conference on Energy Informatics*. Vol. 6 (Suppl 2). DACH+ Conference on Energy Informatics 3. Springer, Oct. 2023 (cit. on p. 138).

[122] Laszlo Lakatos, Laszlo Szeidl, and Miklos Telek. *Introduction to queueing systems with telecommunication applications*. Vol. 388. Springer, 2013 (cit. on p. 139).

[123] Lars Fischer, Jan-Menno Memmen, Eric Veith, and Martin Tröschel. "Adversarial resilience learning-towards systemic vulnerability analysis for large and complex systems". In: *arXiv preprint arXiv:1811.06447* (2018) (cit. on p. 140).

[124] Emanuele Ciapessoni, Diego Cirio, Andrea Pitto, Gerd Kjølle, and Marino Sforna. "An integrated framework for power and ICT system risk-based security assessment". In: *2013 IEEE Grenoble Conference*. IEEE. 2013, pp. 1–6 (cit. on p. 140).

[125] Emanuele Ciapessoni, Diego Cirio, Gerd Kjølle, et al. "Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties". In: *IEEE Transactions on Smart Grid* 7.6 (2016), pp. 2890–2903 (cit. on p. 140).

Erklärung

Hiermit erkläre ich, dass ich diese Arbeit eigenständig verfasst und keine anderen als die angegebenen Hilfsmittel und Quellen benutzt habe. Ebenso versichere ich, dass diese Dissertation weder in ihrer Gesamtheit noch in Teilen einer anderen wissenschaftlichen Hochschule zur Begutachtung in einem Promotionsverfahren vorgelegen hat.

Declaration

I declare that I have written this thesis independently and that I have used only the resources indicated. I also affirm that this dissertation has not been submitted by me, in whole or in part, to any other university for assessment in a doctoral procedure.

Oldenburg, July 17, 2024

Anand Narayan