On the Identification and Analysis of ICT-Induced Stability Risks in Cyber-Physical Energy Systems

A thesis approved for the academic degree of

Doktor der Ingenieurwissenschaften (Dr.-Ing.)

at the

Faculty of Electrical Engineering and Information Technology
TU Dortmund University

by

Marcel Klaes, M. Sc.

Supervisor:	Univ. Prof. Dr.-Ing. habil. Christian Rehtanz TU Dortmund University
Co-Advisor:	Univ. Prof. Dr. rer. nat. Sebastian Lehnhoff Carl von Ossietzky University of Oldenburg

Day of Oral Examination: 18.06.2024

Abstract

This thesis addresses emerging ICT-based stability risks for cyber-physical energy systems (CPESs) in light of the increasingly complex task of coordinating modern generation and consumption assets in power grids. It does so by identifying cyber-physical services as the main drivers of interdependence first. It then provides a general approach on how to assess such a service's dependence on data in general and its sensitivity towards the high-level ICT error categories "latency", "data loss" and "data corruption" in particular. Based on these results, the service states "normal", "limited", and "failed" are introduced in order to summarise the findings in an abstract and more widely applicable as well as comparable manner. These aggregated service states are required as additional inputs for the main method which determines how disturbances propagate through modern CPESs. This method is first presented with a focus on static stability and is later extended to also incorporate dynamic stability phenomena. The resulting disturbance propagation, combined with the service states and the ENTSO-E state description for power systems, can be used to derive a summarising state trajectory which helps compare different CPES layouts and control designs concerning their stability.

Kurzfassung

Diese Arbeit befasst sich mit neuartigen, IKT-basierten Stabilitätsrisiken für cyber-physikalische Energiesysteme (CPES) vor dem Hintergrund zunehmend komplexer Koordination neuartiger Verbraucher und Ezeugungsanlagen in modernen Energiesystemen. Dazu werden zunächst IKT-basierte Dienste als Haupttreiber wechselseitiger Abhängigkeiten zwischen der Energie- und IKT-Domäne im CPES identifiziert. Anschließend wird ein Ansatz zur Bewertung der Datenabhängigkeit solcher Dienste im Allgemeinen sowie ihrer Empfindlichkeit gegenüber erhöhter Kommunikationslatenz, Datenverlust und Datenkorruption im Speziellen vorgestellt. Basierend auf diesen Ergebnisse werden drei Betriebszustände für Dienste eingeführt. Diese lauten "normal", "eingeschränkt" und "fehlerhaft" und dienen der Abstraktion und Vergleichbarkeit der IKT-Abhängigkeit verschiedener Dienste. Im Anschluss wird eine Methode vorgestellt, die der Bestimmung der Ausbreitung von Störungen innerhalb des CPES dient. Die Methode wird zunächst mit einem Fokus auf statischer Stabilität erläutert und anschließend so erweitert, dass auch dynamische Stabilitätsphänomene berücksichtigt werden können. Die sich daraus ergebende Ausbreitung von Störungen kann in Verbindung mit den Betriebszuständen und der ENTSO-E-Zustandsbeschreibung für Stromversorgungssysteme zur Ableitung eines zusammenfassenden Zustandsverlaufs verwendet werden. Mit den so ermittelten Zustandsverläufen wird wiederum ein qualitativer Stabilitätsvergleich verschiedener CPES-Layouts und Regelungskonzepte ermöglicht.

Contents

1 Introduction

1.1 Motivation

The transition of power systems in pursuit of global decarbonisation leads to major changes in the nature of consumption and generation in electrical energy systems. On the one hand, two primary energy sectors, namely, transportation and heat, are bound to undergo some level of electrification to pivot at least partially from fossil to renewable resources [1, 2, 3, 4]. This will lead to a drastic increase in both the total demand for electrical energy as well as the level of simultaneous consumption due to typical charging and utilisation patterns for electric vehicles and heat pumps [5, 6, 7]. On the other hand, a substantial share of today's conventional power plants is to be replaced successively by a plethora of distributed energy resources (DER) which, among others, comes with bidirectional power flows [8]. Besides this fundamental change to the core task of transporting electrical energy from its place of generation to consumers, this also introduces significant volatility due to most DER's dependence on uncontrollable aspects such as solar irradiation or wind speed levels. The decommission of conventional power plants does furthermore mean that DERs need to reliably provide stability-crucial services to system operators in their stead [9, 10]. Thus, an increasingly challenging demand side with higher consumption and simultaneity levels will emerge, combined with a largely new, volatile and complex generation side that will nonetheless have to guarantee a stable operation of the power system.

One resulting main task for this transition is to prepare the electrical grid for the increased demands while keeping the changing nature of electrical energy generation in mind. Conventionally, this task would have been met with physical grid expansion which is designed to withstand even worst-case scenarios but can be expensive, especially when many distribution grids would need to be reinforced simultaneously. This conventional worst-case planning and the corresponding expansion can be an inefficient way to tackle the challenge, though [11]. It accounts for various rare yet extreme situations that would require an equally extreme over-provisioning of the grid with parts of the resulting grid capacity being left unused at most times. A valid alternative would be to – at least partially – substitute physical grid expansion with less costly means to increase the efficiency of the grid as demanded in [11]. This could, for example, mean actively coordinating controllable assets in such a way that

rare load or generation spikes can be avoided [12]. In this light, the second main task for the transition is to create, compare, test and ultimately implement system and control designs as well as processes that would render the provision of control reserve and ancillary services by coordinated DER as reliable as it is with conventional power plants today.

Both main tasks depend on the yet to be realised integration and coordination of millions of DER as well as other modern consumption and storage assets. This coordination can only be realised with the help of information and communications technologies (ICT) [5] as they require automation and therefore a reliable exchange of information or data. A power system that, to some increased degree, relies on ICT is called a cyber-physical energy system (CPES) [13]. While advances in ICT have drastically increased the accessibility and performance of communication in general, one cannot assume ICT to always operate perfectly since the exchange of data can be flawed. These flaws can, among others, result in impaired decision-making of automated or manual system operator processes or delays in time-critical control actions. This is why ICT can no longer simply be assumed to be an ideal system in analyses and simulations of critical infrastructures as it was typically done in past works. As shown in Fig. 1.1, the relevance of considering imperfect ICT performance is further emphasised by the fact that in CPESs the dependence of the power and ICT systems is bidirectional [14]: While stable power system operation will depend on the reliable communication of data, the ICT infrastructure needs reliable power supply in order to enable this very communication. This interdependence gives rise to new cascading and escalating fault scenarios that can have potentially dire consequences for the stability of a CPES [15].

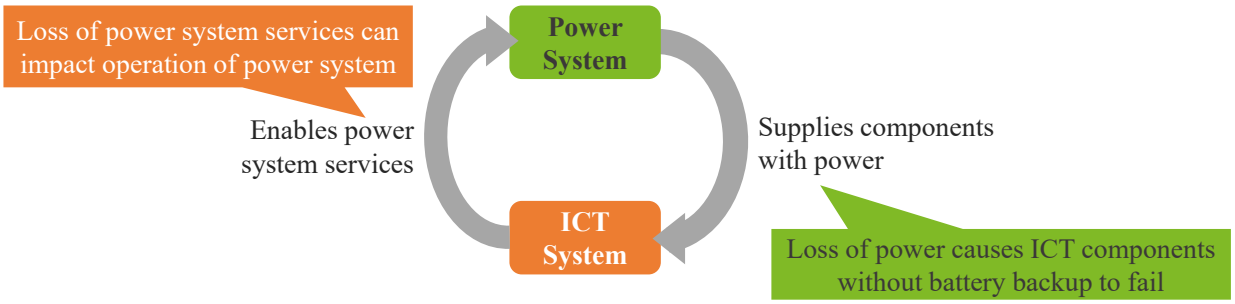


Figure 1.1: Interdependence of Power and ICT Systems in CPES

In short, societies will see a transition towards CPESs with interdependent ICT and power sub-systems. These CPESs are expected to work at least as reliably and even more efficiently than nowadays's power systems, despite the new interdependencies

and the corresponding, potentially undiscovered new risks. Therefore, developing a method to identify and analyse these interdependencies and ideally quantify the added risks for various CPES designs is of utmost importance. Accordingly, the central research question of this thesis is about how the increasing penetration of ICT in modern and future power systems might introduce new risks to the CPES' stability and how to mitigate them. This overarching question can be broken down into three more specific and more approachable research questions:

1. How do disturbances unfold in a modern CPES under consideration of the new interdependencies between ICT and power system domains?
2. How far is the stability of a CPES affected by the growing interdependence?
3. How to compare different CPES designs considering their stability?

1.2 Related Work

The assessment of conventional power system stability is a well-known and thoroughly researched and documented field as demonstrated, for example, in [16] and [17]. In contrast to this, identifying stability-crucial aspects of cyber-physical systems and understanding their internal interdependencies is a younger field of research, especially in the context of power systems, which emerged around 2007 and gained momentum in 2013. Several novel approaches and methods to identify, analyse or describe the interdependence between power and ICT systems and the resulting risks for CPES stability have been published since by, among others, Jean-Claude Laprie, Jonas Wäfler or Mathaios Panteli:

In 2007, Laprie et al. introduced an interdependence model for CPES that describes the state of a power system and the corresponding ICT infrastructures with one out of five different states each [18]. The authors additionally differentiated not only between cascading, escalating and common cause failures, but also between accidental failures, which result from technical faults, and malicious attacks. While the presented model is fairly comprehensive and already hints towards further analyses in combination with other modelling techniques such as Petri nets or stochastic activity networks, the description itself remains on a purely conceptual level, only.

In 2011, Panteli et al. first categorised the chain of ICT-based processes in power system operations and summarised the potential effects of ICT failures on a power system [19]. Based on this chain of ICT-based processes, the author then introduced three

different states of the power system, between which it is crucial to distinguish when assessing the interdependencies in CPES. These states, namely the 'actual state', the 'presented state' and the 'perceived state', ultimately describe how the real, physical instance of a power system can differ from the power system that is presented to and perceived by a system operator and how this can potentially lead to impaired decision-making [19]. Panteli furthermore suggested stochastic modelling approaches like Monte Carlo simulations and, accordingly, provided a case study, too. Between 2012 and 2013 Panteli focused his research on the perceived state, specifically on the impact of situational awareness in CPES operational decision-making in [20] and [21]. He also presented a multi-state Markov model as a means to quantify these effects.

In 2013, Wäfler et al. introduced the term smart grid services. Similarly to Panteli's approach, the authors underlined the relevance of distinguishing between the real, physical system and the perceived view a monitoring service would have onto that real system [22]. In contrast to Laprie et al., Wäfler et al. present a state model consisting of three states each for power and ICT system, namely 'ok', 'excited' and 'failure'. The authors furthermore suggest conducting further quantitative analyses of services based on fault tree analyses by deriving the corresponding dependability parameters with Markov models of the component level first [22]. This suggested approach has then been tested and published in [23]. This assessment was extended in 2015 by a dedicated analysis of interdependence in smart grid recovery processes [24]. Wäfler's aggregated contributions to the research on interdependence in CPES can be found in his doctoral theses [25].

In 2018, Inger Anne Tøndel et al. provided an updated thorough overview of the research on CPES interdependencies [14]. This work furthermore refines and extends Laprie's definitions of common cause, cascading and escalating interdependencies and their differences. Similarly, it introduces a categorisation for methods that aim at the identification and analysis of interdependencies.

In summary, the literature on emerging ICT-based risks in CPESs provides fundamental definitions and categories for a better understanding of the general problem and approaches to solve it. These approaches focus on assessing the likelihood of specific events like component faults and the resulting cascading and escalating failures in the power system.

1.3 Research Gap, Contribution and Structure

A common drawback of the previously presented models and in the literature on CPES interdependence, as also stated by Panteli in [21], is their dependence on statistical data on component failure rates. Adequate data for such stochastic analyses with regard to power system equipment has been collected and published over several decades and is therefore readily available, for example in [26]. In contrast to this, no such data is publicly available for ICT components except for some small-scale data collections that are based on very little data as shown in [27]. A potential reason for the low availability of historical reliability data for ICT equipment is the components' much shorter life cycles as well as the much wider range of different manufacturers and device variants. This shortcoming renders stochastic methods like fault tree analyses and Petri nets impractical. Therefore, the approach presented in the thesis at hand does not focus on stochastic analyses or the likelihood of specific failures in general, but rather on the expected impact of disturbances on a CPES' stability. Regarding these very consequences of disturbances in a CPES, preceding works and literature so far only cover detailed, yet case-specific models on the one hand, or highly generalised models beyond applicability on the other. This is why this work provides a new method for modelling the impact of disturbances and control actions on the CPES with both, a high level of abstraction that enables generalisation and yet sufficient detail regarding the interconnections between ICT and power system domains. This is achieved by summarising service-specific sensitivities to three ICT error categories. The resulting abstraction layer presents operational service state definitions which are based on the ENTSO-E's well-established operational power system states for indicating a power system's current risk level. This approach enables a less complex modelling of a wide set of services and their behaviour in times of degraded ICT performance without the need for full co-simulations. Corresponding models can be used to derive the disturbance propagation (e.g. escalating and cascading failures) within a CPES under consideration of coordinated, ICT-reliant grid services that depend on the successful exchange of information. The resulting trajectory of operational system and service states provides a qualitative indication regarding the CPES' stability.

This work is divided into eight chapters. First, the status quo of analysing the stability of conventional power systems is briefly outlined in Chapter 2, followed by an introduction to the CPES, its new interdependencies, and the resulting implications for grid operation, planning and stability in Chapter 3. Chapter 4 then explains and demonstrates the basic ICT dependence of many modern grid services and introduces

an approach to assess a service's expected performance and summarise it via so-called service states. With this basic understanding of the field of research and the CPES challenges at hand, a method for assessing the propagation of disturbances in a CPES is introduced in Chapter 5 along with a CPES state description that enables the qualitative comparison of different CPES designs with regard to their stability. In Chapter 6, an approach for quantifying said state description is presented to further improve the comparison of CPES designs based on metrics. Chapter 7 extends the method introduced in Chapter 5 so that it can also reflect on power system dynamics in order to allow for dynamic stability assessments. Finally, the results of this work are summarised and discussed in Chapter 8. Fig. 1.2 gives an overview of these chapters, their core topics and the according examples and case studies that are included in this thesis.

Regarding individual contributions, it needs to be stated that the contents presented in Chapters 3, 4 and 5 resulted from several years of collaborative work with Anand Narayan who is associated with Carl von Ossietzky University of Oldenburg. Therefore, contents of his dissertation and the thesis at hand do overlap in said parts. The extended focus of the latter is more on the power system aspects in general and the corresponding dynamic analyses on the service level in Chapter 4.1 and on the power system level in Chapter 7 in particular, though. In contrast to that, Anand Narayan's work has a stronger focus on the ICT system and the grid services it enables. Specifically, formal modelling of the operational states of the grid services is proposed, as well as a method to assess and compare different service designs regarding their resilience. Further information on individual contributions is provided with each publication that the corresponding chapters are based on.

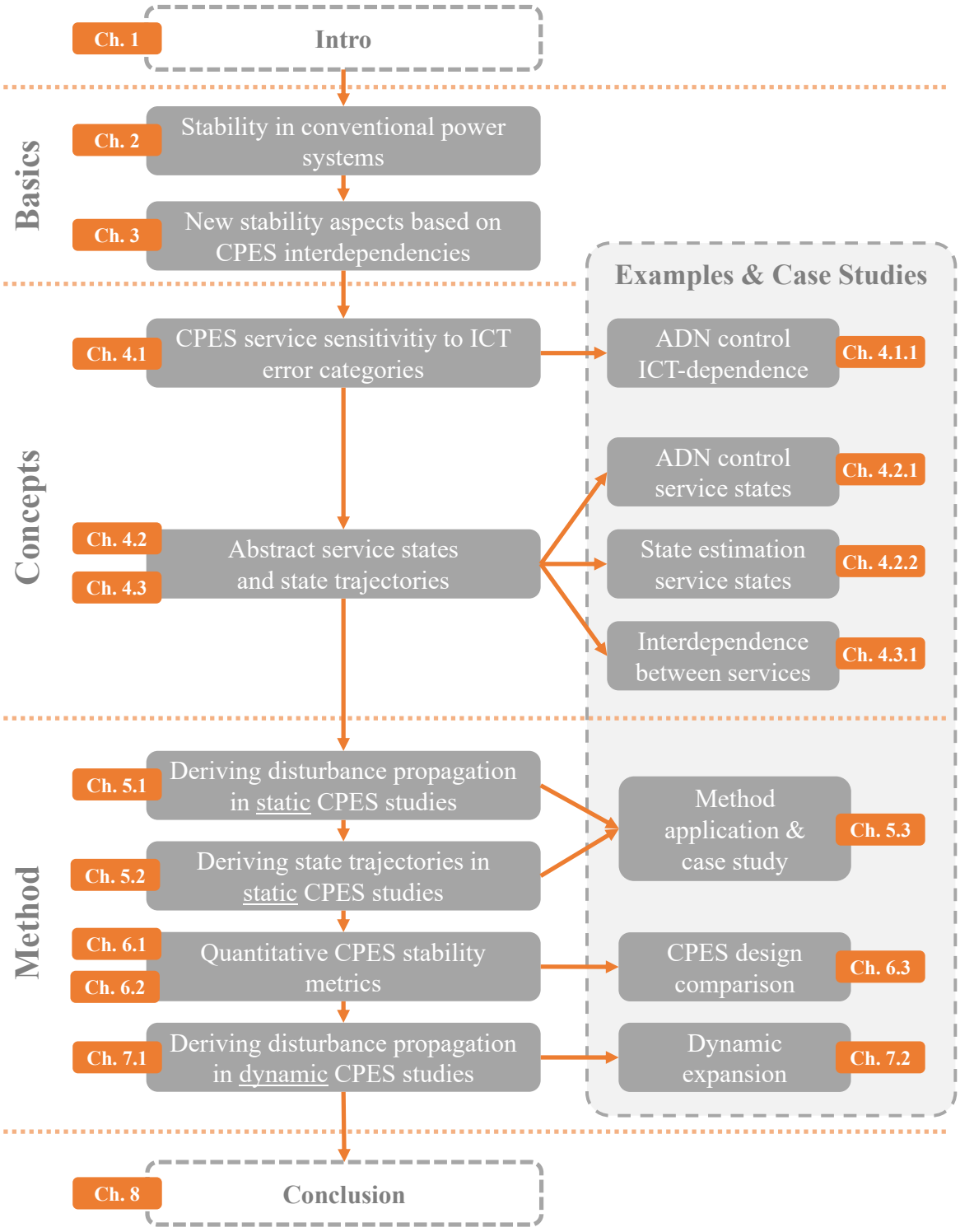


Figure 1.2: Logical structure of this thesis

2 Conventional Power System Stability

The primary technical objective of a power system is to provide electrical energy from generators to consumers [28]. The term power describes the rate at which energy is either converted ('generated' or 'consumed') or transported. Electrical energy is conveyed via electromagnetic fields which temporarily reserve energy. This reserved energy, which is called reactive energy, is required to establish and maintain the electromagnetic fields and cannot directly be used for actual applications such as supplying loads. The energy that is actually transported by the fields and that ultimately supplies consumer loads is called active energy. In power terms, their equivalents are active and reactive power. As a consequence of the principle of energy conservation, energy generation and consumption are always balanced. It is up to the system operators to plan and operate their respective systems in such a way that the resulting balance renders all consumers supplied reliably at all times and even under adverse circumstances, though. The following chapter outlines the most fundamental aspects and categories of power system stability as well as their risks and conventional approaches to analyse them. This is complemented by an introduction to the means and tools leveraged by system operators to plan for and maintain stable grid operation. Even though this chapter is restricted to conventional ('non-cyber-physical') power systems, the resulting knowledge is crucial for understanding the later analyses of stability risks in CPES.

2.1 Static Power System Stability

Prabha Kundur framed one of the most widely used and acknowledged definitions for static power system stability:

Definition 2.1: Static Power System Stability

A power system can be considered statically stable if it is capable 'to remain in a state of operating equilibrium under normal operating conditions and to regain an acceptable state of equilibrium after being subjected to a disturbance' [16].

This well-established yet abstract definition is broken down into less abstract components for the work at hand:

An **acceptable state of operating equilibrium** is reached once energy provision and consumption are in balance and the **transport capacities** between both are sufficient. This means, that for a given set of load requirements, a matching set of control parameters for all controllable assets can be found so that all loads are supplied while all technical constraints are met. These technical constraints are properties of all primary grid assets like power lines, cables, switches and transformers and represent the physical limitations to their point of operation. The first two out of three major limitations concern the assets' **thermal endurance** and their **electrical insulation**:

If an asset's temperature rises too high for too long, for example as a consequence of sustained overload, it will put additional stress on the asset's longevity and potentially break. Typically, such an asset is shut down before permanent damage is applied, though. While various partially external factors like environmental temperature or winds affect a grid asset's temperature, the primary contributor is the electrical current it is conducting. Hence, an upper limit for acceptable currents is defined for every asset and must be respected in operation at all times in conventional assessments in order to avoid damage or protection-based emergency shutdowns. In more recent works, though, accepting short-lived violations of these current limits on power lines and the resulting consequences and implications for power system operation are analysed [29]. Yet, this tolerated and even planned for temporary overstepping is not considered in this thesis.

As for the insulation, it is meant and designed to guarantee currents to flow only where they are intended to and, thus, prevent short circuits, malfunction, component damage, and health risks. This effect is achieved by spatially compressing or distancing the electromagnetic fields so that conducting connections to other surfaces are prevented. The voltage level up to which an insulation can reliably do so depends, among others, on the composition of used materials and the size and geometric design of the conductor, but also on further conductors in the proximity and their distance. While all of these factors are subject to case-specific preferences and both safety- and cost-optimisations during an asset's design phase, they are fixed once the asset is put into operation. This is why, in operation, voltages must not rise above the threshold that the grid assets were designed for as insulation will fail otherwise, leading to deterioration and permanent damage. At the same time, loads require minimum levels of voltage in order to operate as intended. Thus, the voltages on all buses in a power system have to be kept within an acceptable voltage band. According to [30]

this acceptable voltage band relative to a grid level's nominal voltage is defined for transmission systems in continental Europe from 90 % to 111,8 % for all connection points between 110 kV and 300 kV grid levels and from 90 % to 105 % for all connection points between 300 kV and 400 kV. For distribution systems, specifically for low-voltage (LV) grids, voltage levels are acceptable as long as their 10-minute average stays within ±10 % of the nominal voltage at all interconnection points according to [31].

The third major limitation concerns electrical machines like generators and motors and their sensitivity towards operating frequencies. They typically come with a nominal frequency at which they operate efficiently and safely. Yet the frequency of power systems can vary and divert from its nominal value of either 60 Hz in North America, parts of South America, Saudi Arabia, and Japan, or 50 Hz almost everywhere else. Significant deviations from these nominal frequencies may cause mechanical damage to generators and electrical motors due to a 'loss of capacity in the auxiliary gear [or] danger[ous] vibrations' [32]. Therefore, generators have protection mechanisms that will automatically shut them down if frequency deviations exceed specific combinations of extent and duration as shown for example in [33] and [34]. These shut-downs are considered a last resort as they imply a significant decrease in the provision of energy and a general loss in the system's controllability, both of which typically exacerbate any initial problem.

Finally, a **disturbance** is an external event that can affect generation assets just as well as loads or grid assets and potentially leads to **abnormal operating conditions**. Such events can be, for example, trees falling into power lines, natural disasters, components breaking unexpectedly, or collateral damage in construction works. Typical direct consequences of these disturbances can be a change in the power system's topology, an unexpected decrease in available power generation or changes in power consumption. If an adapted system configuration for a new acceptable state of operating equilibrium after the disturbance can be found, the power system is **statically stable** with regard to that specific disturbance. Analyses that focus only on finding such a new operating equilibrium with regard to balanced power generation and consumption and sufficient transport capacities utilise steady-state power system models.

2.2 Dynamic Power System Stability

In this work, a dynamically stable power system is furthermore defined as follows:

Definition 2.2: Dynamic Power System Stability

A power system is **dynamically stable** if a new operating equilibrium state for a disturbed system does not only exist but the transition between the undisturbed and the new equilibrium states can be realised under consideration of the system's dynamic behaviour, too.

In order to study the dynamic stability of a given power system, generally four major steps are necessary according to [35]:

1. Make modelling assumptions and formulate a mathematical model appropriate for the time scales and phenomena;
2. Select an appropriate stability definition;
3. Analyse and/or simulate to determine stability, typically using a scenario of events;
4. Review results in light of assumptions, compare with the engineering experience ("reality"), and repeat if necessary.

Regarding the first of these steps, modelling a power system including all dynamics is theoretically possible, yet overly complex and extremely demanding with regard to computational resources. This is why only the relevant subset of all dynamics is considered in actual studies, while other dynamics are assumed to be out of scope. The individual relevance of asset-specific dynamics depends on the overarching goal of the stability study at hand. In 2004, Kundur et al. defined three main categories of power system stability, namely rotor angle stability, frequency stability and voltage stability [35]. This definition was revisited and extended in 2020 by the IEEE Power System Dynamic Performance Committee and CIGRE in [36]. The summarised outcome of this update can be found in [37], which shows resonance stability and converter-driven stability as two additional main stability categories. The five resulting main categories in total come with various sub-categories, all of which are illustrated in Fig. 2.1.

In addition to the original stability categories, [35] also mentions specific timescales on which different dynamic power system phenomena unfold. This initial definition of timescales was updated and visualised in [37] as shown in Fig. 2.2. Each stabil-

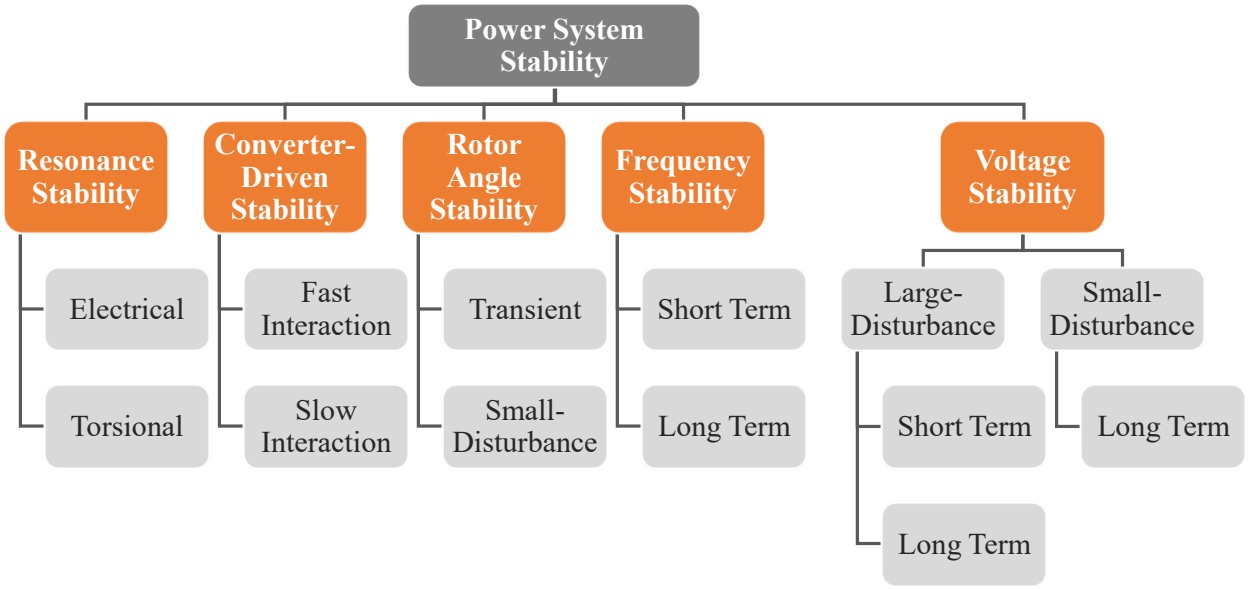


Figure 2.1: Power system stability categories based on [37]

ity category is related to specific dynamic phenomena and their corresponding time scales. Hence, different stability analyses require a different combination of considered dynamics and timely resolution, and therefore a different power system model. A detailed study on overloaded power lines and their rising temperature, for example, would only need to consider the thermodynamic behaviour of the lines which unfolds within up to several minutes before a line reaches critical temperature levels [29]. This is why additionally modelling the electromagnetic behaviour of the line or running simulations with a step size of a few milliseconds would be considered irrelevant and unnecessarily complex for this specific study. Different studies concern rotor angle stability, in which case electromechanic and potentially even electromagnetic dynamics would need to be considered instead of thermodynamics. Furthermore both, the total time frame as well as the required time resolution would vary drastically from the former study.

Based on [38], a power system under consideration of selected dynamics can be formally described by a set of algebraic and differential equations that result in a state-space model:

$$\begin{aligned} \dot{\boldsymbol{x}} &= \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}) \\ 0 &= \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}) \end{aligned} \tag{2.1}$$

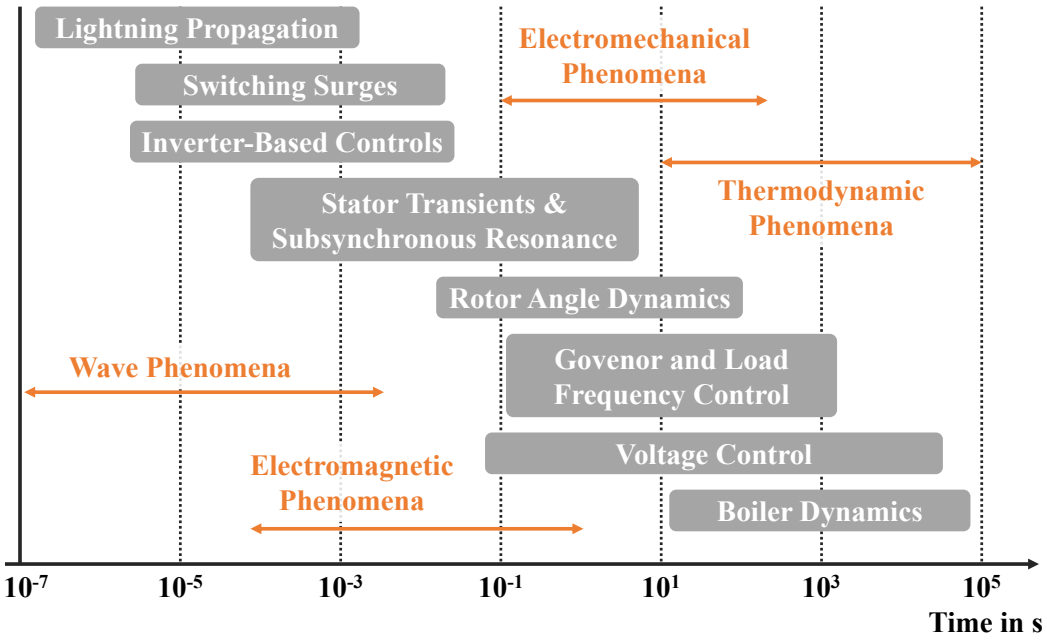


Figure 2.2: Timescales for dynamic phenomena in power systems [37]

The state vector $\boldsymbol{x}$ comprises all differential variables, i.e. all variables of the power system model that can only be described with a derivative term. An intuitive example of such a differential variable is the previously discussed temperature of a line. This temperature does not only depend on factors such as external temperature, cooling winds or the current flow but specifically on their integral over time. In contrast to that, power flow equations are often times described without any derivative terms. Algebraic variables like these are represented by $\boldsymbol{y}$. Finally, $\boldsymbol{u}$ is meant to capture all external control or input variables, e.g. P and Q set-points of generators or reference values for bus voltages.

With a chosen stability category, the according time scale and the corresponding formal power system description in mind, the first step of studying dynamic power system stability is complete. While it results in a model that can be used to calculate the power system state at a given point in time under various circumstances, it does not directly provide any indication of the stability of the system. This is why stability needs to be defined in the context of every specific analysis, which constitutes the second step in the study of dynamic power system stability. For example, the system model can provide a line's temperature over time, but it lacks information about what thermal behaviour would be considered stable or unstable.

The third step in studying dynamic stability phenomena of power systems concerns the actual simulation or analysis of the system. On the one hand, the analytical

approach typically focuses on system-theoretical stability definitions like Lyapunov or input/output stability, both of which are described in [39]. These approaches provide more general and fundamental claims about a system's stability in comparison to simulation-based approaches. Yet, modelling a power system so that an analytical stability assessment is possible requires both linearisation and severe simplifications, rendering the final analytical model less realistic. This is why 'the stability of power systems to large disturbances is typically explored in simulations' [35]. Running simulations based on the dynamic power system model described by equation 2.1, on the other hand, is done with numerical approaches. These simulation-based approaches can only provide case-specific insights, though. While this allows for more realistic and detailed modelling of a specific power system under consideration of specific, well-known disturbances, it also means that no general proof of stability can be made based on simulation results alone.

The fourth and final step requires the simulation results and their interpretation regarding system stability to be critically reflected upon. This implies, among others, to assess the general validity of the results under consideration of all previously made assumptions.

2.3 Stability in Power System Operation

On an application level, maintaining the stability in modern, increasingly ICT-reliant power systems is a growingly intricate challenge for transmission system operators (TSOs) and distribution system operators (DSOs) due to the changes outlined in Chapter 1. Hence, the most central aspects of power system operation with regard to stability are outlined in this chapter.

Handling Disturbances: Remedial Actions and Protection Systems

All generation assets, grid assets, and loads that are flexibly controllable and participate in either balancing generation and consumption or securing sufficient transport capacities are called flexibilities. They can be either controlled by a system operator (e.g. line switches, tap-changing transformers, compensation units), by plant operators or by private owners as is typically the case for small-scale DERs. A remedial action (RA) can be any potential activation of flexibility that is aimed at either

preventing or curing a contingency in the power system. Fig. 2.3 is based on [30] and gives an overview of the different categories of RAs including some examples for each category. This thesis' scope is restricted to those RAs highlighted in orange in Fig. 2.3 only, but the resulting method can also incorporate most other RAs.

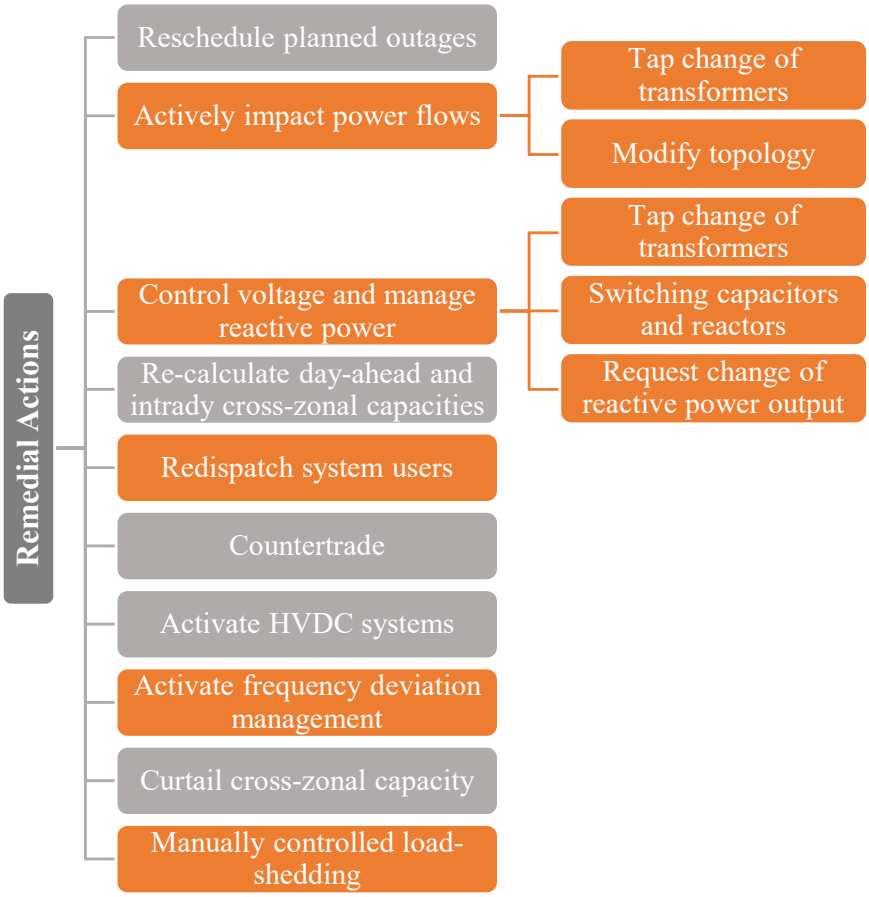


Figure 2.3: Remedial action categories and examples [30]

In addition to these RAs, a wide range of fully-automated protection mechanisms is installed in all power systems. These protection mechanisms are usually designed as a last resort to either prevent permanent damage to assets or protect the power system from spreading or cascading issues. These two categories of protection mechanisms are accordingly called 'device protection' and 'system protection'. Typically, these mechanisms take in local measurements, make decisions based on pre-defined control strategies within tens of microseconds up to a few milliseconds, and, ultimately, trip power lines or initiate an emergency shutdown in other assets. Yet, as this timescale does not allow for remote communication, let alone remote coordination, the protection aspect is out of this work's scope.

Sensing Disturbances: Monitoring

System operators, specifically DSOs, can neither measure the total provision of and demand for P and Q nor the available transport capacities in their system directly in a sufficiently detailed way. While conventional power plants can provide detailed information about their generation, small-scale DERs are often times not connected to the operator's control centre. Additionally, the majority of loads - especially in low voltage grids - are either not connected, as well, or are not even equipped with digital measurement devices to begin with. The chosen solution to this missing knowledge about actual generation and consumption levels is to use indicative substitute measurements. Hence, generator frequencies f and bus voltages V, which can be obtained more easily, are used to monitor and maintain P and Q balances as V and f are directly influenced by P and Q imbalances.

The mere collection of field measurements cannot directly be aggregated, though, as their availability, accuracy and time of origin can vary. Therefore, the so-called state estimation (SE) is implemented in order to transform said collection of raw measurements into a consistent set of voltage magnitudes and angles for all buses. The resulting overview of the real-time operating conditions critically improves the information which the operator's situational awareness and decision-making processes are based on [40]. The SE takes in all available measurements within pre-defined time windows and provides an estimation of the current topology, voltages and currents of the observed power system. Details on SE algorithms, their variants, network observability analyses and the interpretation of SE results can be found in [41]. These SE results can be compared with the previously described technical constraints (voltages and currents) of all assets in order to identify any active contingencies in the system. The ENTSO-E labelled these technical constraints operational security limits (OSLs). As an example, the explicit OSLs definitions of the German TSOs can be found in [42].

Finally, system operators frequently conduct a contingency analysis (CA). Its goal is to assess the power system's preparedness for typical contingencies on the basis of SE results and under consideration of all available RA. For each combination of typical contingency and available RA, a power flow calculation is performed, which uses the most recent SE results as input parameters. The (n-1)-criterion defines a power system as sufficiently prepared for typical contingencies as long as the CA does not identify any violation of an OSL.

Aggregated Threat Assessment: ENTSO-E System States

An acknowledged indicator widely used by system operators to summarise and exchange information about their power system's current health or risk level is the ENTSO-E system state classification. Despite its high abstraction level, this state classification considers many complex aspects of power system risk assessment. This state classification defines the five operational states **normal, alert, emergency, blackout** and **restoration**. This chapter about the simplified ENTSO-E system state classification is based on [MK1] and all original details can be found in the official EU regulations [30, 43]. The classification itself is based on the five aforementioned states. The Restoration state takes a special role as it is subsequent to the Emergency and Blackout States [30] but it is not a direct result of the state identification process itself. Therefore, the work at hand focuses on the remaining four states, all of which can be defined exactly for each point in time of operation. Each abnormal state (i.e., alert, emergency and blackout) has a range of predefined measures and actions, which the system operator can take to bring the system back to the normal state. Note that according to Article 2 of [30], these system states are also applicable to DSOs, however, detailed investigations regarding DSOs are out of the scope of this work. Fig. 2.4 summarises and illustrates the ENTSO-E state identification process based on [MK1]. In order to increase the clarity of its core concepts, two simplifications are made: For one, not all possible transitions between the states are depicted. For the sake of clarity, the CA is shown as a process with two separate calculation steps, which, in reality, would be one single step. Based on the results from the CA and the check on OSL violations, the current power system state can be identified as follows:

A power system is said to be in its **normal state** as long as the check on current OSL violations is negative and the CA does not identify any potential contingencies which would cause OSL violations, as well.

The **alert state** is triggered if the CA identifies at least one potential contingency that cannot be handled appropriately based on the current SE results and the currently available RAs and would thus violate an OSL. Note that in this state, there is no OSL violation in the real power system yet. The alert state and the CA are focused on impact of additional theoretical disturbances. Nonetheless, a lack of more than 20 % of the required amount of active power reserves for more than 30 minutes triggers the alert state, too. RAs that are activated to bring the system back from alert to normal state are preventive RAs.

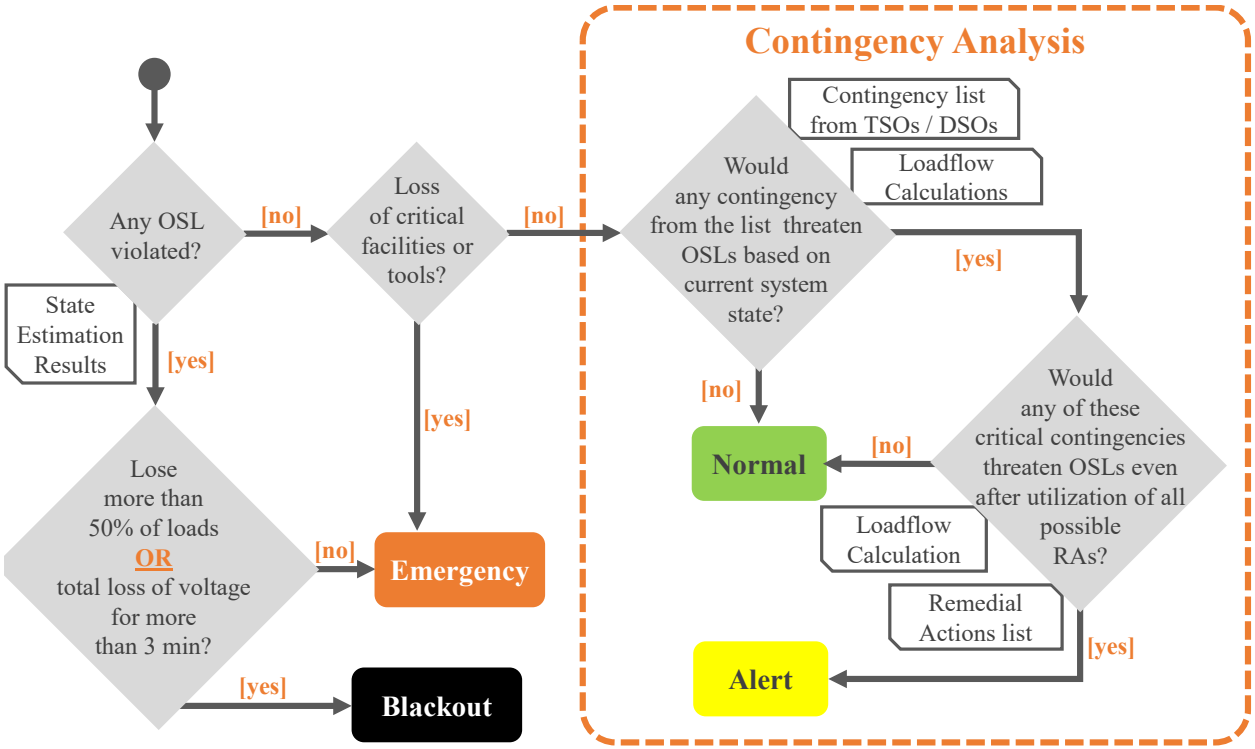


Figure 2.4: Simplified overview of the ENTSO-E state identification process

If any OSL is violated, an immediate transition to the **emergency state** is triggered. The second important condition for a transition to the emergency state is the failure of any critical tool or facility defined in [30] for more than 30 minutes. They include monitoring tools such as the SE but also functions like switch control, the communication between multiple TSOs and the operational security analysis itself. However, the impact on the system state when the failure of these critical tools and facilities is less than 30 minutes is not defined in [30]. Additionally, the system is also in the emergency state when at least one measure of the System Defence Plan, described in [43], is activated. All RAs that are being activated in order to bring the system back from the emergency state to either its normal state or at least its alert state are labelled curative RAs.

If the loss of loads exceeds 50 % of the total load in a transmission system or if there is no voltage for more than 3 minutes, the system is defined to be in the **blackout state**.

Mitigating Disturbances: System Planning

While this work is about ICT-induced stability risks in CPES and thus mostly about stability in operation, system design and planning are critical, too. Not only can short-term planning improve the availability of preventive and curative RA, but also does long-term planning include the physical extension of grid components, which increases redundancy and thus passive grid robustness in general. As stated in Chapter 1, many modern challenges could be solved by over-provisioning in form of extreme dimensions of physical grid extension. In accordance with conventional grid planning, this would imply increasing grid redundancy to a point where even rare worst-case scenarios would no longer lead to any overload or congestion. Yet, increasing the total potential and control-ability of flexibility providers promises to be a more efficient partial substitute to physical grid expansion in many cases [11]. This is why being able to assess and compare different system and control designs with regard to their efficiency but also their impact on the CPES' robustness, is of great importance for appropriate system planning.

This Chapter's Core Insights

- Conventional power system stability studies can be divided into static and dynamic assessments. Static assessments aim at finding new operational state equilibria for a changed or disturbed system configuration. Dynamic assessments investigate whether the new operational state equilibrium can be reached under consideration of dynamics.
- In power system operation, the operators rely on sensor data for establishing situational awareness and on the successful transmission of control data in order to prevent, contain or remedy disturbances.
- The dependence of system operators on data transmission increases with the degree of remote/centralised asset coordination in the power system.
- The current threat level of an operator's power system is signalled to other operators with the help of ENTSO-E system state classification. Its corresponding well-established system states are 'normal', 'alert', 'emergency' and 'blackout'.

3 Interdependence in Cyber-Physical Energy Systems

The basic aspects and means of analysing the stability of conventional power systems have been explained in the previous chapter. The next step is to understand what modern CPESs are, how far they differ from such conventional power systems, and how their ICT and power subsystems interact with and depend on each other. Only then an appropriate method for analysing ICT-induced stability risks in CPESs can be discussed.

3.1 Introduction to CPES

In theory, power systems have always been dependent on communication to varying yet limited extent. The transmission of both, measurements from sensors in the grid to the control centre and control commands to generators, transformers and switches, has always been crucial to the operation of transmission systems since it enables coordinated decision-making. Conventionally, this part was realised by fully dedicated assets, the so-called 'secondary equipment'. This abstract dependence of power systems on communication and decision-making processes is illustrated in Fig. 3.1, which is based on [44]. In abstract terms, the depicted communication layer can be considered a filter that can affect both sensor and control data. More specifically, a realistic communication layer is vulnerable to disturbances which lead to potentially undesired differences between sent data and received data, whereas an ideal communication layer does not have any impact on that data at all.

In conventional systems, the frequency and amount of information that needed to be generated and transmitted were low in comparison to modern and future power systems, and so was the amount of remotely made control decisions. This allowed for rather relaxed ICT requirements: Adequate communication could already be realised based on primarily local communication (e.g. within a station or substation), manual human-to-human communication, or communication via a dedicated communication system with few dedicated communication lines between stations and control centres. This limited amount of necessary communication connections could furthermore be laid out securely and very robust due to affordable redundancy and limited public access to the communication hardware. This is why the ENTSO-E

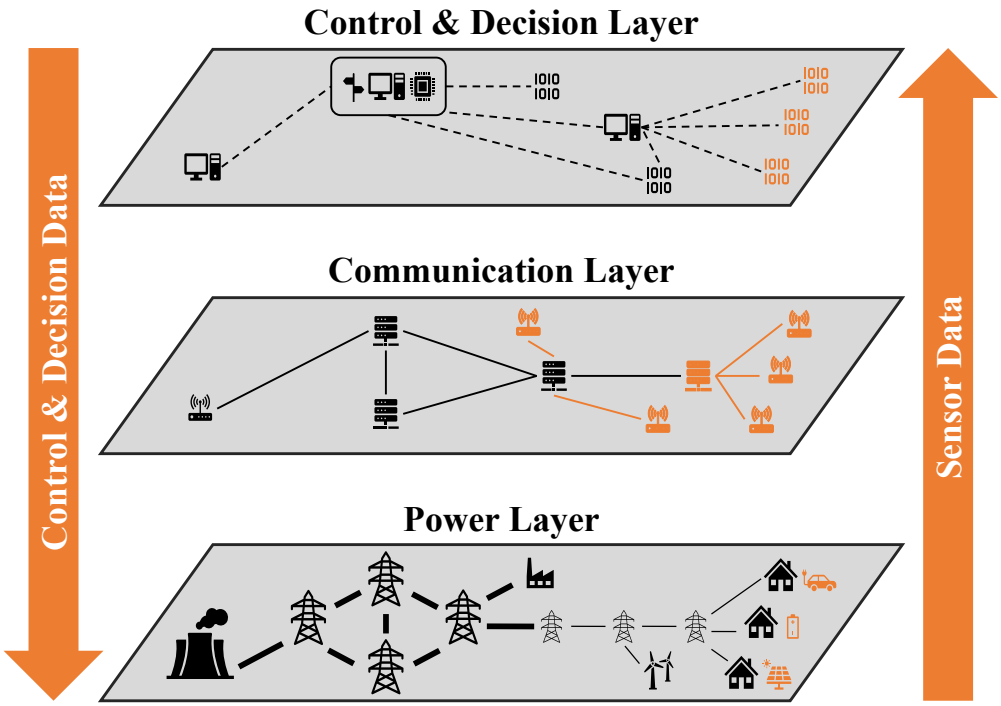


Figure 3.1: Abstract dependence of power systems on communication and decision systems (with emerging aspects in orange)

recommends avoiding the use of publicly operated communication networks on the TSO level [45]. Yet, in conventional distribution systems, communication was less frequent and considered less critical to the point where some DSOs never established any ICT connection to assets in their LV-grids. With the upcoming changes and challenges to power systems mentioned in Chapter 1 in mind, these requirements towards communication are bound to change, though. The increasing need for remote coordination and the rising volatility on both generation and consumption sides render conventional means and practices of power system communication unfit for the tasks ahead, especially on the DSO level. On the one hand, the total amount of controllable assets and decision variables in power systems increases drastically with the rise of DERs. On the other hand, the necessity to coordinate assets instead of relying on sufficiently over-provisioned grid capacities grows, too. Hence, improved automation is required. For this automation to function, the many new DERs need to exchange information with system operators. As the number of DERs and the level of their decentralisation is much higher than those of conventional generation units, dedicated secure communication lines to every single unit cannot be realised any longer due to extreme costs [46]. Instead, last-mile connectivity will have to be realised primarily by leveraging pre-existing wired and wireless communication infrastructures. These

existing infrastructures already provide internet connectivity to most households and DER sites. Using internet technology for CPES control purposes, too, implies a comparatively simple and cost-efficient integration of assets on the one side, but also a wide spectrum of common security concerns on the other [47, 48].

In light of these changes and challenges, communication cannot be assumed to be an ideal aspect of power system studies any longer. The ICT system becomes an integral component of power systems that furthermore demands a more detailed and realistic consideration in modern stability assessments. This justifies the dedicated name of 'cyber-physical energy systems' in order to underline the more complex and critical involvement of ICT.

Finally, Fig. 3.2 demonstrates this increasing complexity of ICT in CPES in comparison with conventional power systems. It depicts all involved actors and their bilateral communications required for a wide-area voltage control process in MV and LV grids based on a German study [49]. The exact roles and details of the actors are irrelevant for this demonstration, yet all actors and all remote communications that are proposed to be added to the conventional grid are coloured orange. Remote communication that is already required in conventional power systems is coloured green and all local communication is coloured grey.

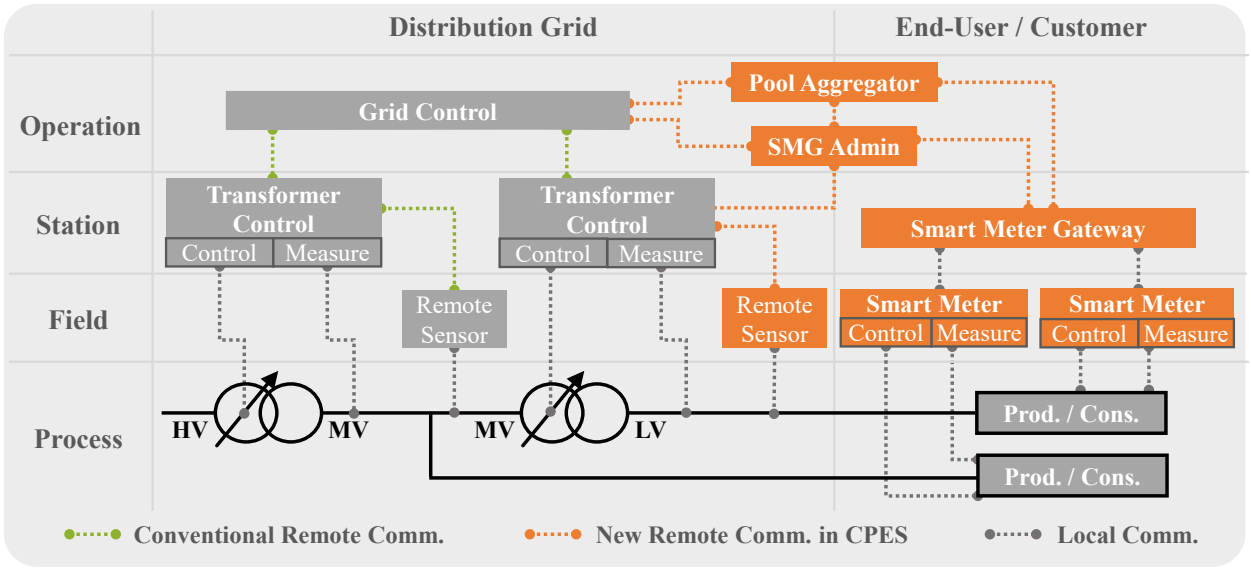


Figure 3.2: Example for increasing ICT complexity in CPES

3.2 Circular Interdependence in CPES

A CPES can easily be subdivided into its power and ICT domains, but this does not suffice for analysing ICT-induced risks as the interfaces between the domains remain abstract and hard to identify. Thus, further decomposition is recommended: In addition to the already known **ICT level** and **power system level**, a new **data level** and a **service level** are introduced in this work. These two additional levels focus on said interfaces and enable a more concrete consideration of the interactions between the domains. Metaphorically speaking, the data and service levels represent the bridgeheads that connect the abstract ICT and power sides of a CPES.

In this concept of four distinct CPES levels, the power system level comprises all passive topological and physical aspects of the power system infrastructure. Analogously, the ICT level is defined to represent all passive aspects of the CPES' ICT system such as its topology, hardware configuration and parameters. The impact of adverse ICT conditions on the performance of the data that is transmitted by the ICT system is represented by the data level. At last, any control function or service that can actively change the topology, generation or consumption of the power system is located on the service level.

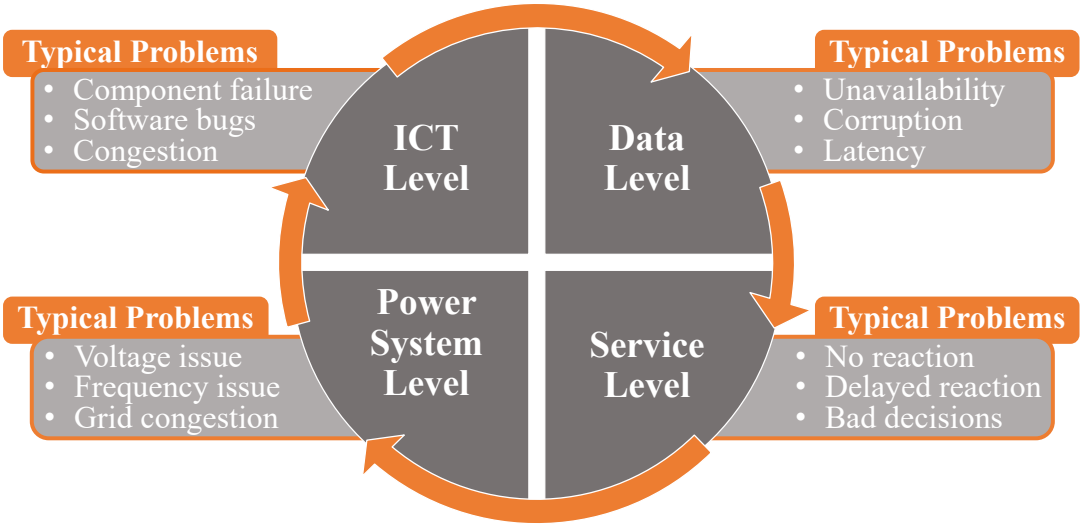


Figure 3.3: Circular CPES dependencies causing cascading and escalating failures

Each of the four CPES levels can have an impact on another while potentially being affected by a third one. Data, for example, can only be transmitted correctly and in time if the underlying ICT infrastructure has been designed adequately and is

operating as designed. Flawed data itself can cause an ICT-reliant (power system) service to show delayed reactions or incorrect decisions. These adverse circumstances on the service level can again lead to critical problems in the power system or to a situation in which an uncorrelated contingency in the power system cannot be remedied adequately any longer. All these different examples of cascading failures can be summarised as a circular dependence among the CPES levels. This concept of circular CPES dependence is illustrated in Fig. 3.3, which can also be considered a more detailed extension to Fig. 1.1. The details about this concept of circular CPES dependencies, the four levels and how they are connected are explained next:

The power system level is where the passive physical behaviour of the power system is described, simulated and assessed. 'Passive' in this case means that only the intrinsic response of the grid and connected assets without any remotely coordinated control influence is considered. Therefore all kinds of coventional power flow calculations, dynamic grid equations and further stability assessment methods previously explained in Chapter 2.1 are assigned to this power system level. Disturbances on this level can lead to unsupplied loads in the grid, which include communication devices.

Analogously to the power system level, **the ICT level** describes the ICT system's components, topology, and its passive behaviour with regard to changing the power supply. Due to this work's focus on CPES interdependencies, the ICT level is assumed to only comprise basic ICT devices that enable the transmission of abstract data, namely communication links, routers, servers, sensors, and controllers. While, of course, many more types of ICT devices are used in real-world communication systems, they typically don't react differently in case of power outages. For example, it does not make a difference, if a switch, a gateway, or a router is affected by a loss of power as in all cases data cannot be transmitted or forwarded by the device any longer. Hence, power system events primarily impact the ICT system's topology, which is therefore critical to consider in CPES studies. Communication networks on a scale of metropolitan or wide area networks, such as those required to communicate between DER sites and substations or even control rooms, are typically realised based on up to four different topologies. Wired communication networks use meshed, ring-shaped or tree topologies and wireless communication networks typically use the star topology with one central station that many devices connect and interact with. Similar to power systems, the used topology of a communication network varies with its level: Meshed topologies with redundant connections between the nodes are mostly

used for the backbone or core (communication) network of network service providers. The ring topology is most prominent on the medium communication network levels in-between core and access networks, such as regional or metro networks. Tree and star topologies, which lack redundancy, are typically used for the so-called 'last-mile connectivity' in access networks. In the context of power systems, this term has previously been used for example in [47] to describe the connection of communication endpoints, such as substations, with the communication core network. While the problem today is no longer about connecting substations but rather DER sites, the potential technological solutions and their advantages and disadvantages are fundamentally unchanged. As described in [47] and [48], valid communication technologies are satellite communication, power line communication, wireless communication, and wired communication technology. Satellite communication comes with viable yet still significant costs and poses the risk of weather-dependent connection issues [47]. In a worst-case scenario, these issues might render controlling many DERs within an area during extreme weather phenomena impossible. This is why satellite communication is unlikely to become the default technology for communication in CPESs while it can still be considered an excellent option for remote sites or as a redundant backup communication for particularly important assets. Power line communication, despite already being used in some cases of power system communications and being a 'perfect fit with the smart grid ecosystem' [50], still struggles with noise levels that are increased by new DERs and electric vehicles on the one hand, and various cyber security concerns on the other [50]. A dedicated new wired communication infrastructure, as mentioned before, would impose unreasonably high costs. A viable and practical solution to this particular problem is to leverage the pre-existing wired communication infrastructure. As most households and industrial sites nowadays already have a functional wired internet connection, the idea of using this very connection for power system purposes, too, comes naturally. While this approach initially promises low investment costs, the desired level of connectivity also requires DERs, sensors and other new assets in a CPES to use the internet (communication) protocol [51]. A communication based on this protocol means relatively simple and cheap integration of devices as modern assets typically come with native internet capacities or can be rendered compatible with off-the-shelf gateway solutions. On the downside, using an open standard like the internet protocol implies a high risk of cyber attacks [51, 52]. Mitigating these security issues, as done in Germany with a vastly complex authorisation sub-infrastructure [53], is likely to noticeably increase costs again, though. It furthermore leads to an increase in the overall level of complexity of the system as well

as the number of required service providers and actors [54]. Wireless communication technology, too, mitigates the issue of costly last-mile connectivity. Depending on the chosen sub-type of wireless communication technology, the pre-existing cellular communication infrastructure can be used, too. The drawback of wireless communication, though, lies in places with weak signal reception, such as basements, which DERs and smart meters are often installed in. Furthermore, using the established cellular network implies the use of internet technology along with its advantages and disadvantages, again. The different communication technologies, topologies and levels that are potentially involved in CPES control are illustrated in Fig. 3.4, which is based on [55]. Any disturbance on the described ICT level might affect the exchange of data which is realised by the corresponding ICT system.

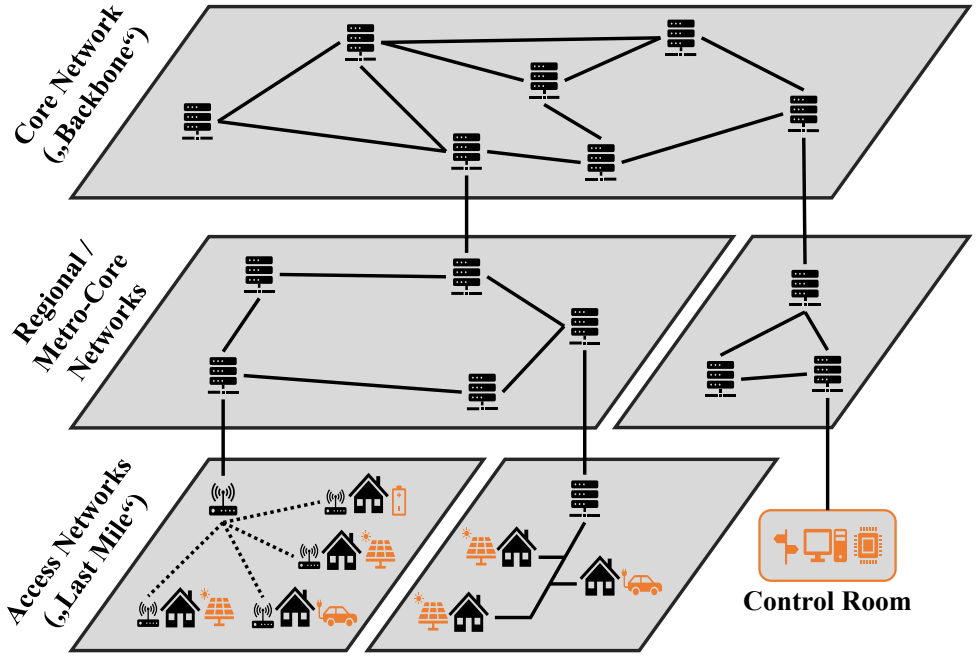


Figure 3.4: Communication levels, topologies, and technologies in CPESs

The data level is meant to represent the quality of transmitted data independent from a specific service in a simplified or aggregated way. For example, this data can be measurement data from a sensor, received at the control centre just as well as it can be a control signal received by a substation. Considering analyses of stability critical ICT-induced risks, one should always assume all transmitted data to potentially be affected adversely by a wide range of faults on the ICT level. As a means of simplification and abstraction, the three most relevant categories of adverse data effects, namely **latency** (delayed data), **unavailability** (unavailable data) and **corruption**

(incorrect data), are used throughout this work. These categories were presented in [MK2][1] and partially overlap with the known aspects of quality of service but aim at an even higher level of abstraction as well as the inclusion of incorrect information. As shown in fig. 3.5, latency is about data that is received with an abnormally high delay but is otherwise correct. Exemplary reasons for increased latency could be an ICT network congestion, potentially caused by a component failure or abnormally high network usage as a consequence of either unforeseen events or coordinated attacks. Unavailability describes a temporary loss of data at the receiving end. For non-time-critical scenarios, unavailability can overlap with latency whenever unavailable data can be requested again and used at a later point in time. For time-critical scenarios or in cases with communication protocols that do not support re-transmissions (like UDP), unavailable data does impose an additional set of risks to services, though. Data loss can be a typical consequence of broken communication links and unexpected congestion. Data corruption represents all cases in which received data does not represent the information that it is expected to do. In this case, it is irrelevant whether the data is affected by an early-stage sensor failure or whether it gets altered shortly before arriving at the receiving end. Corrupted data can be the consequence of either technical problems like said sensor failure and software bugs or specialised cyber-attacks such as man-in-the-middle attacks. Any of these adverse conditions of received data can potentially lead to unintended or inaccurate results for those services that rely on that data.

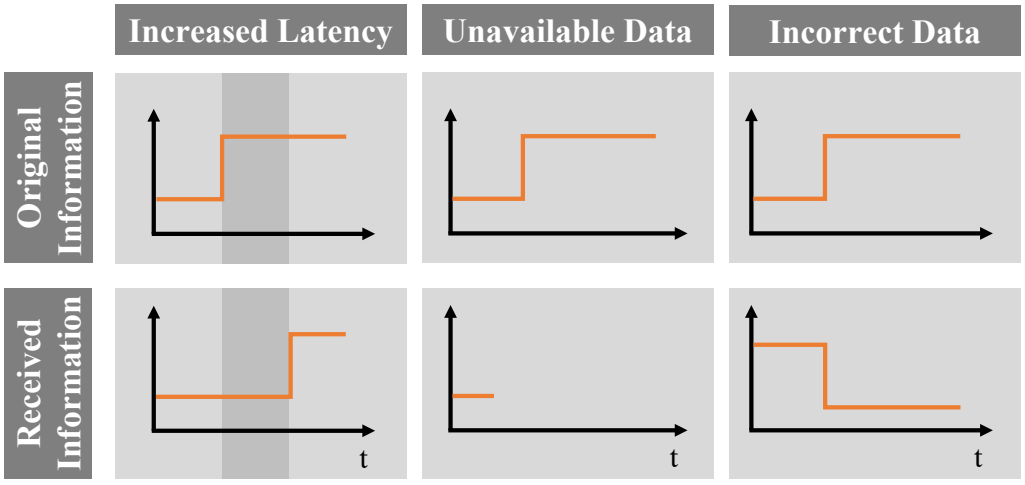


Figure 3.5: Abstraction of the ICT-level: Considered ICT error categories

[1]This work was done in full collaboration between A. Narayan and M. Klaes, individual contributions cannot be assigned.

The service level comprises all functions, tools or facilities in a CPES that are designed to actively change either its topology, or the generation or consumption of the active and reactive energy of consumers and DERs. As these services provide system operators with the means to counter impending voltage and frequency problems as well as to manage network congestion, the reliability of these services is of utmost importance [22]. Two types of services are distinguished in this thesis: Conventional power system services that operate autonomously and based on locally available data with no dependence on communication on the one hand and cyber-physical services on the other. The latter represent all services that include remote coordination and therefore depend on communication and ICT to some degree. It is irrelevant whether communication and control schemes for a service are centralised, decentralised or distributed; if the service requires the functional exchange of information, it is considered a cyber-physical service and a part of the service level. A disturbance on the service level can therefore be caused by degraded ICT performance and can have diverse consequences depending on the specific service affected. A critical RA service with deteriorated performance can potentially render the system operator incapable to mitigate or manage disturbances on the power system level. Most conventional services, which also contain the majority of protection systems, can rather be considered part of the power system level, as their automatic behaviour is deterministically predictable and does not rely on remote communication.

The service level can theoretically also include services that dynamically change the parameters or configuration of the ICT system instead of the power system. Virtualisation, for example, can decouple software and hardware and dynamically allocate computational resources to those services deemed most critical for a specific situation [56]. Software-defined networking, as described in [57], represents another example. It is meant to prioritise crucial communication over generic network traffic and thereby guarantee acceptable performance of critical services even in times of limited bandwidth or (communication) network congestion. Yet, the consideration of such services that are meant to coordinate and adapt the ICT domain exceed the scope of this work.

Definition 3.1: Services

Since this work focuses on the ICT-based interdependencies in CPESs, the term 'service' refers to cyber-physical power system services which rely on remote coordination and communication unless stated otherwise.

3.3 Implications for CPES Operations

The intertwinement of the four abstract CPES levels has a couple of direct implications for the operation of a CPES. These implications are outlined next in order to explain how far stability analyses differ between cyber-physical and conventional power systems as described in Chapter 2.3, and additionally demonstrate where impaired data can have an impact. This understanding can later be leveraged to adapt system planning processes accordingly and under consideration of crucial interdependencies.

On the one hand, non-ideal data can lead to **impaired control capacities**: For all RAs that are not implemented locally and autonomously, a direct dependence on the functional exchange of information is obvious. If, for example, control data (e.g. an activation command) is delayed or lost, the RA is only beginning to counter a given disturbance later than expected by the operator or not at all. Another case is based on details of the activation command being altered either by a technical error or by an attacker. The consequences of undetected corrupted control data can potentially be diverse and arbitrarily extensive. Therefore, understanding the impact of all three ICT error categories on any service that is found to be crucial for the CPES' stability is imperative and detecting compromised control capacities can be a critical contribution to the operator's situational awareness. In addition to that, the consideration and implementation of so-called fallback strategies that mitigate the impact of non-ideal data are recommended. A simple example of such a fallback strategy is an alternative mode of operation which is more robust or even autonomous but potentially less efficient and is activated once communication-based problems are detected.

On the other hand, **impaired monitoring and decision making** can be a consequence of data problems just as well: As explained in Chapter 2.3, the SE represents a crucial service as its results are used as a basis for critical system operator decisions. The operator furthermore plans and activates RAs in case of disturbances based on his perceived view of the CPES. Thus, bad state estimation results, which can be caused by impaired data, can potentially lead to incorrect decisions on the operator's side even under otherwise ideal circumstances. This is why SE services are typically equipped with features designed to detect and filter out bad or implausible data. Yet, the SE is not the only service that relies on external data for decision making. In general, for each service that either fully depends on or optionally takes in state

estimation results or other remote data, the cases of delayed, missing and especially incorrect information need to be considered. This is aligned with the differentiation between the actual system state and the perceived system state of system operators, made by Panteli in [19].

In addition to these two direct operational implications, the indirect impact of **impaired power supply for ICT components** for CPES operation must be considered, too: While it appears obvious that ICT components require a functional power supply for their operation, the further consequences for power system stability are often underestimated in studies. In modern, highly automated power systems with a high penetration of ICT, cascading failures in CPES can no longer be ignored or considered a mere detail prone to simplification into neglect. Escalating failures, which describe cases with an initial failure in one domain not directly causing but exacerbating another failure in the other domain, must not be ignored any longer, too. Instead, the circular dependence described in Chapter 3.2 needs to be understood, acknowledged, and, finally, addressed adequately in stability assessments.

All these possible consequences of impaired data can be addressed best in the planning process of a CPES. The additional investment cost required to mitigate any of said risks by increasing the security and redundancy in either power or ICT system cannot be accepted by default for all functions and services within a CPES. Yet, it is recommended to identify and improve those services that are too important for stability or simply too costly for operators to accept them failing.

This Chapter's Core Insights

- The power and ICT domains of a CPES depend on each other.
- This interdependence nowadays primarily results from centrally coordinated services and their dependence on the exchange of data and on ICT equipment requiring power supply.
- In future CPESs, distributed services might substitute centrally coordinated service. These distributed services still require data to be exchanged.
- Degraded ICT performance may lead to impaired monitoring, impaired decision making or impaired control capacities for power system operators. A degraded power system performance may lead to a degraded exchange of data due to unsupplied ICT equipment.

4 Interdependence Caused by Cyber-Physical Services

The service and data levels have previously been explained and identified as crucial connections between the two primary domains of a CPES. A cyber-physical service, as defined in Chapter 3.2, takes in a combination of sensor information and measurements and potentially reacts based on these inputs by sending control data to actuators which are controllable assets in the CPES. Following the guideline on electricity transmission system operation [30], this reaction is ultimately aimed at preventing or managing a disturbance or contingency in the CPES by adapting the system configuration, e.g. its topology, generation or consumption accordingly. Depending on the type of disturbance, the required speed and precision of the service's reaction may vary. If a reaction is too slow or too inaccurate, the initial problem might not be remedied appropriately or might even get exacerbated. This chapter's focus is first on assessing isolated services, their general dependence on data and their specific performance degradation in case of impaired data. Based on these insights, a new service state description is presented. These service states are meant to indicate the currently expected performance of a service based on previously assessed data requirements of the service on an abstract level. Finally, an approach to combine the well-established ENTSO-E operational states with these novel service states for multiple services is outlined.

4.1 Dependence of Cyber-Physical Services on Data and Communication

When it comes to analysing the dependence of power system services on ICT, running a detailed co-simulation with both power and ICT networks is a popular approach. Co-simulations are capable of considering detailed bandwidth constraints in combination with realistic network traffic, resulting in dynamic, precise levels of package loss and delay on the ICT side. Their significantly increased complexity is a drawback, though, as it leads to higher demands towards in-depth knowledge of both power and ICT domains as well increased modelling efforts and higher computational requirements.

The primary objective of these service analyses, in the context of this work, is to find out how far a service depends on successfully exchanged data and what consequences deteriorated communication would have on the service's performance. The reasons for and origins of impaired data are thus out of this thesis' scope. A full co-simulation can therefore be avoided while still being able to answer the leading question. The starting point of the corresponding assessment, hence, is not the ICT topology, components, and their statistical failure rates but rather the ICT error categories as described in Chapter 3.2. The resulting ICT requirements for services then need to be coupled with conventional power system stability assessment methods. First, the respective service's communication processes need to be known. This includes information on which device or actor is sending what kind of data to which recipient in what order. Ideally, thresholds for acceptable delays for each communication process or for the complete process are known upfront. Fig. 4.1 shows a sequence diagram that provides an overview of all relevant communication and computation processes in a severely simplified service, namely a flexibility activation as a remedial action (RA) via a DER pool aggregator.

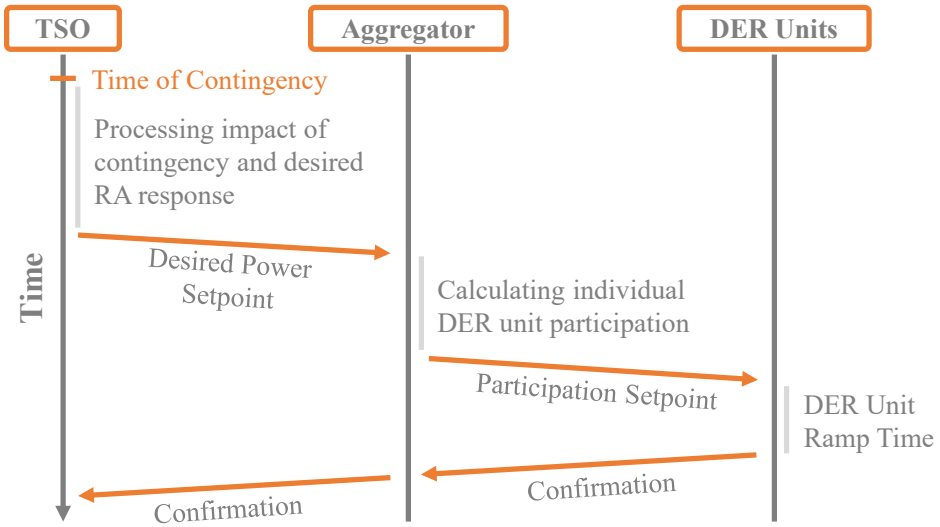


Figure 4.1: Simplified communication and computation sequence of a flexibility call

The illustrated flexibility call process shows that the actual activation command in the form of a new desired setpoint for active power is first sent from the responsible TSO to an aggregator. The aggregator breaks down the total change in provided (or required) active power to one participation setpoint for each involved DER unit. Each unit's participation setpoint then needs to be communicated to the respective DER unit. The communication between TSO and aggregator can – in theory – be considered

reliable due to redundant communication routes or dedicated communication lines. This assumption does not hold for the communication between aggregator and DER units, though, as the costs for redundantly laid out communication lines grow with the number of involved actors. Considering the hundreds of thousands of small-scale units in future decentralised power systems, the cost for a fully redundant wired communication system on all levels down to DERs in LV grids can be considered 'extremely high' [46]. In contrast to that, wireless or cellular communication systems are cheaper yet prone to low signal range and reliability as well as interferences [58].

The next step for analysing this service's dependence on the successful exchange of data lies in a set of simulations where each communication process is assumed to be affected by the three types of ICT errors. This crucial step is very implementation- and system-specific as the results will vary drastically between different power system topologies, different types of DER units and especially different kinds of aggregator controllers. For example, a more sophisticated implementation of this service could include an additional communication process which aims at updating the aggregator about each DER unit's currently available flexibility potential. In that case, it must be decided how the aggregator handles missing updates from some (or all) DER units. The aggregator could assume the last known value to still be correct or decide to consider all units with unavailable updates to not participate in the provision of flexibility until a new update is received. The multitude of combinations of controller designs and system topologies renders general statements on service requirements towards ICT and data difficult. This is why more detailed analyses must happen on a service-specific level next.

4.1.1 Case Study: Active Distribution Network Control

The following chapter comprises a case study on a service similar to the previously shown flexibility call example and it covers the analysis of the service's dependence on data delay, data loss and data corruption. It is meant to prove that modern and future grid services potentially rely on the performance of data exchange means and that adverse ICT conditions can render these services unfit for their dedicated purpose. The grid service selected for this study comes with a wide range of application scenarios in future CPESs and can therefore be considered a valid and representative choice. The case study in this chapter is a summary of the collaborative work

presented in [MK3][2] and [MK4][2], which contain all details.

Active Distribution Networks as a Service Platform

In a largely decentralised energy system that partially relies on DERs to provide ancillary services, it can be reasonable to cluster DERs for control purposes. This can be beneficial since clustering can compensate for the individually higher failure rates of DERs (compared with conventional plants) with a low simultaneity of failures within the cluster. One approach to this clustering focuses on preexisting structures such as distribution networks. When DERs within a distribution network are controlled as one group in order to adapt the power flow at the interconnection point to a higher voltage level, the setup is called an active distribution network (ADN). Such ADNs can be utilised by TSOs as remedial actions for both voltage and frequency contingencies, as well as for congestion management. Thus, ADNs form a representative platform for various critical yet ICT-reliant services which is why the assessment of an ADN's dependence on data in a specific power network poses a fitting demonstration.

In order to initiate an ADN as a remedial action, a TSO is assumed to send a desired new setpoint for the active or reactive power flow at the interconnection point P_{IP}, which is highlighted green in Fig. 4.2, between distribution and transmission systems to the ADN controller. This controller measures the current power flow at P_{IP}, calculates the required changes, breaks them down to a DER-specific level of detail and, finally, sends these DER-specific setpoints to the DERs. This transmission of setpoints to DERs is assumed to be realised by a broadcast signal. In order to assess an ADN's capability to remedy different types of disturbance, the settling time between the ADN controller receiving the new setpoint from a TSO and the measured power flow successfully adapting to it is chosen as the most relevant key performance indicator. The power flow at the interconnection point is considered to have adapted successfully once it stays within a tolerance band of $\pm 5\,\%$ around the new setpoint as suggested in [59]. Note that in the preceding work [MK3] the controller's overshoot is considered a secondary key performance indicator, which did not yield remarkable or unexpected results, though, and was therefore not considered any longer.

[2] M. Klaes' contribution to both these works, besides writing, lies in the conceptualising and implementing ICT errors into the dynamic power system simulation model, which was created by J. Zwartscholten, as well as in running the simulations. Research and result evaluation was done together with A. Narayan, who focused on assuring the quality of simulation parameters.

Simulation Setup

For this explicit case study, the rural 20 kV SimBench benchmark grid, which is described in [60], was modelled in MATLAB Simulink in conjunction with the ADN controller. This grid and the interconnection point between voltage levels are illustrated in Fig. 4.2. The ADN controller receives measurement information from a sensor at this interconnection point and the DERs are located at the nodes.

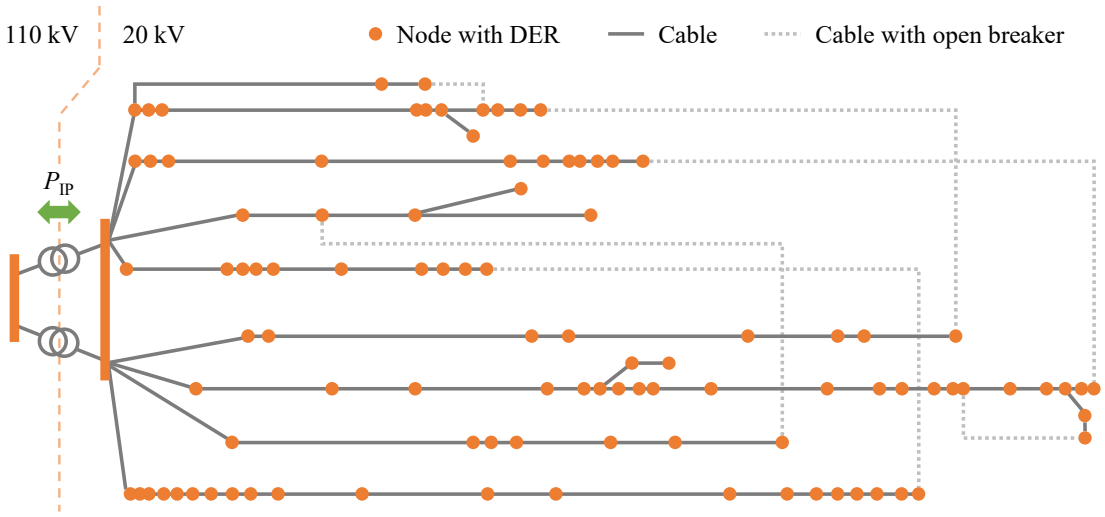


Figure 4.2: SimBench 20 kV rural benchmark grid

The transmission of both, measurement data to the controller and control data to the DERs, is modelled so that the ICT error categories presented in Chapter 3.2 can be simulated. More specifically, data latency is simulated by varying the control data delay and the measurement data delay between 20 ms and 600 ms each. This is implemented as depicted by Fig. 4.3, which shows the full structure diagram for measurement and control system and a simplified flow of data. Accordingly, the original measurement of active power at the interconnection point P_{IP} is sent to the ADN controller via the ICT system. During this stage of the process the first communication-based delay T_{meas} is simulated. The controller then defines the power setpoints $P_{Y,1}$ for each DER based on the received measurements P_{meas}. These setpoints $P_{\mathrm{Y,1}}$ are then transmitted from the controller to the DERs, which requires the simulation of another communication delay T_{con}. The two delays T_{meas} and T_{con} are expected to vary independently from each other as collecting measurement data is assumed to be realised with a different communication network than the transmission of control data.

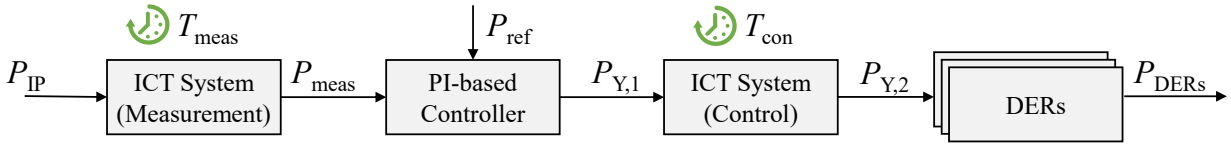
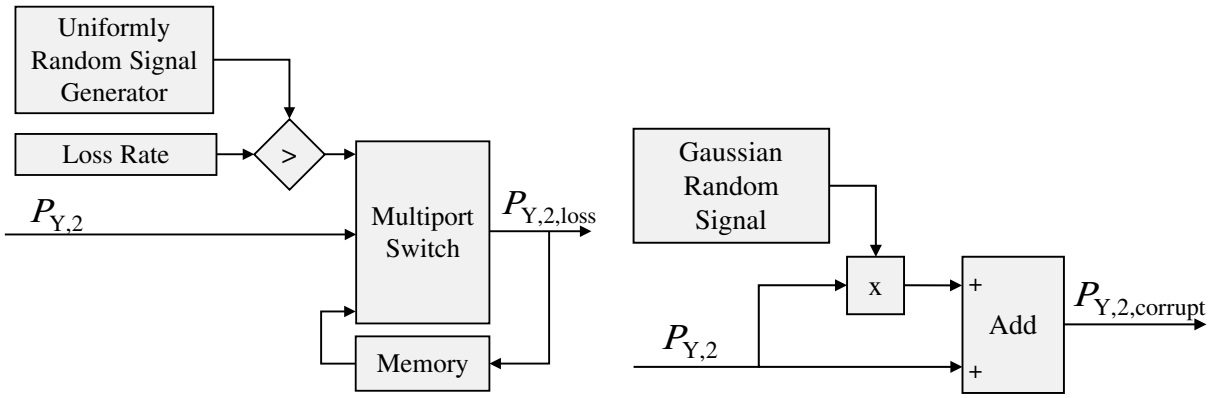


Figure 4.3: Structure diagram with focus on latency in the control system model

For simulating data loss, the control signal that is to be received by the DERs $P_{Y,2}$ is modified. A uniform random signal between 0 and 1 is generated based on a random seed for each transmission. This signal is then compared with the chosen loss rate between 10 % and 90 %, and the outcome of this comparison decides whether $P_{Y,2}$ is dropped or transmitted. The corresponding adaptations to the model structure diagram are shown in Fig. 4.4(a).

Finally, data corruption is simulated by adding noise to the original measurement P_{meas} or control signal $P_{Y,2}$ as shown in Fig. 4.4(b). This noise is the product of the original signal and a random seed-based Gaussian random signal with an adjustable standard deviation σ. The simulations were done for a range from $0.01\,\sigma$ to $0.2\,\sigma$.



(a) Adaptations for unavailable data (b) Adaptations for corrupted control data

Figure 4.4: Model adaptations for simulating unavailable and corrupted data

Note that for all simulations regarding data loss and data corruption, a basic communication delay of 20 ms was assumed. Furthermore, for each simulated data loss rate and standard deviation, a series of 100 simulations with different random seeds was conducted.

Case Study Results

As for the results of the case study's simulations, it is important to point out their case-specific property. It means that all shown results are only valid in the context of the chosen power network, asset configuration, controller design or implementation and simulation parameters. While the shown settling times for given sets of data issues cannot be assumed valid in other system configurations, their abstract correlation can be generalised. Furthermore, note that in all simulations only one ICT error category is introduced at a time.

An interpretation of whether a resulting settling time is sufficient or not depends on the ADN's concrete use case. For demonstration purposes, the ADN is assumed to be used as a means of frequency containment reserve (FCR) which demands a full activation time of no more than 30 s in accordance with [30]. This full activation time can be interpreted as the maximum tolerated settling time in FCR scenarios. Therefore, this threshold is marked by a red horizontal line in the following figures.

The analyses that focused on the impact of static communication latency on the ADN controller's settling time resulted in Fig. 4.5.

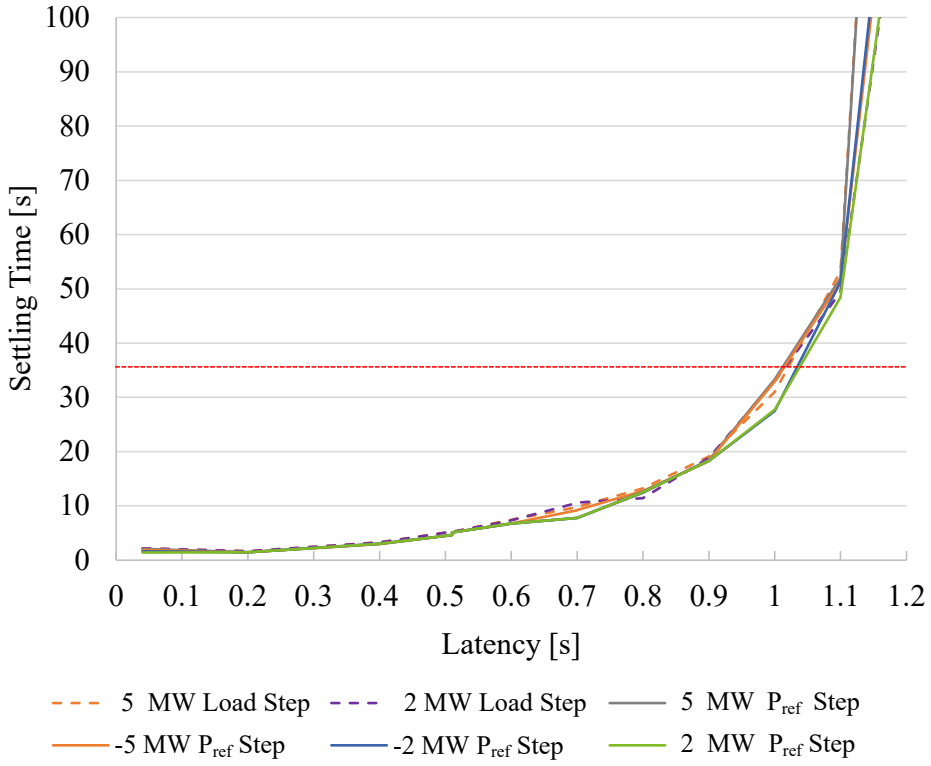


Figure 4.5: Impact of latency on settling times for different steps in load and P_{ref}

It shows a clear, exponential correlation between latency and settling times. This implies diminishing returns for investing in faster ICT on the one hand and clear acceptable latency thresholds for given settling time requirements on the other. In addition, Fig. 4.5 shows that neither size nor direction of the changed setpoint has a relevant impact on the settling times. Two more simulation series were done with active load steps instead of updated setpoints in order to see how well the ADN controller can maintain a previous setpoint in case of an unforeseen disturbance. The corresponding results indicate that the controller handles load steps and setpoint changes equally well. In general terms, the total communication latency, including the transmission of both measurements and control data, should not rise above 1.1 s. With regard to the chosen example services, the required settling time of 30 s can only be achieved while the communication latency stays below 1 s.

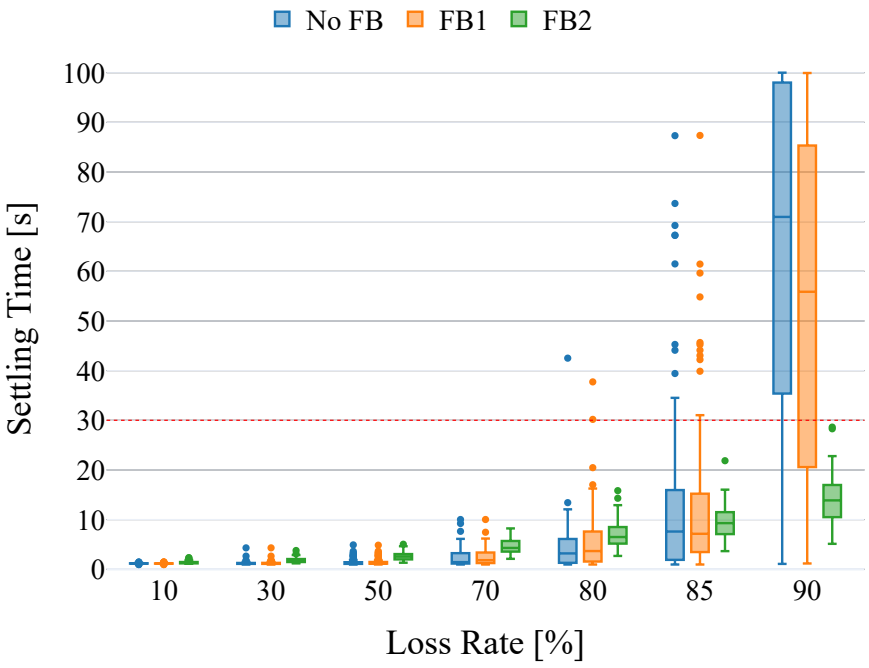


Figure 4.6: Impact of data loss on settling times with no fallback strategy, FB1 and FB2 with 100 random seeds per loss rate

The relevant simulation results regarding data loss and its impact on ADN settling times are summarised in Fig. 4.6 which depicts the settling times for a series of 100 simulations with different random seeds for each simulated loss rate and each applied fallback strategy. The two considered fallback strategies (FB 1 and FB 2) aim at mitigating the impact of increased loss rates. FB 1 does so by holding onto the most recent known measurements and for FB 2 an additional anti-windup feature is

implemented. It can furthermore be seen that, without fallback strategies in place, loss rates over 80 % drastically increase the settling time and beyond 85 % many simulations exceeded the maximum simulation time of 100 s, which implies even worse results than depicted. FB 1 does slightly improve the outcome and FB 2 leads to a drastic decrease in settling times. Considering the chosen example settling time threshold of 30 s, the loss rate may not exceed 70 % without fallback strategies. With FB 2 active, though, even loss rates of up to 90 % result in sufficiently fast ADN responses in all of the 100 simulations. For all these results, the fact that in this simulation setup data is being retransmitted very often must be considered, though. If data was retransmitted less frequently, data loss is expected to have a more severe impact on the settling times already at lower loss rates. While the results render this specific controller design to be very robust against even high levels of data loss in general, it also proves the general correlation between data loss and ADN settling times. From the available results, an exponential correlation can be assumed, again.

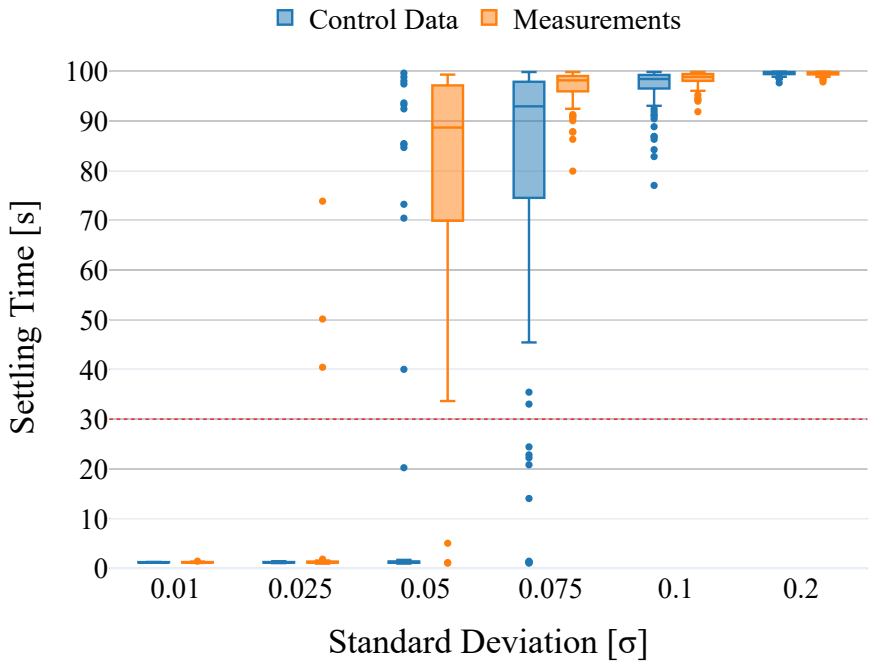


Figure 4.7: Impact of corrupted measurements and control data on settling times with 100 random seeds per σ

Finally, Fig. 4.7 outlines the corruption-based simulation results. In summary, it provides two important insights: First, the initially assumed correlation between corrupted data and ADN settling times is proven and seems to behave exponentially, too. And second, the ADN controller is more sensitive to corrupted measurement

data, for which settling times grow fast for $\sigma > 0.025$, than corrupted control data, for which settling times only start to increase significantly for $\sigma > 0.05$.

Thus, the sensitivity of the ADN controller to all three ICT error categories is known. Note that each ICT error category has only been analysed isolated from the other two. This implies that a combination of simultaneous ICT errors of different categories is not covered by the demonstrated study and might cause further extended settling times.

The results of this case study clearly show that a degraded ICT system can cause services in power systems to deteriorate to a point at which they can no longer fulfil their designated purpose. In this example, different types and degrees of ICT errors cause the ADN controller's settling time to exceed the regulatory requirements for an acceptable FCR service performance. Hence, the potentially critical role of ICT peformance in the context of CPES stability and grid services is proven.

The chosen ADN-based approach can be interpreted as a basis for a wide range of future grid services and a realistic aggregation scenario for DERs. Still, the simulation results are only valid for the specific controller and the corresponding parameters. A similar controller with different parameters is very likely to result in different settling times, too.

Regarding the choice of power system and its model it must be stated that the case study results will have little general validity. A different power system will lead to different results. Yet, a short analysis based on an LTI system and root locus was done in [MK3], too. This analysis yielded similar results for the impact of data latency on settling times despite completely neglecting the grid topology and only focusing on the control loop's behaviour and DER dynamics. While far from proving any general validity of the results in this chapter, said similarity of results still implies a limited meaningfulness for other power system topologies with similar DER configuration.

4.2 States of Cyber-Physical Services

The knowledge gained from in-depth service analyses such as demonstrated in Chapter 4.1.1 can be leveraged to map data availability, timeliness and correctness onto a service's expected performance on a more abstract level. To keep this mapping as generally applicable as possible, a set of service states as shown in Fig. 4.8 can be defined based on the collaborative work presented in [MK1][3] and partially inspired by [22]. Two of these states are intuitive, namely the **normal state** and the **failed state**. In its normal state, a service is defined to operate ideally or as intended, while a service in the failed state cannot be considered an appropriate remedial action any longer as it is expected not to respond or function with sufficient speed or precision. In addition to these two states, a service can potentially also be affected by impaired data to the point of partial degradation. Hence, the so-called **limited state** is meant to represent all situations in which a service

- responds slower than intended,
- with decreased accuracy,
- within a limited range of operation or
- is making decisions based on insufficient information.

As for the expected performance of a service, it can be said that a service in its normal state is guaranteed to realise a command as intended while a service in its failed state is most likely not to react as desired. A service in the limited state cannot be guaranteed to do either but is defined to be at least more likely to respond adequately than not. This is why the outcome of a limited service's activation is subject to a non-deterministic process.

The conditions that would trigger a state transition between 'normal, limited' and 'failed' need to be identified for each service individually and under consideration of its specific implementation and the power grid it is supposed to interact with. In most cases and for most services, these triggering conditions must be identified with simulations first as data on the service's exact data requirements is not available. In some cases, though, a service's dependence on data is already known to some degree. For each case, the simulation-based service state definition and the logically derived state definition based on existing knowledge, one example is provided next.

[3] M. Klaes' contribution to this work lies in the dissemination of the ETNSO-E state classification and the identification of potential connections points between it and general ICT performance. He also assisted in creating and describing the case studies.

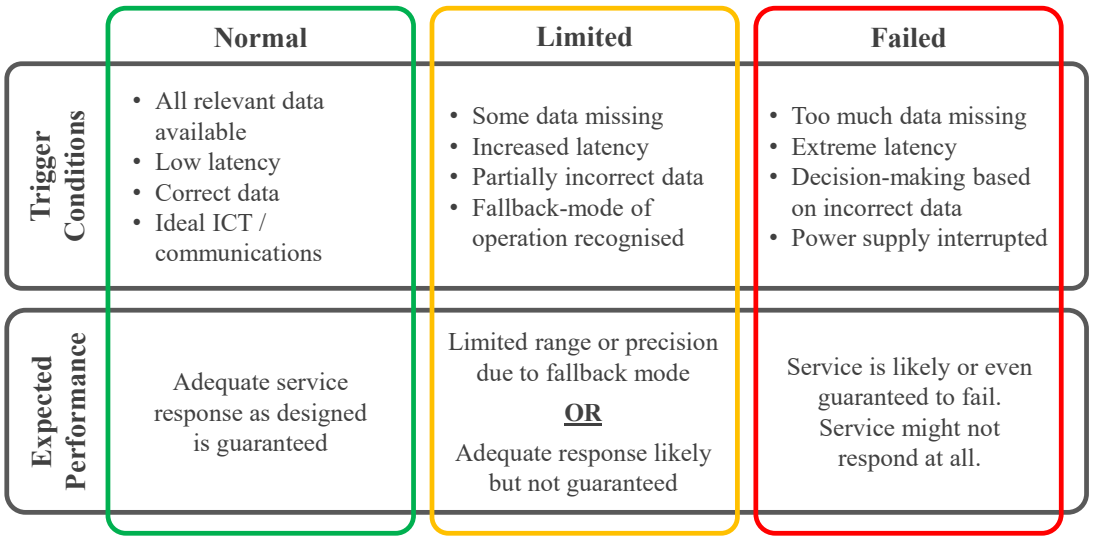


Figure 4.8: Abstract service state description summary

4.2.1 Example 1: ADN-Based Service States

The first example is based on the previously published collaborative work [MK4]. It is a continuation of the ADN case study from Chapter 4.1.1 since the previous simulation results regarding the ADN controller's sensitivity towards impaired data are mapped onto a service-specific state description. For this, the previous ADN use case as an FCR provider with an acceptable settling time limit of no more than 30 s is chosen once again. The resulting service state definition, including those conditions that lead to settling times beyond 30 s and would thus trigger state transitions, can be taken from Fig. 4.9. For each ICT error category, the figure shows those operational ranges that would guarantee a sufficiently fast response of the ADN controller with regard to the 30 s settling time target. It also shows the ranges for which merely the median of all simulated settling times is sufficiently fast, which defines the limited state in this example, and a third set of ranges that most probably result in an unsatisfying response speed. The latter matches the definition of services' failed state. For example, the ADN controller's settling time can be guaranteed to stay below 30 s for data loss rates up to 70 % because none of the 100 simulations with these loss rates resulted in a longer settling time according to Fig.4.6. For loss rates between 70 % and 85 %, the vast majority of simulations resulted in sufficiently fast settling times, still. The resulting service state would be 'limited' as the intended response is still expected but cannot be guaranteed any longer. For data loss rates beyond 85 %, the median of the controller's settling time rises above the 30 s threshold in simulations with either no fallback strategy of FB 1. Hence, the service is considered

unlikely to respond as intended and is therefore in its 'failed' state. It is important to point out again that the shown sensitivities towards ICT errors and their impact on ADN settling times is only to be considered individually. Thus, a combination of adverse ICT performance scenarios e.g. increased delay and increased data loss rates, might result in a degraded service state, even though their individual assessments would define the service to stay in its normal state.

	Normal	Limited	Failed
Delayed Data	$T_{total} \leq 0.9s$	$0.9s < T_{total} \leq 1.0s$	$T_{total} > 1.0s$
Data Loss (No FB)	Loss Rate ≤ 70%	70% < Loss Rate ≤ 85%	Loss Rate > 85%
Measurement Corruption	$\sigma_{meas} \leq 0.01$	$0.01 < \sigma_{meas} \leq 0.025$	$\sigma_{meas} > 0.025$
Control Data Corruption	$\sigma_{ctrl} \leq 0.025$	$0.025 < \sigma_{ctrl} \leq 0.05$	$\sigma_{ctrl} > 0.05$

Figure 4.9: ADN service states as presented in [MK4]

Regarding the sensitivity of the ADN controller towards data loss, it should be mentioned that with fallback strategy FB 2 in place, all simulated loss rates would still result in acceptable settling times. This means that, with FB 2 active, data loss rates up to the highest simulated level of 90 % would no longer trigger any service state degradation. The results underline that the knowledge about a service's sensitivity to non-ideal data can be crucial in the planning phase of a CPES. Only then, adequate fallback strategies can directly be implemented.

4.2.2 Example 2: State Estimation Service States

The second example focuses on the SE as a critical service. Its data- and ICT-dependence have already been established and researched in the past and approximate data on the SE's requirements is available in the literature, for example in [61] or [62]. In [MK5][4], Hassan et al. present a model to assess the performance of the SE service in terms of service states as defined in [MK1] with regard to the completeness, timeliness and correctness of data. Fig. 4.10 depicts the resulting service states of said work,

[4]M. Klaes' contribution to this work lies in checking the resulting state definition and reviewing.

which will only be summarised here. Full details about this model as well as a proof of concept can be found in [MK5].

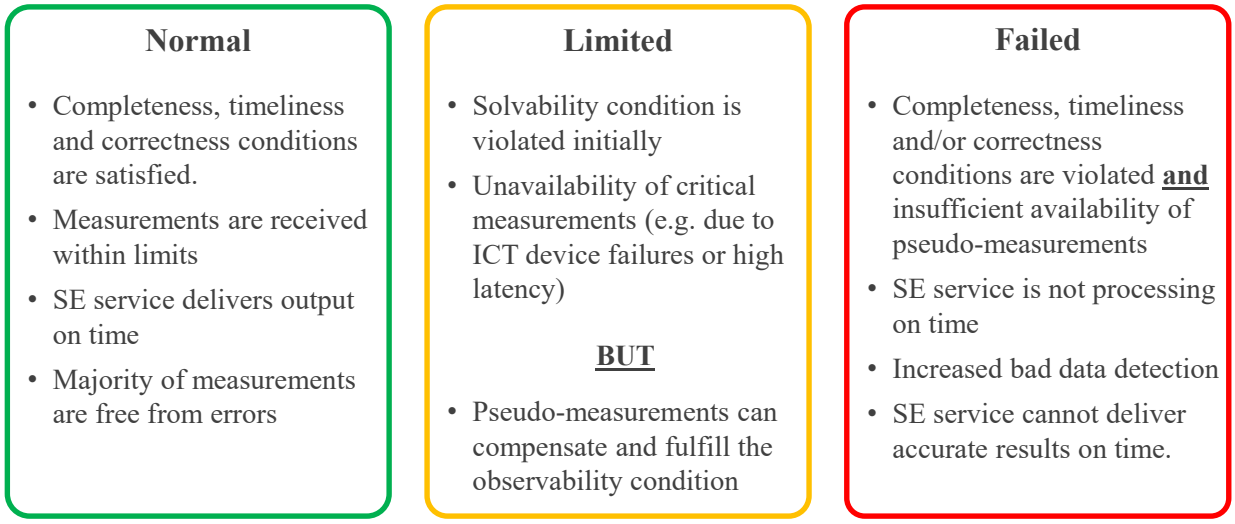


Figure 4.10: SE service states (based on [MK5])

The SE takes in measurements and calculates a consistent state of the corresponding power system. In general, the accuracy of the SE result improves with an increasing number of measurements available to the SE. Thus, it is ideally provided with measurement data from all buses. The minimum number of available measurements is expressed by the solvability criterion. It dictates that, at the very least, typical SE algorithms require twice as many measurements as there are buses in the system, minus the number of reference or slack buses. Furthermore, in real power systems, the measurements at some buses are critical and their unavailability directly leads to local unobservability. For both these problems, too few measurements available to satisfy the solvability criterion, and missing critical measurements, the utilisation of so-called pseudo-measurements is a common fallback strategy. They are supposed to replace the actual measurements if needed and are, for example, derived from historical data, former simulations or other predictive models. While these pseudo-measurements can bring back the SE's solvability in times of low measurement availability, the precision of the results can be drastically decreased.

Similar to the previous ADN-based example, the conditions that trigger an SE state transition comprise ICT-based conditions that would provide highly reliable SE results in the normal state, less reliable yet typically sufficiently precise SE results in its limited state and no results in the failed state.

4.3 Multiple Service States and the ENTSO-E System States

So far only singular services have been considered with regard to their ICT dependence and their resulting service states in an isolated manner. Next, an approach is presented that puts multiple services with potentially different core tasks in context with each other and assesses their interdependence. As explained in Chapter 2.3, the ENTSO-E system state classification is a commonly used and acknowledged framework for connecting various aspects of conventional power systems and summarising the general threat level of the power system on an abstract level. Bringing together this established ENTSO-E state classification and the newly defined service states allows for improved consideration of ICT-induced risks to the stable operation of CPESs. The following explanation of how to bridge between ENTSO-E states and service states is based on work presented in [MK1].

In order to integrate the service states into the ENTSO-E states, two service-related elements of the ENTSO-E state classification have been identified first. On the one hand, there are the so-called 'critical tools & facilities', which aid in gathering measurements as well as performing the SE or further operational security analyses like the contingency analysis (CA). A sustained loss of such a critical tool or facility for an extended period time of over 30 minutes is already defined as an emergency state-triggering condition in the ENTSO-E state classification. Yet, this definition does neither consider partial performance degradation nor does the chosen 30-minute threshold appear appropriate under consideration of the increased volatility and flexibility of modern and future power system operation.

On the other hand, the RAs, which are a crucial aspect of the CA, are expected to become increasingly ICT-reliant in future. As described in Chapter 2.3, the CA simulates the activation of all viable RAs for each potential contingency under consideration of the most recent SE results. For these simulations, it is generally assumed that each RA is either applicable in the current situation or not, but the concept of an available yet degraded RA is neglected. This situational applicability can, for example, be based on the currently available operational flexibility of DERs. For each contingency that can only be averted by an ICT-reliant RA, the current state of the service that provides the RA must be regarded, as well. Otherwise, a control decision that would be considered sufficient from a power system perspective could potentially turn out to be unavailable if the ICT system's state and its impact on the service's

performance are ignored. Additionally, depending on its specific implementation, an RA may also directly depend on certain critical facilities or tools, for example, a controller with an SE-based decision-making process. Disturbances in the ICT system directly affecting RAs – not only on their availability but also on their performance – are yet to be considered in the conventional ENTSO-E state classification.

4.3.1 Example: State Estimation and Tap Changer

The following example is a summary of the case studies presented in [MK1] and concerns a small CPES with a focus on a distribution system that also provides measurements to a centralised monitoring and control system similar to the one presented in [63] or to the decentralised system presented in [64]. In theory, this system could also be part of the DSO's control room. The monitoring and control system calculates and transmits SE results to the controller of an on-load tap changer (OLTC) which then changes the transformer's tap position as a means of voltage control. Thus, the example utilises two services at the same time, with one partially depending on the other. The complete setup including the distribution system, the monitoring and control system, and the OLTC and its controller is depicted in Fig. 4.11.

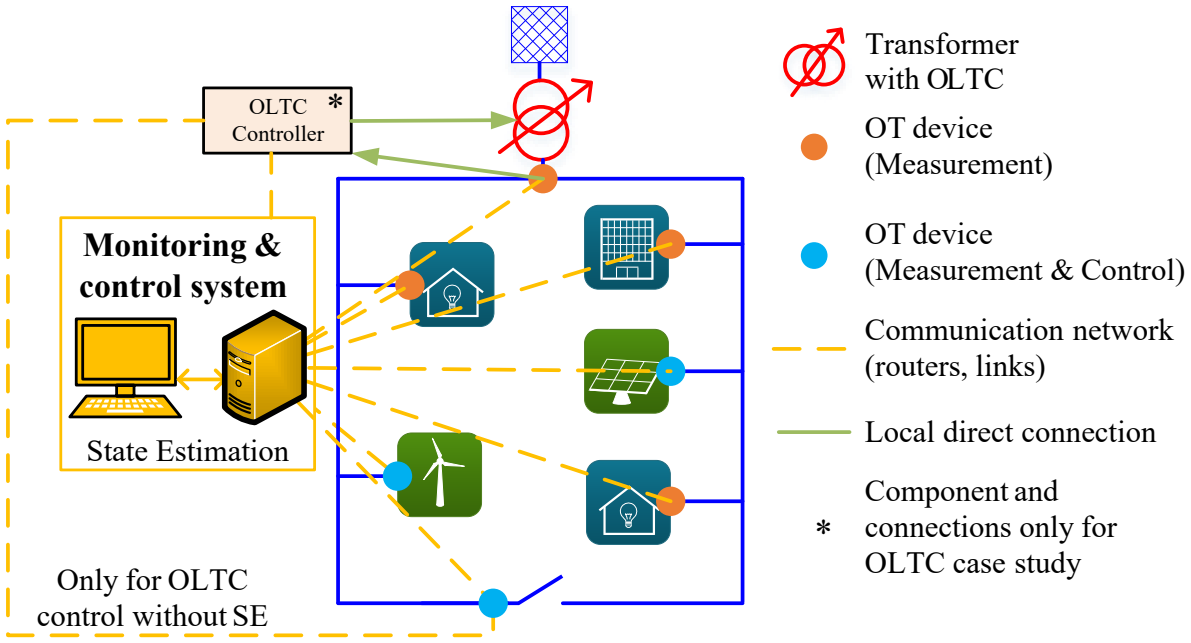


Figure 4.11: CPES with SE and OLTC services

The service states of the SE service have already been introduced in Chapter 4.2.2 and summarised by Fig. 4.10. Just like these SE service states are focused on the availability of data and the current activation of any fallback strategies (such as the utilisation of pseudo-measurements), another set of service states needs to be defined for the OLTC control service, which provides the exemplary system operator with an RA. The OLTC controller is designed to take in SE results, check for any buses showing voltage violations, and correct them, if necessary and possible, by changing the OLTC's tap position. The SE-based decision-making of this controller design is capable to mitigate or at least consider voltage violations at any bus. More conventional OLTC controller designs only considered a single measurement at the OLTC-bus, or, in some suggested cases, very few additional measurements at the end of feeders or other locations with critical voltage levels [65]. While this might have been sufficient in conventional, radial power grids with monotonically decreasing voltage levels over the feeders' length, both of these conventional controller designs are not fit for use in grids with DERs. A decision based only on a single bus voltage runs the risk of increasing a feeder's general voltage level without seeing that the voltage is already critically high at a different bus with a DER. Thus, the SE-based OLTC controller provides an improved decision-making process at the cost of increased dependence on communication with the monitoring and control system. In case of this communication being disturbed, which renders SE results unavailable, a fallback strategy is meant to be activated. This fallback simply switches the OLTC controller from the more sophisticated SE-based operation to the described conventional operation mode. The full definition of OLTC service states can be found in Fig. 4.12.

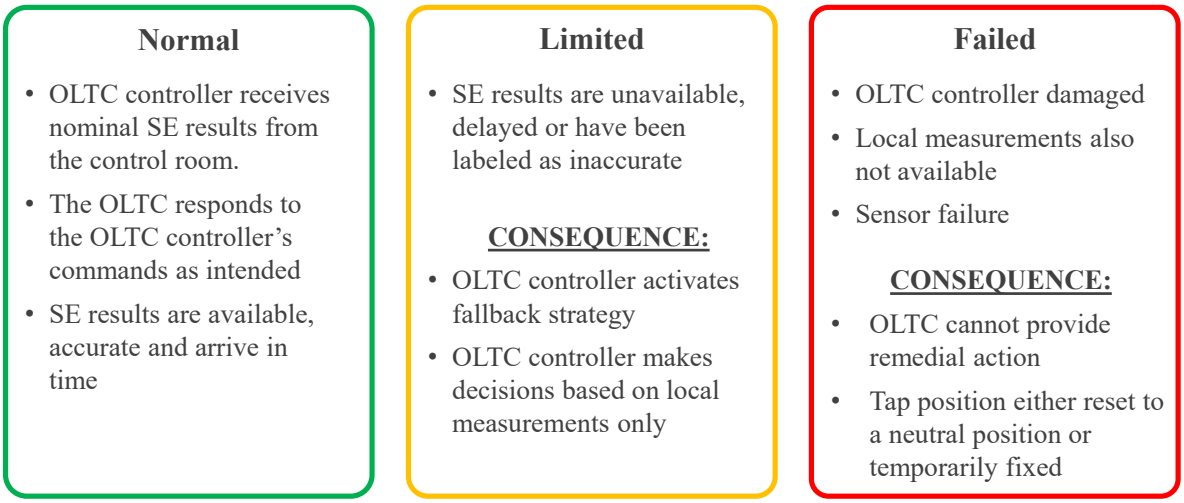


Figure 4.12: OLTC service states based on [MK1]

With the OLTC service states defined, an exemplary analysis of CPES interdependencies with regard to both ENTSO-E system states and the newly introduced service states as well as their transitions can be derived. Accordingly, Fig. 4.13 summarises a set of cascading state trajectories for the exemplary setup and the black arrows in that figure denote direct, deterministic state transitions. For instance, in case of a failed OLTC control service, the only available RA of this system becomes unavailable. This leads to the CA finding typical contingency scenarios for which there are no solutions available. According to the ENTSO-E state classification, the power system is defined to drop to the alert state under these circumstances.

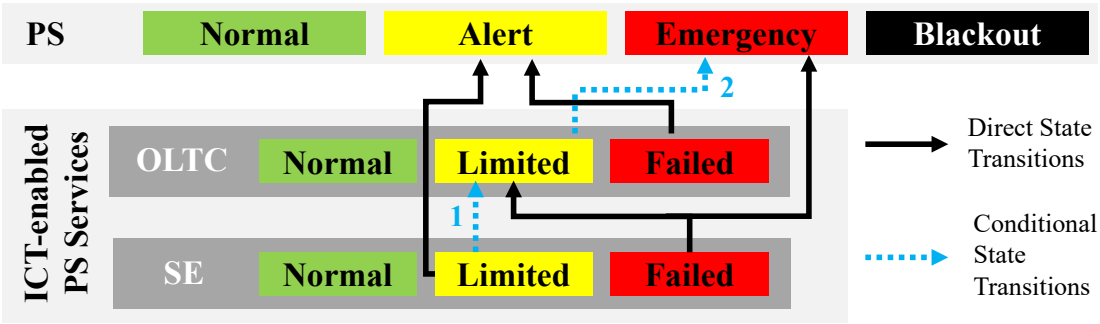


Figure 4.13: CPES state transitions with interdependent SE and OLTC services

The blue arrows represent examples of conditional state transitions that should be added to the ENTSO-E state classification in order to obtain a state description for the CPES as a whole. They indicate non-deterministic transitions. Two such exemplary conditional state transitions are shown in Fig. 4.13, as well. In the case of the first conditional state transition, the consequence of the SE being in its limited state is that voltage estimates with decreased accuracy are sent to the OLTC controller. Even though the limited state of SE does not affect the state of the PS, it can cause the OLTC service to drop to its limited state. The OLTC can then either use these insufficiently accurate SE results or rely on the local measurement only. This is important as it might lead to cascading failures as demonstrated by the second conditional state transition case. Here, the OLTC controller receives insufficiently accurate SE results or local measurements only, leading to an incorrect tap position. Since the OLTC controller is the only available RA in this case study, a faulty tap change can therefore lead to a voltage violation in case of a contingency. In accordance with the ENTSO-E state classification, the PS would drop to the emergency state as a consequence. This state transition demonstrates the possible impact of an RA operating incorrectly due to another service being in its limited state.

The results of this example are based purely on logical conclusions. A more substantial, simulation-based analysis for a very similar system setup is provided in Chapter 5.3.1 once this work's core method has been introduced and explained.

This Chapter's Core Insights

- Cyber-physical services drive interdependence in CPES by being both, crucially important for the power system's stability and reliant on the successful exchange of information.
- Services typically comprise multiple communication processes, each of which is prone to experience ICT errors such as delays, data loss and data corruption.
- In order to fully understand the ICT dependence of a service, each of its communication processes needs to be assessed regarding its sensitivity towards each ICT error category.
- The insights from these service assessments and their resulting ICT requirements can be summarised with the help of service states. These service states map currently measured ICT performance onto the expected service behaviour.
- The service state can be 'normal', 'limited' or 'failed':
  - 'Normal' indicates a state in which nominal service behaviour can be guaranteed.
  - 'Limited' indicates a likely successful response of the service.
  - 'Failed' indicates a likely unsuccessful response of the service.

5 Assessment of Static Stability

Details about domain-interdependencies in CPES as well as CPES and service states have been explained in the previous chapters. The following chapter aims at modelling a CPES with a strong focus on its interdependencies as well as deriving and analysing the extended CPES state trajectory as a result of propagating disturbances. For this, a method partially inspired by [66] was created and presented in the collaborative works [MK6][5] and [MK7][6]. The resulting method can be broken down into 3 steps: First, the impact of a disturbance needs to be assessed under consideration of the three implications for CPES operations which represent the abstract interdependencies within a CPES (see Chapter 3.3). Additionally, the trajectories of the CPES state and all service states in accordance with Chapter 4.3 and Chapter 4.2, respectively, need to be derived. Finally, these state trajectories allow for qualitative comparisons of different system designs' performances with regard to their robustness and reliability towards remedying contingencies.

5.1 Calculating Disturbance Propagation

The developed method for assessing the propagation of disturbances in a CPES under consideration of its interdependencies comprises eleven phases. An overview of these phases is provided in Fig. 5.1, along with each phase's main objective in the power system and ICT domain. The arrows between the domains indicate that a phase's result from one domain is either a direct input for the next phase in the other domain or in other ways relevant for it. Hence, these arrows also represent concrete examples of the domain-interdependence in a CPES. The details of each phase as well as the special meaning of the phases coloured yellow are explained and discussed in the following subchapters.

Two important properties of this method are its adaptability and modularity. While each of the eleven abstract phases is essential for the assessment of a CPES' stability, the explicit implementation can be adapted. For example, Phases 1 - 3 and Phase 10

[5]The authors A. Narayan and M. Klaes both implemented the simulations and case studies together. M. Klaes' focus was on implementing the OLTC controller and the contingency analysis.

[6]The first four authors contributed equally to this work from conceptualisation to writing the paper. M. Klaes focused on designing and implementing the differences between global and perceived views.

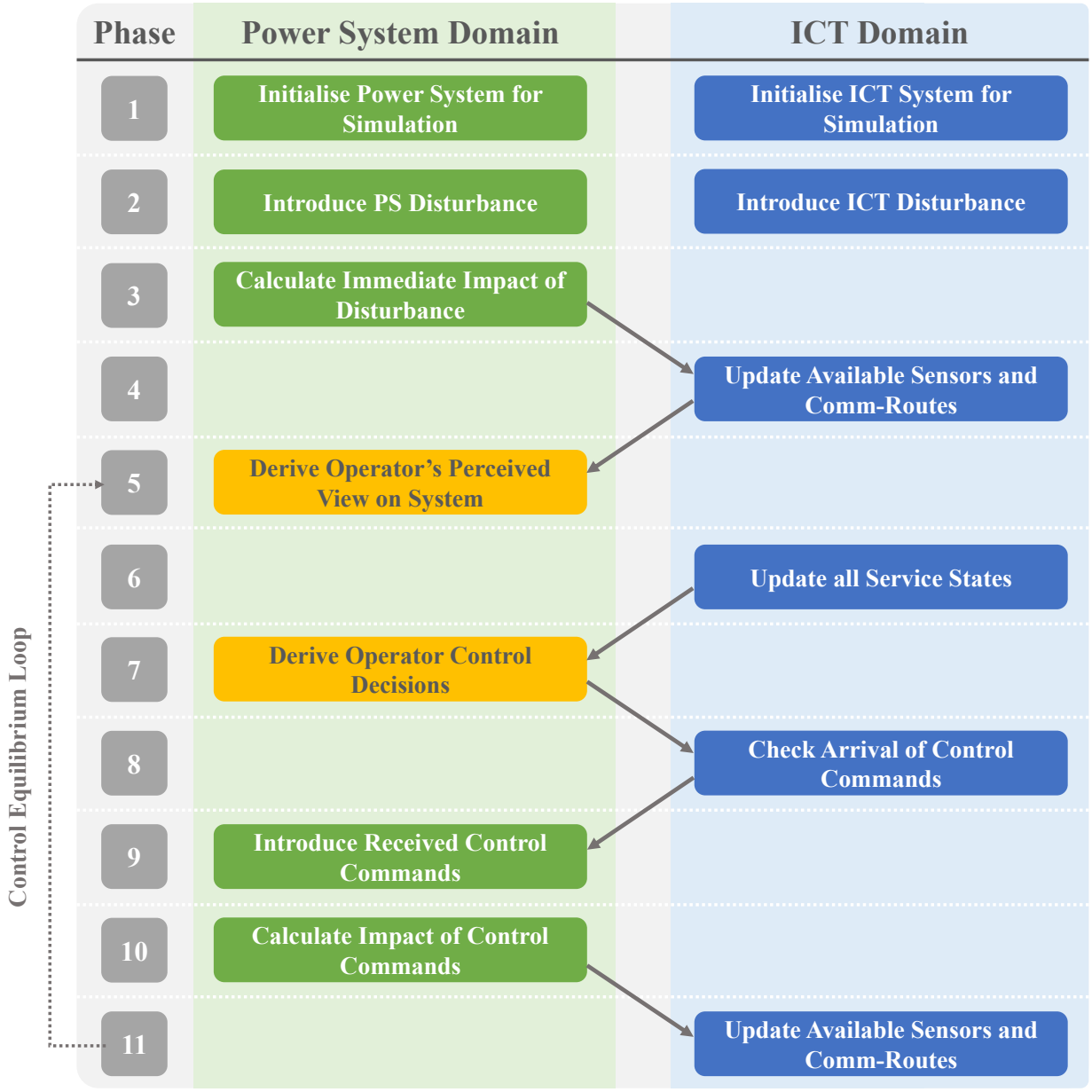


Figure 5.1: 11 phases for assessing CPES disturbance propagation

can be implemented focused on either static or dynamic power system simulations. Dynamic simulations would allow for the study of dynamic stability phenomena, which is discussed later in Chapter 7. Another example of the method's adaptability concerns the operator's decision-making process. Here, a variety of approaches to derive an operator's decision can be applied, such as a simplistic decision-trees, an optimisation or an agent-based approach that would allow for considering distributed coordination processes. This is why the following details about implementing the eleven phases should be considered as examples, only.

Phase 1: Initialise System

Phase 1 is about the initialisation of both the power system and the ICT system. Regarding the power system side, this concerns information on the buses, lines, and grid topology. To be more specific, the aggregated active and reactive power P_{Bus} and Q_{Bus} needs to be known for each bus that either provides power to the grid (PV-bus) or draws power from it (PQ-bus). The same goes for the complete admittance matrix $\boldsymbol{Y}$ with

$$\boldsymbol{Y} = \begin{bmatrix} Y_{11} & -Y_{12} & \dots & -Y_{1j} \\ -Y_{21} & Y_{22} & \dots & -Y_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ -Y_{i1} & -Y_{i2} & \dots & Y_{ij} \end{bmatrix} \tag{5.1}$$

where each diagonal element $Y_{ij} \,|\, i = j$ describes the sum of all admittances connected to the bus i while all remaining elements describe the negative admittance between the two buses i and j. Finally, for generation-buses, P_{Bus} and bus voltages V_{Bus} need to be known upfront, too. Fig. 5.2 shows an example of a fully initialised power system topology and $\boldsymbol{Y}$.

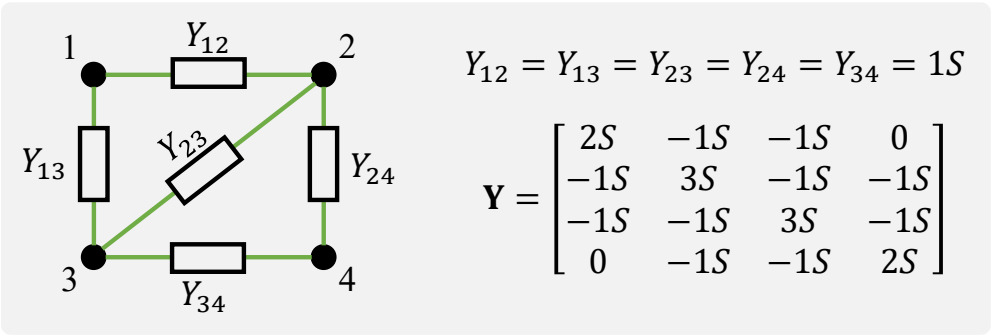


Figure 5.2: Example of an initialised power system topology

The fully initialised power system furthermore requires all bus voltages V_{Bus} and line loadings $L_{\text{Line},ij}$ to be known, too, which can optionally be obtained via power flow calculations once P_{Bus}, Q_{Bus}, and $\boldsymbol{Y}$ are defined.

The ICT network can be represented by an undirected graph that comprises vertices V_i and edges E_{ij} where each V_i corresponds to an ICT node and each E_{ij} represents a direct communication line between two nodes. The fully initialised system requires knowledge about each node's details, e.g. the node type (actuator, server, router)

on the one hand, but also information on the count of measurements and pseudo-measurements connected with each node. Furthermore, information about a node's associated measurements as well as acceptable threshold values for correctness and latency need to be known upfront. All this information can be formally described by a node property matrix $\mathbf{\Pi}$ as shown in [MK7], yet this formal description will not be used in detail in this work for the sake of readability.

Analogous to the admittance matrix for the power system, the so-called distance matrix $\mathbf{\Delta}$ (see Equation 5.2) needs to be known for ICT system initialisation, as well. It is a symmetrical matrix that contains information about the end-to-end delay δ_{ij} of the shortest path between the two nodes i and j in a system with N nodes.

$$\mathbf{\Delta} = \begin{bmatrix} \delta_{11} = 0 & \delta_{12} & \dots & \delta_{1N} \\ \delta_{21} & \delta_{22} = 0 & \dots & \delta_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \delta_{N1} & \delta_{N2} & \dots & \delta_{NN} = 0 \end{bmatrix} \tag{5.2}$$

where a distance of 0 implies that the communication is local while an infinite distance implies that there is no path available between the respective nodes. An example of an initialised undisturbed ICT system topology and $\mathbf{\Delta}$ can be seen in Fig. 5.3. Note that in this example the ICT topology was simply assumed to be identical to the power system topology and the shortest path and thus the delay between Nodes 2 and 3 (δ_{23}) does not result from the direct connection as communication via Node 4 has a shorter delay.

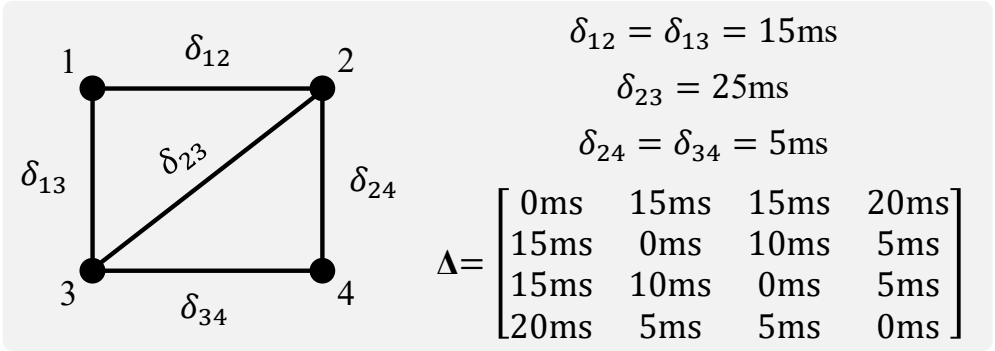


Figure 5.3: Initialised ICT system topology

Phase 2: Inject Disturbance

After the CPES has been fully initialised, an external disturbance and its resulting CPES fault can be introduced into the system. The presented method is capable of considering any CPES fault that can be modelled as a change in P_{Bus}, Q_{Bus}, $\boldsymbol{Y}$, $\boldsymbol{\Pi}$ or $\boldsymbol{\Delta}$. As this implies a layer of abstraction, the explicit type of the underlying original external disturbance is mostly irrelevant. Only the abstract CPES fault is relevant as it determines the affected simulation parameters that will need to be adapted in accordance with the fault. This process of abstracting external problems to electrical faults and mapping their impact onto these system configuration changes is summarised in Fig. 5.4.

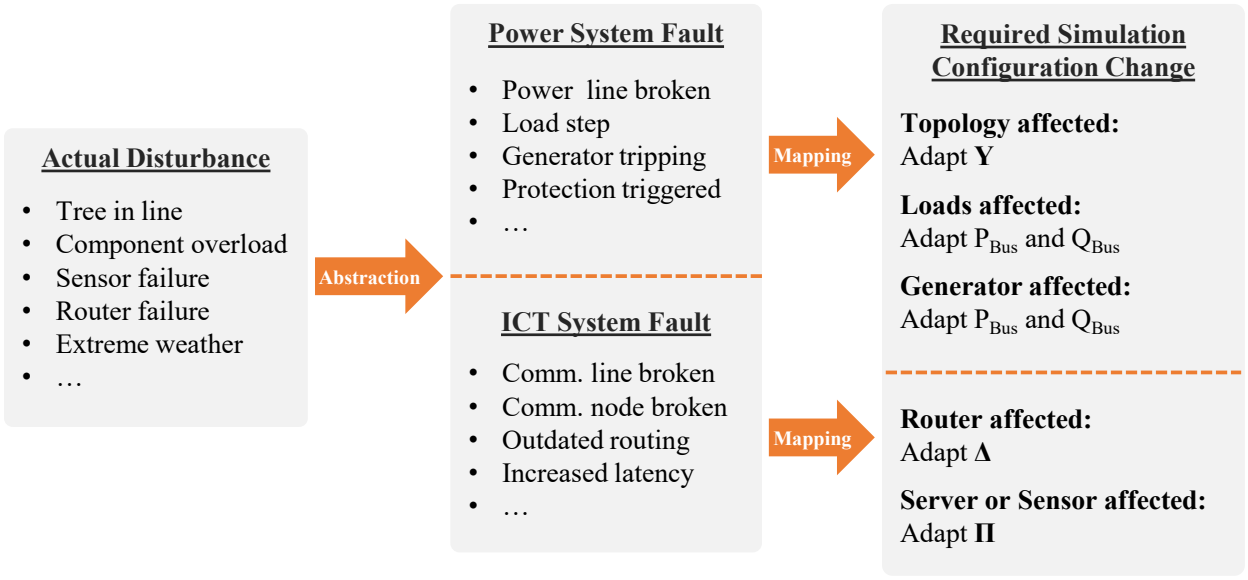


Figure 5.4: Translating real-world disturbances to abstract simulation changes

Note that this phase only concerns the immediate, local, predictable and thus trivial effects of a disturbance and does not cover the resulting consequences, nor does it require any predictions about CPES interdependencies. Thus, for example, a tree falling into a power line only leads to a change of $\boldsymbol{Y}$ regarding the very line that was hit while further implications such as unsupplied ICT equipment, overloaded parallel lines or power imbalances are to be determined in the subsequent phases. The changed simulation configuration for an exemplary disturbance, namely 'tree in the Line 3-4', are highlighted in Fig. 5.5.

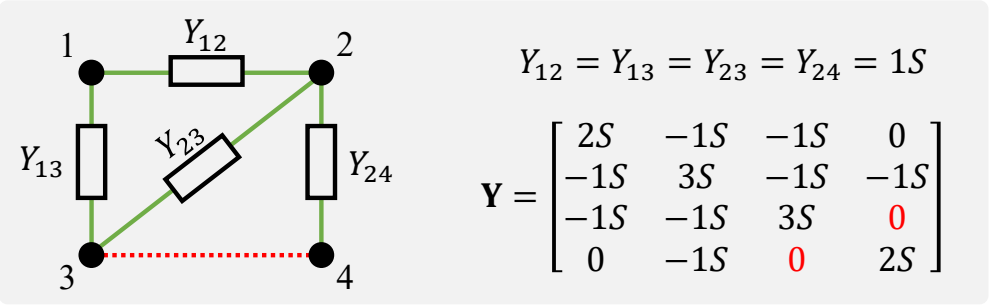


Figure 5.5: Changed simulation configuration after a tree crashing into Line 3-4

Phase 3: Simulate Intrinsic Response to Disturbance

Once the external disturbance has been translated into a change in the system configuration, the direct and – predefined protection mechanisms and schemes aside – the uncontrolled initial response of the power system has to be simulated. The goal of this phase is to identify any non-trivial consequences of the injected disturbance. This step corresponds to the power system level explained in Chapter 3.2. If the initial disturbance is an ICT disturbance, Phase 3 can be skipped since all ICT-reliant services can be assumed to be designed so that their mere unavailability would not directly cause any problems for the CPES without an additional disturbance in the power system.

The suggested tool for this phase is another iteration of power flow calculations based on the system configuration after its adaption to the effects of the disturbance. The continued example shown in Fig. 5.6 illustrates a potential result of such a power flow calculation, indicating Line 2-4 being overloaded after Line 3-4 dropped. As a consequence of either automatically triggered protection schemes or mechanical failure due to extreme overload, Line 2-4 is assumed to be disabled or failed, too.

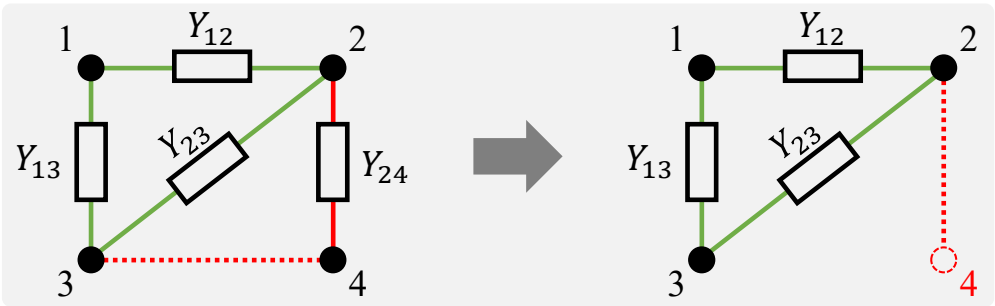


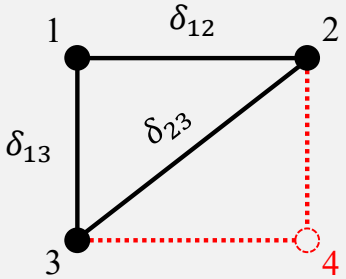
Figure 5.6: Line 2-4 dropping due to overload in accordance with power flow results

Phase 4: Update ICT Topology

As an initial disturbance in the power system domain might cascade to the ICT domain, Phase 4 is about checking the power supply to all buses with ICT components assigned to them and then, if necessary, updating $\mathbf{\Pi}$ or $\mathbf{\Delta}$ accordingly. Thus, this phase concerns the 'potentially impaired power supply for ICT components', one of the three main implications of CPES operations introduced previously in Chapter 3.3. This phase also maps initial ICT disturbances to changes in the ICT system even though no severe consequences for the CPES are to be expected from an ICT disturbance alone. Still, for scenarios with several sequential disturbances, the method must be able to capture a purely ICT-based disturbance followed by a different disturbance in the power system.

For updating $\mathbf{\Pi}$, the most simple approach is to change the availability of measurements connected to nodes that experience power outages to zero while the number of available pseudo-measurements stays unchanged. Updating $\mathbf{\Delta}$ on the other side requires updating the ICT network graph so that it reflects the potential loss of nodes by removing the corresponding E. It will furthermore require an updated calculation of the shortest paths between all nodes and thus updated δ_{ij}.

Phase 4 concludes the first stage by determining the state of both power and ICT systems immediately after an external disturbance but before any actively coordinated RA has been applied. Fig. 5.7 demonstrates fictional results of this phase in the context of the previous tree-in-line example. Not only does it show Node 4 not being available any longer due to the corresponding Bus 4 not being supplied with power, but also has δ_{23} increased from $10ms$ to $25ms$ since the shorter route via Node 4 became unavailable.



$$\delta_{12} = \delta_{13} = 15\text{ms}$$
$$\delta_{23} = 25\text{ms}$$
$$\delta_{24} = \delta_{34} = \infty$$
$$\mathbf{\Delta} = \begin{bmatrix} 0\text{ms} & 15\text{ms} & 15\text{ms} & 20\text{ms} \\ 15\text{ms} & 0\text{ms} & 25\text{ms} & \infty \\ 15\text{ms} & 25\text{ms} & 0\text{ms} & \infty \\ 20\text{ms} & \infty & \infty & \infty \end{bmatrix}$$

Figure 5.7: Affected ICT system with dropped Node 4 and increased δ_{23}

Phase 5: Derive Perceived System View

Next, the system operator's understanding of the current state of his CPES and thus his basis for decision-making needs to be derived. It is of utmost importance to understand that this phase implies a shift in perspective. Phases 5 to 7, which are highlighted in yellow in Fig. 5.1, are based not on the actual physical CPES, but on the operator's perceived view of it. While this perceived system can be identical to the real system under ideal circumstances, chances are that there will be differences to varying degrees. Primarily, any degradation in the performance of the SE will inevitably lead to the perceived view deviating from its physical counterpart. If the perceived view is too different from the physical system, or sufficiently different in a particularly unfortunate time or region, operator decisions that are based on his perceived view might not remedy or even exacerbate contingencies. Phase 5 covers one crucial dependency of power system operation on ICT performance, namely the 'potentially impaired decision making' aspect, the second high-level implication of CPES operations addressed in Chapter 3.3.

A straightforward approach for deriving this operator's perceived system view is to run the SE under consideration of potentially unavailable measurements as a consequence of an altered ICT topology. Only those measurements that are taken by power-supplied sensors and transmitted to the control room via the communication network nodes after the initial disturbance can be used as input for this SE iteration. Pseudo-Measurements, if available for the missing sensors, may be utilised, though.

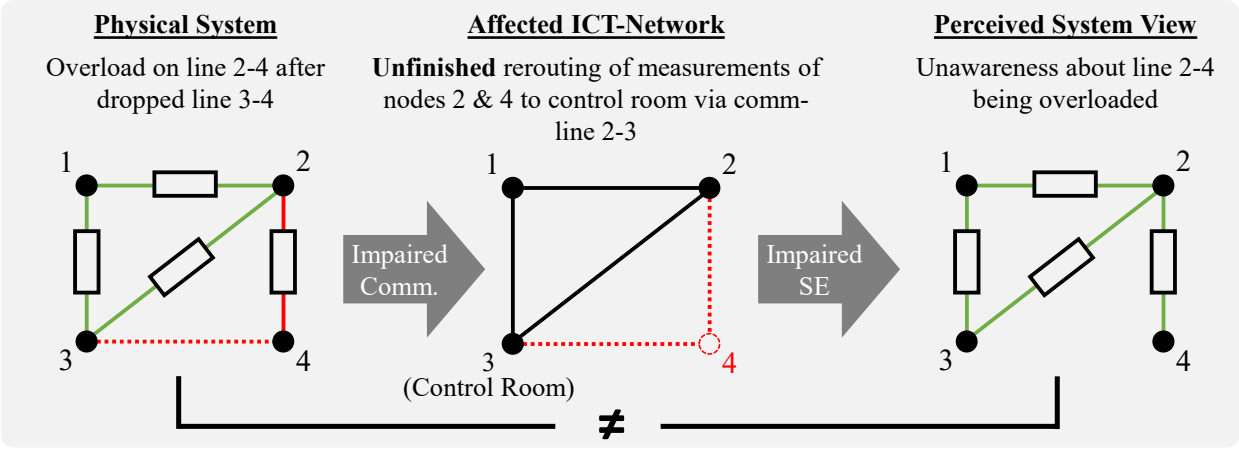


Figure 5.8: Example of a diverging perceived system view caused by delayed SE input data

Fig. 5.8 illustrates this phase with help of the continued, simple example. It assumes that the rerouting process for delivering measurement data from sensors at Nodes 2 and 4 to the control room, which is located at Node 3, is not finished yet. Thus, these measurements are not available to this SE iteration, resulting in locally inaccurate results. Since the likelihood of this specific chain of events is very low in reality, the example only serves an explanatory purpose. Significantly more detailed and realistic examples of how degraded ICT performance affects SE results and further examples on how degraded SE results lead to impaired decision-making have been provided in Chapter 4.2.2 (based on [MK5]) and Chapter 4.3.1 (based on [MK1]), respectively.

Phase 6: Update Service States

The service states need to be assessed and updated next, as it can and should be assumed that the operator knows the current state of each connected service and that these states affect the control decisions. Hence, in Phase 6, the service states as previously defined in Chapter 4.2, are calculated. This is done by comparing the currently experienced data availability, latency and corruption and comparing them with the service state thresholds. This could, for example, imply comparing the current latency between the control room and an RA's controller node as the actuator, which is with the δ_{cr-ra} in $\mathbf{\Delta}$, with the RA's acceptable latency thresholds that would be part of the initially mentioned node property matrix $\mathbf{\Pi}$. The check for unavailability of data is a mere check on whether δ_{cr-ra} is infinite or not and whether the service itself is operating. With regard to data corruption, a simple check at this stage could be realised by introducing a corruption matrix which, similar to $\mathbf{\Delta}$, depicts the aggregated noise on the full communication between two nodes. A simpler way would be to have each service estimate the correctness of its currently used measurements and compare that estimate with the known thresholds that lead to service state transitions. This way, a service-specific implementation for situational awareness and bad data detection can be considered. Of course, such precautionary means can be expensive and their criticality should therefore already be assessed for each service, ideally during its planning process. An example of how Phase 6 is proposed to work is given in Fig. 5.9.

The example depicts the degraded ICT network from the previous examples along with the modified $\mathbf{\Delta}$ as well as a simplified list of service-specific state definitions. Based on these simple assumptions, the SE service would result in its limited state as it does not have access to measurements on bus 4, but solvability is still given due

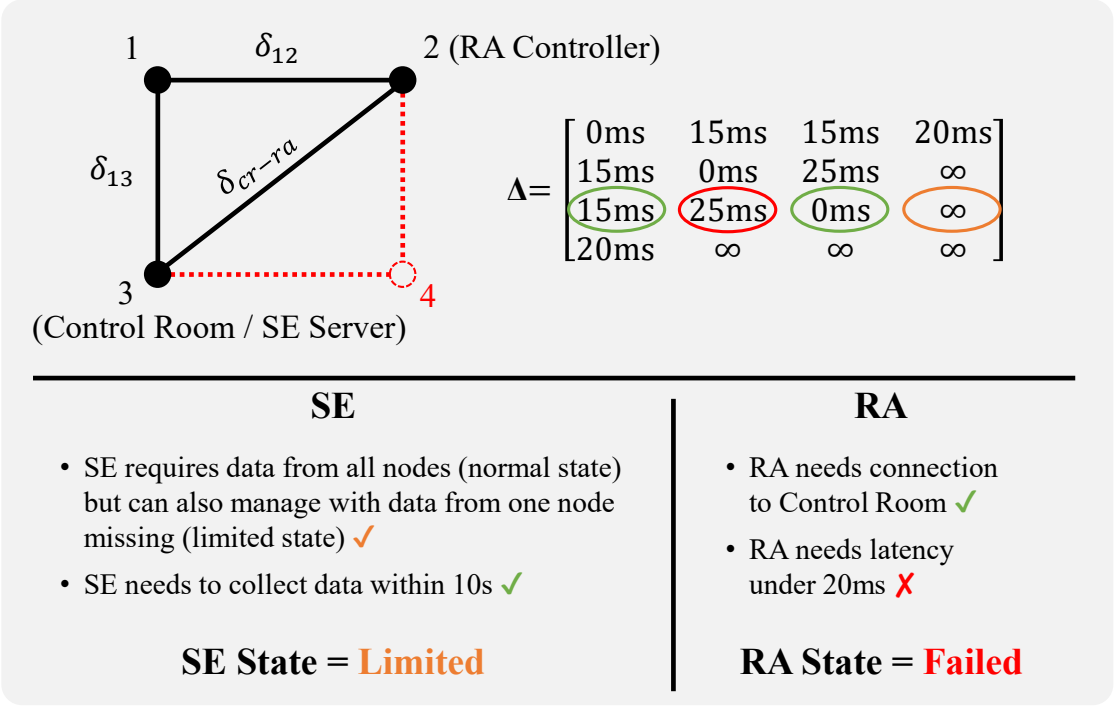


Figure 5.9: example of deriving service states based on a given $\boldsymbol{\Delta}$

to (for example) pseudo-measurements. The RA on the other hand could require a very fast response time to solve the fictional disturbance. This fast response cannot be realised under consideration of the increased latency δ_{cr-ra} between the control room and the RA controller.

Phase 7: Derive Operator Control Decisions

After the system operator's perceived view of the CPES has been calculated, the actual decision-making of the system operator is simulated in Phase 7. This decision-making process conventionally implies human interaction. In light of ongoing automation, though, fully automated decision-making is more likely in many cases and must therefore be included, too. The outcome of this phase is a set of control commands for supposedly connected and available services with which the operator intends to remedy an observed disturbance or optimise the current operation of the CPES.

The proposed approach to simulate an operator's decision-making process is based on the Optimal Power Flow (OPF) method. As explained in [67], the OPF combines an objective function with multiple sets of technical and/or economical constraint functions in order to formulate an optimisation problem. By changing the optimisation function itself, the OPF can be altered so that it aims at optimising different aspects

such as minimising operational costs, electrical losses or the required changes controlled by the operator. In order to consider both the reliability of the power system and the economic component, a set of cost functions that also comprise specifically high costs for the loss of loads is proposed. Such a combined objective function can, for example, be formulated as

$$\min \sum_i cg_i \cdot P_{G_i} + cd_i \cdot \Delta P_{D_i} \tag{5.3}$$

with cg_i being the generation cost for generators at bus i, and P_{G_i} being their active power output. Furthermore, cd_i and ΔP_{D_i} represent the penalty costs for unsupplied or shed loads and the total amount of unsupplied or lost active power demand at bus i, respectively.

The set of equality constraints for OPF is derived from the power balance criteria in power flow calculations. Depending on the level of detail to be considered in simulating the decision-making process, a full AC-OPF or a linearised DC-OPF can be applied. This chapter aims at explaining the general method with its eleven modular phases and their high-level connections instead of providing details for each potential implementation. Hence, the less complicated linearised DC-OPF approach is chosen here. This leads to the common equality constraints in the shape of the power balance criterion and the simplified power flow equations

$$\begin{aligned} \sum_i P_{G_i} &= \sum_i P_{D_i} \\ P_{ij} &= \gamma_{ij} \cdot Y_{ij} \\ Q_{ij} &= 0 \end{aligned} \tag{5.4}$$

with P_{G_i} and P_{D_i} representing the power provided to and demanded by all generators and loads connected to bus i, respectively. P_{ij} and Q_{ij} correspond to the active and reactive power flow between buses i and j, and, finally, γ_{ij} is the voltage angle between these buses, and Y_{ij} is the admittance between the same buses.

The inequality constraints on the other hand typically bring in the physical and operational limitations of the power system's assets. Conventionally, the inequality constraints are

$$\begin{aligned} P_{G_i}^{min} &\leq P_{G_i} \leq P_{G_i}^{max} \\ P_{D_i}^{min} &\leq P_{D_i} \leq P_{D_i}^{max} \\ V_{\text{Bus}}^{min} &\leq V_{\text{Bus}} \leq V_{\text{Bus}}^{max} \\ L_{\text{Line},ij} &< L_{\text{Line},ij}^{max} \end{aligned} \tag{5.5}$$

which represent the acceptable operating ranges for generator output, load supply, bus voltage magnitudes V_{Bus}, and line loadings $L_{\text{Line},ij}$, respectively.

With regard to the explicit problem of simulating the operator's decisions under consideration of a varying set of CPES and service states, the list of inequality constraints needs further adaptation. For one, the range of flexibility of control parameters like P_{G_i} or P_{D_i} can be modified so that it obeys additional operational restrictions. The simplest example of this is the shedding of loads in an emergency situation as a means of containing a local outage. While the OPF should potentially be able to consider the option of non-contracted load-shedding, it should only do so if the CPES is in the alert or emergency state at the time of decision-making. This concept of a dynamically changing set of acceptable actions in dependence on the current ENTSO-E system state is generally mentioned in [43] and exemplary details on a national implementation level can be found in [42]. Implementing this option into the OPF means dynamically adapting the P_{D_i} for all affected loads i so that it can be set to 0, if required. Any service that would ultimately affect P (or Q) consumption or generation can be covered in a similar way by changing the allowed P-range of the service-controlled buses accordingly. For services that affect the grid topology, though, a different approach is required since the admittance matrix $\boldsymbol{Y}$ is assumed to be an uncontrollable input for an OPF. For every possible power system grid topology that is supposed to be considered a valid alternative by the OPF, one iteration of the OPF must be executed. Once all iterations are solved, the resulting values for the objective function need to be compared and the result with the best value represents the optimal topology configuration. This approach does impose problems with scalability concerning large-scale systems with many possible topology configurations, though.

The service states can be implemented into the OPF in different ways, depending on how their states are defined: In cases where a limited service state affects the operational range or available flexibility, the state can directly be mapped onto fur-

ther changes in the OPF constraints. For example, a flexibility provider that can only guarantee 50 % of its expected flexibility range while in limited state can be represented by changing the corresponding P- or Q-ranges on all affected busses. Yet, a different approach is required for those services that have their states defined by whether their successful activation can be guaranteed or not, as shown in Chapter 4.2.1. In these cases, an additional loop of OPF calculations is recommended where the first iteration does only consider services that are guaranteed to work. If this iteration does not converge and cannot find a solution, a further OPF iteration under consideration of non-guaranteed services is done. While this solution introduces uncertainty into the decision-making process it can still be better than not allowing for non-guaranteed services to participate at all. An overview of the steps involved in this phase is provided in Fig. 5.10.

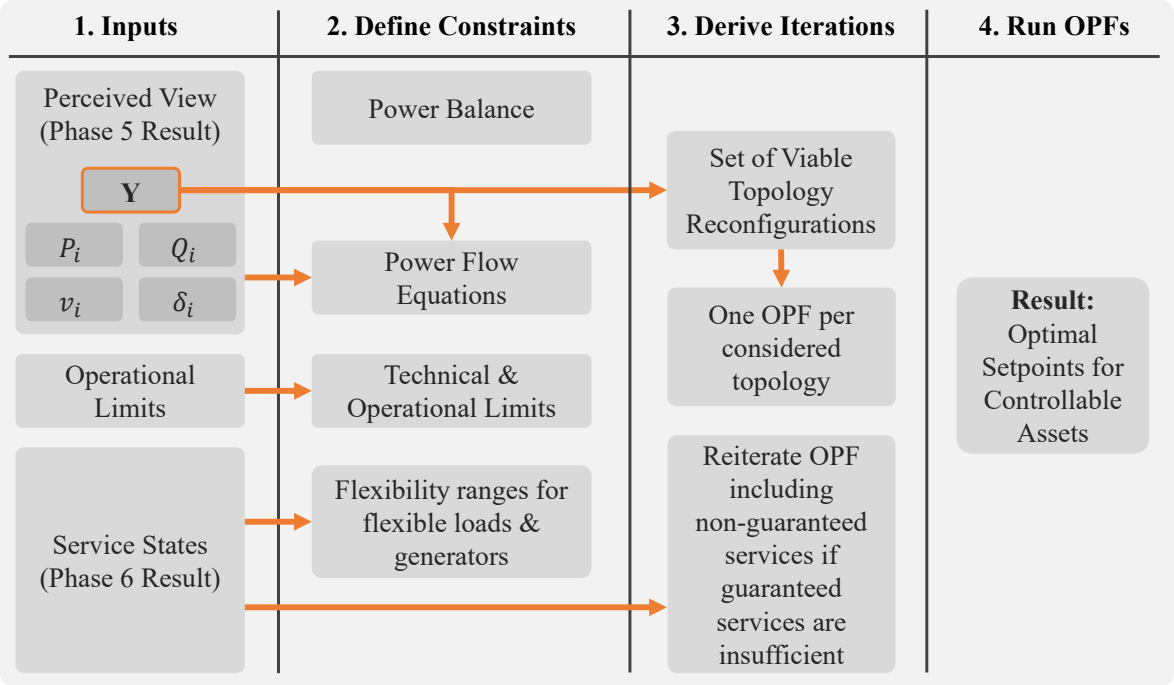


Figure 5.10: From perceived view to operator control decisions

Once all constraints have been adapted to the expected performance of the relevant services and the CPES state and all valid versions of $\boldsymbol{Y}$ have been defined, the OPFs are executed. Information on how to implement and solve OPFs is sufficiently provided in the literature, for example in [68]. The OPF result provides the ideal power system grid topology along with a set of system parameters that can be controlled by the operator and that are supposed to lead to an optimal CPES configuration based on the perceived system view. Note that the depicted approach provides general

options to incorporate various types of services in a modular way. Hence, the resulting optimisation problem cannot be guaranteed to converge as the complexity of the chosen services and their impact on the OPF constraints might result in unsolvable situations.

Phase 8: Check Transmission of Control Commands

This phase covers the third and thus last remaining high-level implication of CEPS interdependencies for system operation, the 'potentially impaired control capacities' as a consequence of degraded ICT performance. Once the operator's desired control decisions have been derived in Phase 7, it must be checked whether these very control commands can actually be transmitted to the service controllers. Thus, in Phase 8 the focus is shifted back from the perceived system view to the real, physical system view. Some of the assumed to be available, activated services might not be available any longer due to impaired communication. Determining which commands can be transmitted successfully is done by calculating the required ICT connections between the sender, typically the control room node, and the receiver, e.g. the service controller's node, and checking whether they are still both available, connected and whether rerouting and therefore increased communication delay beyond the allowed threshold is experienced. Each control signal experiencing a latency $\delta = \infty$ is to be discarded and the corresponding controlled change will not be considered in the following steps. This phase captures those cases in which the operator's awareness of one or multiple service states is wrong or outdated.

Phase 9: Inject Control Commands

Phase 9 concerns the injection of those control commands that have successfully been transmitted to service controllers into the system configuration. Similar to the injection of disturbances in Phase 2, these received control commands are translated into changes of P_{Bus}, Q_{Bus} or $\boldsymbol{Y}$. In theory, active ICT-based services for adapting or improving the ICT system via $\boldsymbol{\Pi}$ or $\boldsymbol{\Delta}$, such as software-defined networking solutions as shown in [57] and [69], could also be considered here. As the focus of this work is rather on the power system, such 'RA-equivalents for the ICT subsystem' are not considered any further.

Phase 10: Simulate Controlled System Response

This phase works analogous to Phase 3 and is meant to calculate the impact of the operator's control actions on the power system. Thus, a further iteration of power flow calculations based on the previously changed system configuration is recommended. It ultimately provides the disturbed and controlled version of the power system.

Phase 11: Update ICT Topology

As previously shown in Phase 4, this phase focuses on the aspect of the changed availability of ICT components. Updating the ICT topology is done analogously to the process described in Phase 4 and is meant to capture both, potential improvements in the ICT system as a consequence of successful CPES operator decisions, as well as exacerbated ICT degradation as a consequence of unsuccessful or even contra-productive operator decisions.

Looping Criterion

Finally, it must be checked whether a control equilibrium has been reached. This is the case once no further control decisions or commands are issued by the operator. Until that point, Phases 5 to 11 are looped with the fully controlled CPES being fed back into the process of creating an updated perceived view with updated ICT component availability. Once Phase 7 no longer results in any desired controlled system changes, both the inserted disturbances and the corresponding control actions have fully unfolded and the system has either reached 'a state of operating equilibrium' as introduced in Chapter 2.1, or it has experienced a blackout.

5.2 Deriving State Trajectories

Once the propagation of a disturbance – or a set of disturbances – through the CPES is known, the states of both the CPES and the services can be determined. The goal of this step is to obtain a means for qualitatively assessing the CPES reliability and robustness in the context of said disturbance(s). More specifically, a series of 'snapshot-based' state assessments with multiple sets of CPES and service states for different points in time is proposed. This way, a detailed record of the impact of both

the cascading and escalating disturbances in the CPES on the one hand and control actions on the other, can be created. The actual assessment of the CPES state is done in accordance with the ENTSO-E state presented in Chapter 2.4. The service states are determined via comparison with the service-specific state definitions, which need to be known upfront and have been introduced in Chapter 4.2. For demonstration purposes, Fig. 5.11 shows a fictional state trajectory for a generic CPES comprising an SE and one SE-based RA and being subjected to multiple disturbances and control actions.

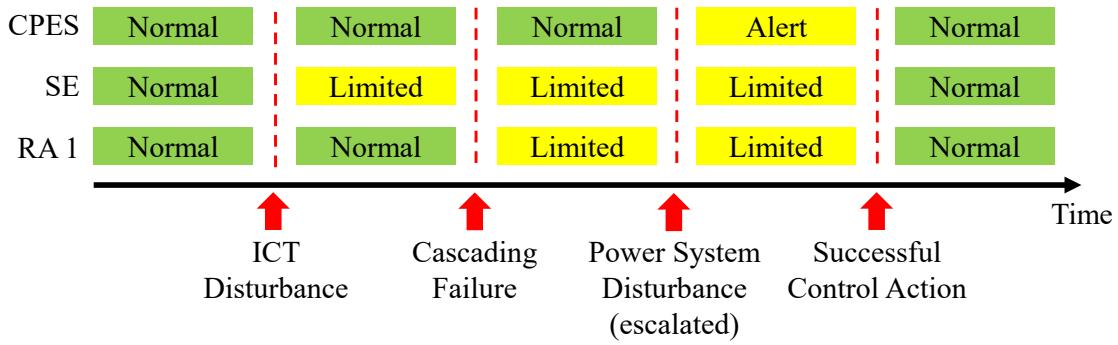


Figure 5.11: Exemplary State Trajectory for a CPES with SE and a generic RA

The shown example could describe a scenario in which a coordinated fast redispatch with RES resolves local network congestion despite the SE operating with decreased accuracy.

With regard to the phases described in Chapter 5.1 three points in the process can be identified for iterating on the state assessment in order to create an insightful state trajectory. Assessing the CPES and service states right after Phases 4 and 11 (marked as red lines in Fig. 5.12) allows keeping track of the actual system states based on the physical CPES after a disturbance has unfolded and after control decisions have been realised. In addition to that, the perceived states can be assessed based on the results of Phases 5 and 6 (orange line). This is considered optional as this step merely captures potential errors in the operator's situational awareness, which might explain unfit decision-making.

The state trajectories can be leveraged for comparing different CPES or service designs regarding their reliability and contribution to resolving emergencies in the CPES. A change in an RA's implementation, for example, can lead to a completely different state trajectory for the same disturbance and otherwise unchanged system. In this context, assuming the RA shown in Fig. 5.11 did not have a fallback mechanism

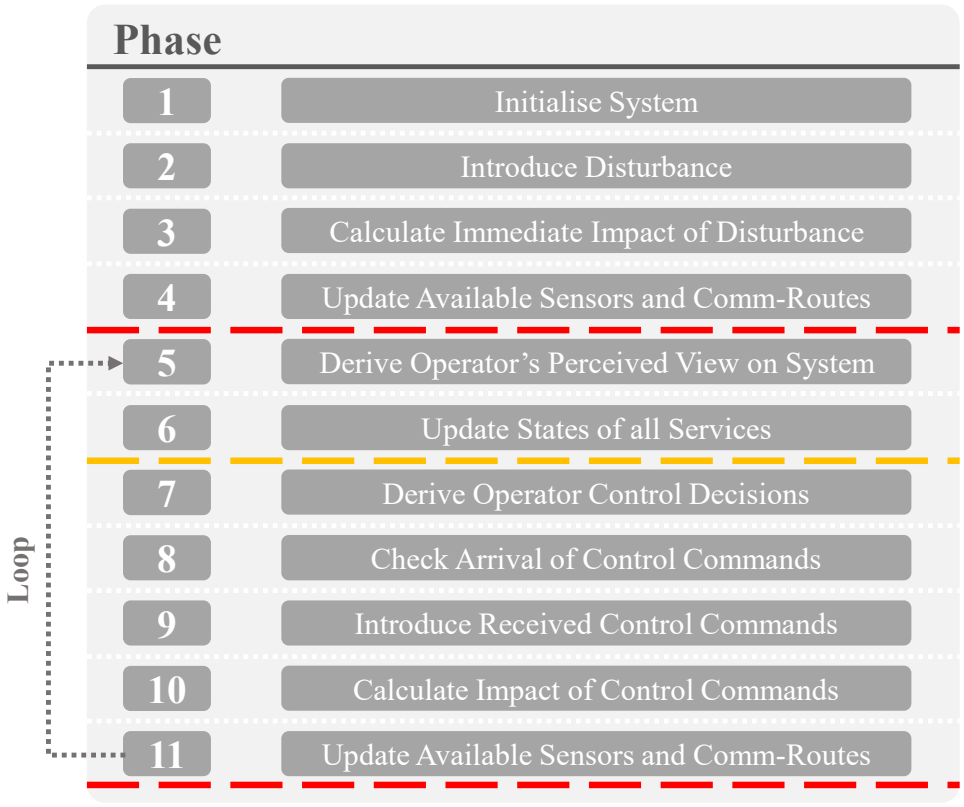


Figure 5.12: CPES and service states are assessed after Phases 4, 6 and 11

to compensate for locally inaccurate SE results, the corresponding state trajectory could potentially rather look as shown in Fig. 5.13. In this fictional case, the RA is not able to operate without precise SE results and can therefore not be used to remedy the network congestion. This leads to a thermal overload of lines after some time and, ultimately, causes the CPES to drop to the emergency state.

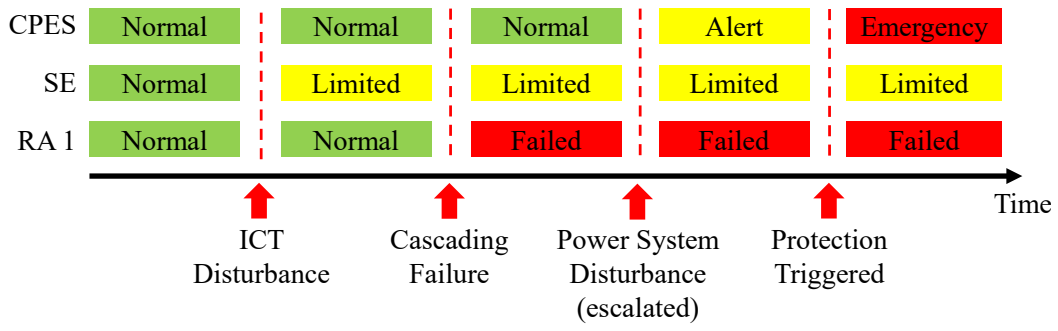


Figure 5.13: A changed RA causing a different state trajectory

5.3 Method Application

The relevant aspects of interdependencies, ICT-based risks and cascading disturbances in CPESs have been described and a method to analyse them qualitatively has been outlined, as well. These concepts and methods can primarily be utilised during the planning process of CPESs. Once the concept of state trajectories itself as well as the method to obtain them are fully understood, the trajectories can be utilised for the qualitative comparisons of different CPES designs with regard to their stability in adverse circumstances. The ENTSO-E-based CPES state trajectory provides an acknowledged health indicator for the system over time. Not only does this indicate whether the CPES is able to ultimately withstand an external disturbance, but it also shows the criticality of specific disturbances, control actions, and situational awareness of the system operator. Once the state trajectories for different system expansion scenarios, control schemes or disturbance scenarios are available, the impact of these changes to the system's stability can be compared as explained in Chapter 5.2. Hence, the method presented in this work can help identify areas in a power system that would require changes to maintain the used level of stability and reliability in the face of the ongoing transformation towards decentralised, cyber-physical systems. It can furthermore provide recommendations about whether and where to apply physical grid expansion or upgrade the ICT system for an improved inclusion of DER-based services and thereby justify investment costs. The added value of newly planned redundant means of communication can be assessed for different scenarios and compared with alternatives, too.

In addition to this primary use-case, the presented concept of service states could also be used in CPES operation. Such service states can be frequently updated and presented to system operators in order to provide insights into the currently expected performance of ICT-reliant remedial actions and other services. From an operator's perspective, this information can serve as an early warning signal for impending system threats or at least prepare the operator for degraded service performance. The official ENTSO-E states description incorporates the availability of crucial services to some degree, but the definition of service-based degradation of system states lacks details.

5.3.1 Case Study on Static CPES Stability

The following chapter presents a detailed case study that is meant to demonstrate the methods described in the previous chapters along with their usage. This study's objective is to simulate a CPES with a focus on said interdependencies and assess the propagation of selected disturbances. Additionally, the system's static stability is assessed by comparing the qualitative state trajectories resulting from different simulation scenarios. Thus, the study follows the method presented in Chapters 5.1 and 5.2 but replaces the OPF-based decision-making with a simpler set of predefined trigger-conditions and actions. The following descriptions and results have previously been published as a collaborative work in [MK6], which is also the origin of this chapter's figures. An additional, very similar case study using an OPF was furthermore conducted in [MK7] with similar results.

5.3.1.1 System Models and Service State Definitions

The CPES for this study consists of one system model for each domain. For the power system, the CIGRE medium voltage benchmark grid is chosen. As shown in Fig. 5.14, it comprises 15 busbars, two 110/20 kV transformers and 13 loads with Bus 0 being the slack bus with a connection to an external grid. One of the transformers, namely $T1$ is equipped with an OLTC. This OLTC allows for $\pm 1\,\%$ changes in the voltage ratio per step and a range of 10 tap steps in total. As for the operational limits, $(1 \pm 0.05)\,p.u.$ is chosen as the tolerance of the voltage band and the threshold for the maximum tolerable line loading is set to 80 % of the lines' capacities. In accordance with Chapter 2.3, any violation of these limits results in the CPES dropping to the emergency state and if more than 50 % of the busses experience a loss of voltage, the blackout state is assumed. 50 % of all buses is equivalent to more than 7 buses with regard to the chosen benchmark grid.

As no adequate simplified ICT architecture for the CIGRE medium voltage benchmark grid can be found in the literature, it is created manually, following the method explained in [70] and [71]. Each substation of a busbar is associated with a router. This means that a busbar without power supply will directly render the associated router and other devices in the substation (e.g. sensors and controllers) non-functional. All communication within a substation is local and therefore out of scope for this work. Two routers in different substations are connected if the corresponding substations are connected by power lines. This represents the inter-substation

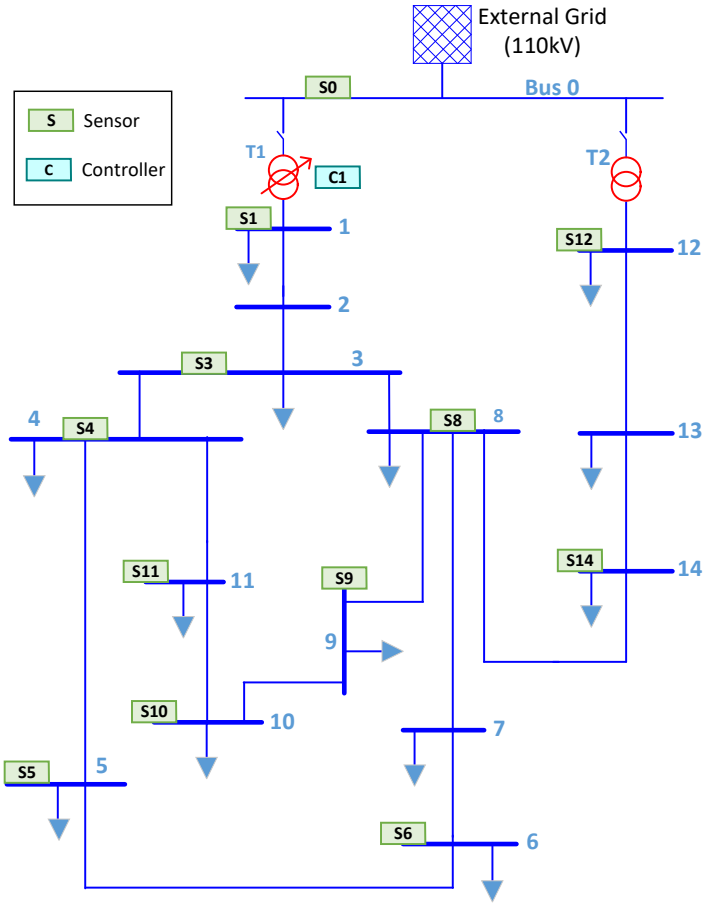


Figure 5.14: CIGRE MV benchmark grid

wide-area network. Note that Bus 0, 1 and 12 are associated with the same router as there are no power lines between them. The control room is assumed to be located at the node with the highest betweenness centrality i.e. Bus 8, which represents the most central node in terms of data flows. The resulting ICT topology is shown in Fig. 5.15.

While the described model can be extended to also consider communication latency, this aspect is neglected for this study. The reason for that lies in it focusing on static stability, for which the time scope is on the multi-minute spectrum while communication latency typically only delays information up to several seconds in worst-case scenarios. Since no explicit requirements of services towards the correctness of data were found in the literature, this case study only considers data (un)availability.

The case study furthermore assumes the CPES to be equipped with two services, the SE and a voltage controller, to be more precise, the latter of which leverages the OLTC for maintaining the voltage band.

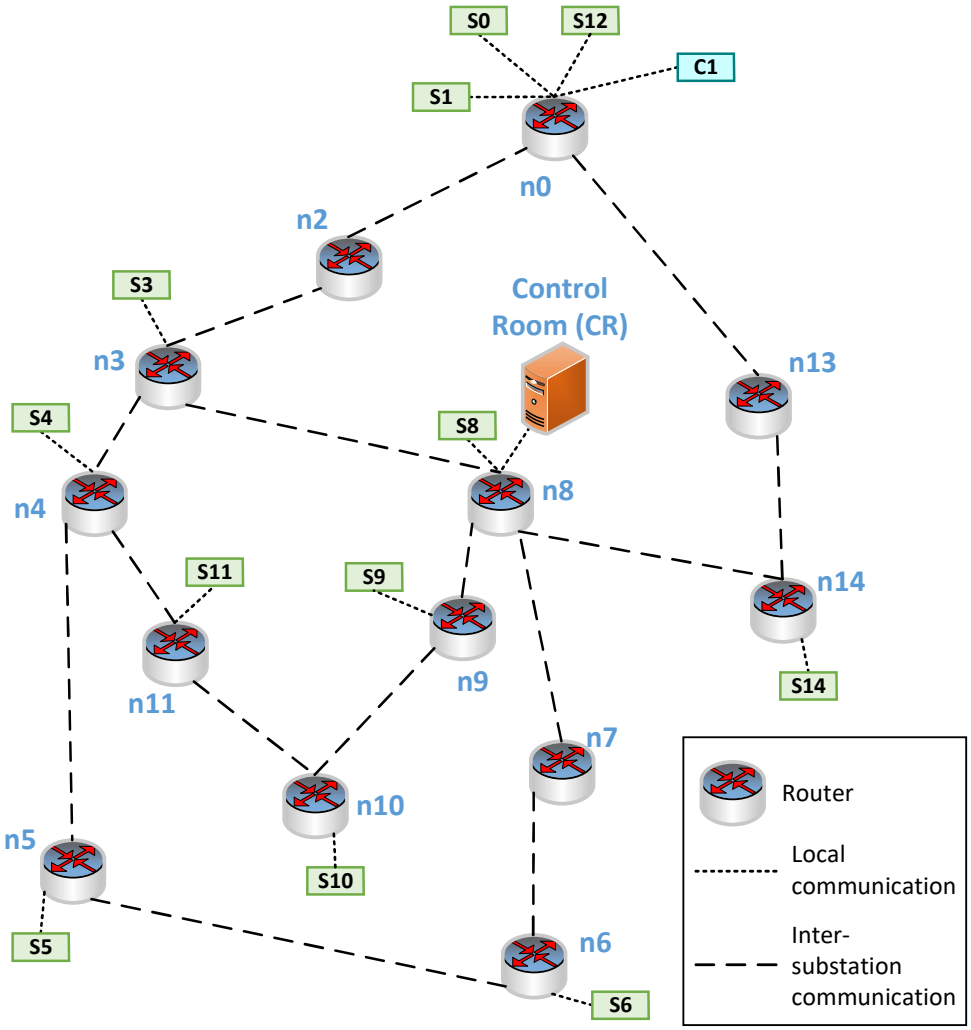


Figure 5.15: ICT Network for the CIGRE MV grid

As for the SE, the sensors measure both P and Q injections at the buses and P and Q flows in the lines on the feeding side. For example, the power flow between Bus 3 and Bus 4 is measured by $s3$ at Bus 3. These measurements are transmitted to the control room via the shortest communication path (e.g. the path with the lowest number of hops) if possible. The control room hosts the SE algorithm, which then processes the received measurements and estimates the bus voltages. Failures in the control room server will directly cause the SE service to fail unless there is a backup or redundant server. In accordance with [MK5], the necessary condition for the solvability of a typical weighted-least-square SE is $\rho(H) = n_{sv}$, where $\rho(H)$ is the rank of the Jacobian matrix (H) and n_{sv} is the number of state variables. H relates to the field measurements with the state variables and is calculated based on the count of available field measurements. In such cases of insufficient available measurements,

solvability can be satisfied by substituting some of the missing measurements with suitable pseudo-measurements (m_p), which are typically calculated based on historical measurements. For this study, m_p is simply based on the last known measurement, which can preserve SE solvability on the one hand but will also increase the uncertainty of SE results on the other. The resulting service state definition for the SE service is summarised in Fig. 5.16.

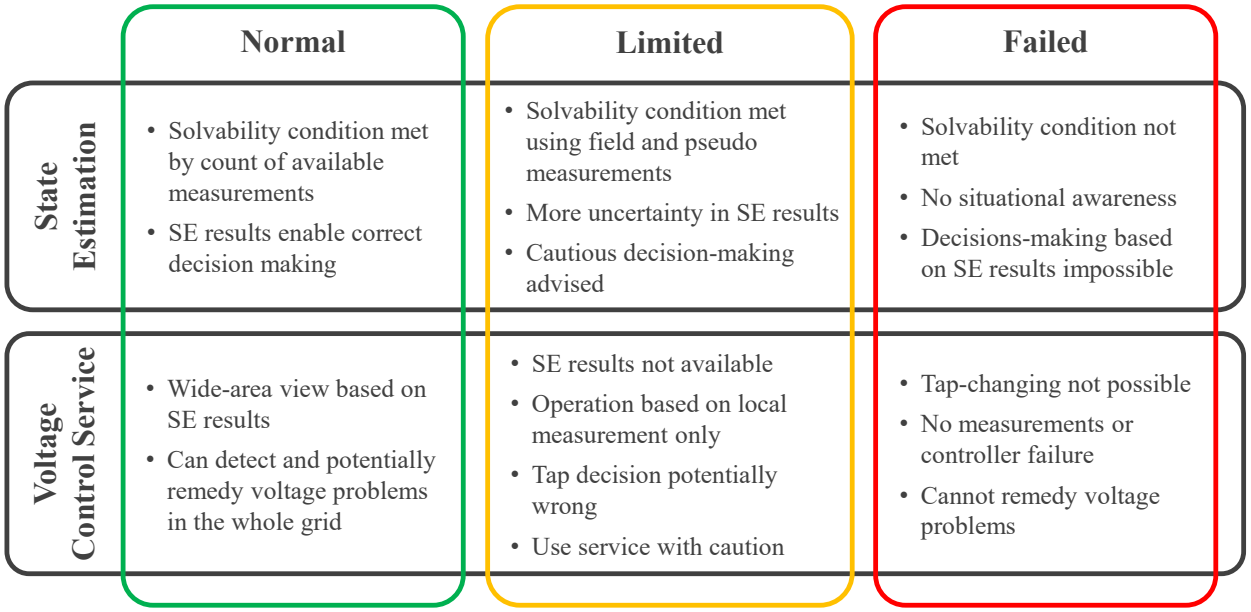


Figure 5.16: Service states

Fig. 5.16 also shows the state definition for the second service in this study, namely the voltage control service, which represents the single implemented RA. The normal operation of the voltage controller depends on two conditions: The availability of either SE results or local measurements with which bus voltages can be monitored, and the possibility to change taps accordingly. In order to have a wide-area view of the system, $c1$ needs to receive SE results from control room via the communication network. Based on this, if $c1$ detects a voltage band violation in any of the buses, it changes the tap accordingly. It then has to wait until it receives the updated SE results in order to know if the voltage violation was remedied or if further tap changes are required. This is done until the violation is resolved, the OLTC has reached its tap limits or until SE results show that both upper and lower voltage bands have been violated and remedying the disturbance with the OLTC is rendered impossible.

Critical disturbances such as $c1$ failure or the OLTC being damaged will directly cause the voltage control service to fail while ICT disturbances can hinder the communication of SE results from the control room to $c1$. This implies that the voltage controller

no longer has a wide-area view. In this case, the OLTC can only act based on local measurements, i.e. the voltage at the secondary side of the transformer (from $s1$). This is a fallback mechanism, using which the service can only detect and potentially remedy local voltage violations and is defined to drop to its limited state. Note that in the case of a meshed grid or a grid with DERs, this may cause voltage problems in other parts of the grid. This implies that, when this service is in the limited state, the operator should use it with caution.

5.3.1.2 Simulation Setup and Disturbance Scenarios

The co-simulation framework for this case study is implemented in python and comprises three main components: On the one hand, the described power system as well as its corresponding services are modelled either directly with or as an extension of pandapower [72]. The same goes for the implementation of the CA module, which is required in order to assess whether the CPES is in the alert state or not, according to Chapter 2.3. This module automatically runs power flow calculations with pandapower for a manually predefined list of expected disturbances under consideration of the OLTC's capacities to mitigate voltage issues. If any disturbance from that list leads to a violation of operational security limits, the CA module changes the power system state to 'alert'. The ICT system, on the other hand, is modelled as a graph using NetworkX[7]. It is used to update the availability (and theoretically also the latency) of communication routes and thereby determine which measurement and control data can be transmitted successfully and which cannot. The third main component is the simulation controller. It initialises and coordinates the two other components and exchanges critical information between them. In addition to the current services states, this critical information comprises a continuously updated list of currently unsupplied busbars, which directly implies unsupplied ICT components, as well as another list of measurements that are currently available to the SE and the voltage controller. An overview of this setup focusing on the ICT- and power system components as well as the critical information exchanged between the two is shown in Fig. 5.17. Each run of the simulation ultimately results in a trajectory of CPES and service states which qualitatively indicate the CPES stability in the face of the chosen disturbances.

[7] https://networkx.org/

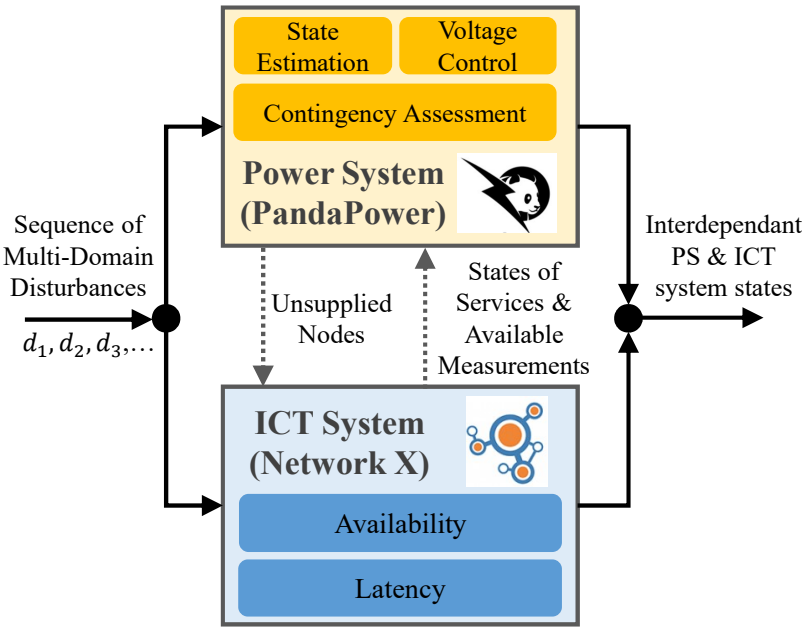


Figure 5.17: Overview of the simulation setup

As for choosing disturbances to be simulated, it is important to understand that this case study does not aim at a comprehensive analysis of all possible disturbances and their combinations, but rather at demonstrating both the propagation of disturbances as well as their impact on the system's stability. Therefore, only a selected number of exemplary state-changing disturbances is chosen and listed in the following Table 5.1.

Disturbance	**Domain**	**Description**
d_{s3}	ICT	Sensor $s3$ outage
d_{s11}	ICT	Sensor $s11$ outage
$d_{no,c1}$	ICT	Link between router $n0$ & controller $c1$ fails
d_{load10}	PS	Reactive (Q) load step at Bus 10
d_{bus9}	PS	Bus 9 failure

Table 5.1: Description of the disturbances in this case study

Sensor failures (d_{s3}, d_{s11}) can occur as a consequence of hardware or software problems while $d_{n0,c1}$ could result from physical damage at the communication links such as fibre-optic cables. Disturbance d_{bus9} can result from a short circuit fault at Bus 9 resulting in the isolation of the bus. The step increase in reactive power at d_{load10} decreases the bus voltage from $0.978\,p.u$ to $0.940\,p.u.$ (i.e. under-voltage), thereby requiring the voltage control service for remedy.

5.3.1.3 Simulation Results

For Scenario 0, which is the reference case, disturbances d_{bus9} and d_{load10} are introduced into the CPES sequentially. The initial d_{bus9} leads to the CA identifying a potential further contingency as irremediable and, hence, the CPES drops to the alert state. This specific contingency is a failure of the power line between Bus 4 and Bus 11 in which case the voltage band would be violated with no means to adequately manage the situation. Disturbance d_{bus9} furthermore renders the ICT components at Bus 6 powerless. The state of the SE service is not affected, though, as sufficient redundant measurements are still available. Additionally introducing d_{load10} has no further consequences for the states because the voltage controller is able to successfully remedy the under-voltage with an adequate change of the OLTC's tap position. The full state trajectory for Scenario 0 is illustrated in Fig. 5.18.

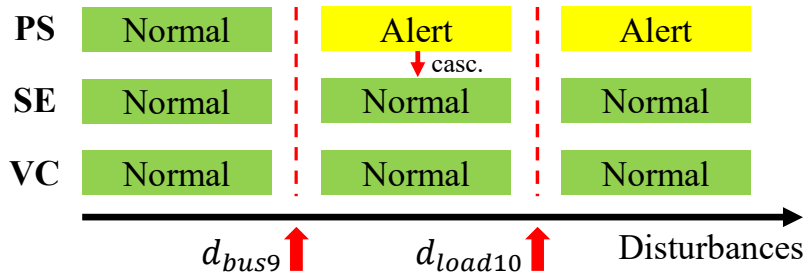


Figure 5.18: State trajectory for the base scenario

Scenario 1 aims at demonstrating disturbance propagation under consideration of voltage control service states. The disturbance-sequence considered is $d_{n0,c1}$, d_{bus9} and d_{load10} and the resulting CPES state trajectory is shown in Fig. 5.19. Disturbance $d_{n0,c1}$ causes this service to degrade to its limited state as it prevents the SE results from the control room to be successfully transmitted to $c1$. This indicates a partial performance degradation of the service (i.e. local view only). Similar to the base scenario, d_{bus9} causes the CPES state to degrade. However, in this case, d_{load10} causes the CPES to drop even further to the emergency state. This is because the voltage control service in its limited state uses local measurements only and is therefore not able to detect and remedy the voltage band violation at Bus 10. This under-voltage situation, if not remedied, could trigger protection systems to trip, thereby causing the loads at Bus 10 to lose power supply. This scenario demonstrates an escalating disturbance where an ICT disturbance ($d_{n0,c1}$) exacerbates an independent PS disturbance (d_{load10}). It also shows that the efficiency of the fallback mechanism

depends heavily on the concrete disturbance.

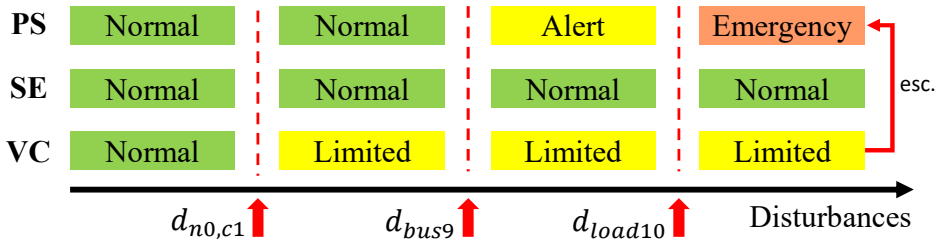


Figure 5.19: State trajectory for Scenario 1

Scenario 2 is split into two parts, namely Scenario 2A and Scenario 2B. The former assumes disturbance d_{s11} to be introduced even before d_{bus9} and d_{load10}. While d_{s11} causes a loss of measurements from $s11$, the SE still remains in the normal state due to the availability of redundant measurements. With d_{bus9} introduced next, the CPES drops to the alert state just as in Scenario 0. In contrast to the reference scenario, the additional loss of power supply to and measurements from $s9$ and $n9$ can no longer be compensated by redundant measurements. As the SE is forced to use pseudo-measurements in this situation in order to fulfil the solvability criterion, the SE state changes to 'limited'. This leads to a regional imprecision in the SE results, which can no longer capture the voltage band violation resulting from d_{load10}. With no available information about any operational security limit violations, the voltage controller is not triggered and the unseen violation persists, ultimately leading to the CPES dropping to the emergency state as shown in Fig. 5.20. Note that this exact sequence of disturbance is very unlikely to happen in real systems and was tailor-made to demonstrate the escalating effects of disturbances within a CPES.

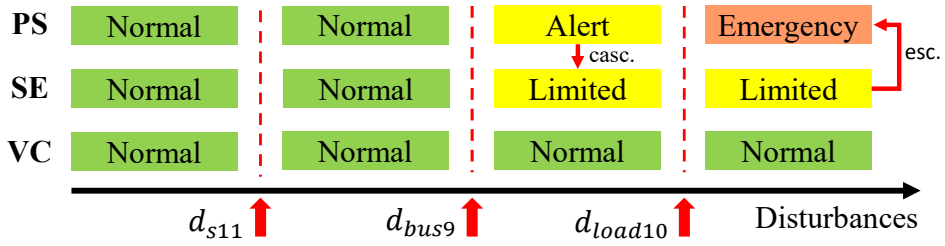


Figure 5.20: State trajectory for Scenario 2A

Finally, Scenario 2B is designed to demonstrate that a limited SE service, despite the results of Scenario 2A, does not necessarily cause severe CPES state degradation in this case study's setup. It considers d_{s3} (instead of d_{bus9}) between d_{s11} and d_{load10}. Although the occurrence of d_{s3} still causes the state of SE to degrade to its limited

state and use m_p (corresponding to either $s11$ or $s3$), the voltage control service is still able to remedy the under-voltage caused by d_{load10}. This shows that the unlikely regional overlap of imprecise SE results and a consecutive voltage band violation in exactly this affected region leads to the amplified CPES state degradation observed in Scenario 2A. Without this regional overlap but an otherwise similar sequence of disturbances that also leads to the use of pseudo-measurements and a voltage band violation, the CPES state remains normal. This can be seen in Fig. 5.21.

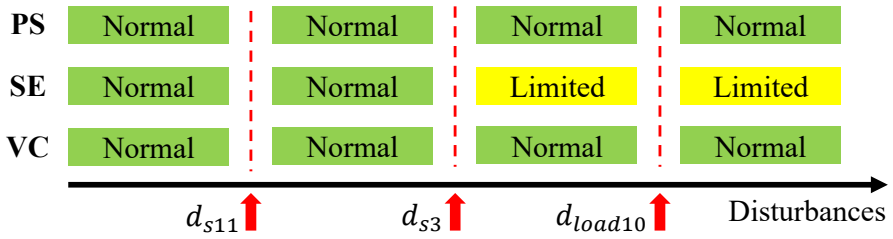


Figure 5.21: State trajectory for Scenario 2B

This case studies' results prove that the propagation of disturbances through a CPES can be derived with the method presented in Chapter 5.1. It furthermore proves that the stability of a CPES with different disturbance scenarios and system designs can be compared qualitatively with the help of state trajectories as described in Chapter 5.2. The particular simulation results are only valid for the chosen power and ICT systems and their corresponding components, controllers, and topologies.

Regarding the applicability of the used method, it can be said that – at the time of writing – this work's author is unaware of any incompatible power systems. As for the compatibility of ICT-reliant CPES services, though, it can be challenging to map complex services to the three service states in a consistent way. The states of different services can therefore not be compared with each other. This means that if two different services are rendered 'limited' in two otherwise identical simulations, one cannot make any claim about which scenario is more stable or critical.

Last, it must be stated that the interpretation of the resulting state trajectories must always be put into context of the specific disturbances introduced during the assessment. The stability of a CPES may well be different in case of other disturbances that have not been included in the assessment.

This Chapter's Core Insights

- The impact of a disturbance can be assessed by an 11-step approach which roughly covers system initialisation, disturbance injection, the potentially degraded operator decision making and the integration of operator control decisions into the studied CPES.
- The presented method's phases are modular and their explicit implementation can be changed with regard to the task at hand.
- The CPES state, as well as all service states can be assessed repeatedly during the 11-step approach. This results in a time-discrete state trajectory which summarises the CPES health
- The state trajectory can be used in order to qualitatively compare different CPES setups and control designs.

6 Stability Quantification

The previously introduced and demonstrated concept of CPES state trajectories provides a qualitative high-level overview of a CPES' stability at different time steps of varying disturbance scenarios. While this approach is aligned with the similarly qualitative ENTSO-E system states, a higher level of detail would improve the comparability of the stability of different CPES designs. Therefore, an approach for quantifying the previous simulation results is introduced next. The resulting metrics focus on the power system domain of the CPES. A complementary definition and study of metrics for the ICT-reliant CPES services can be found in the dissertation of Anand Narayan.

Common metrics for power system reliability focus on the frequency, duration, and extent of supply interruptions [73, 74]. For transmission systems, the corresponding metrics according to [73] are, for example, the 'loss of load expectation', the 'loss of load duration', and the 'expected demand not supplied'. For distribution systems, the 'system average interruption duration' and the 'system average interruption frequency' are common metrics that, among others, have been established as standardised indices by the IEEE Standards Association in [75]. As the method presented in Chapter 5 is using time-discrete, event-based simulations of short time frames right after disturbances occur, all metrics based on long time frames, such as the commonly used average frequency and duration of disturbances over the course of a year, are inadequate. Instead, the supply situation at each time step with a changed steady-state of the power system is used as a basis for metrics in this work. Specifically, the combination of the current 'loss of load' (LOL) and 'load at risk' (LAR) is leveraged to improve the level of detail in state trajectories. Said combination is able to preserve the severe difference in criticality between the alert and emergency state of a power system as provided by the ENTSO-E system states. For example, even a single asset showing a violation of an operational security limit (OSL) will trigger the emergency state but even if all assets are identified as endangered during the CA, the system state is defined as 'alert' only. This is why merging the LOL and the LAR into one metric is not recommended as it leads to an undesirable softening of the critical threshold between the two states. Said two new metrics are based on already established reliability metrics, but they are used to quantify the ENTSO-E system states in this work. As these states rather focus on the risk and stability of power systems, the LOL and LAR are interpreted as stability indicators here.

6.1 Loss of Load

The LOL comprises the active power of loads that have been shed by protection mechanisms as a consequence of m external disturbances $d_{\mathrm{EX},m}$ and loads shed by the system operator as a last-resort remedial action (RA). As described before, the violation of operational security limits (OSL) is the primary trigger for a transmission system to be moved to its emergency state. Loads that are disconnected as a consequence of power system disturbances imply such a violation. Non-contracted loads that are shed intentionally by the operator do not exactly match the definition of an OSL-violation, but are considered equally severe in this work. Any change in the load situation as a consequence of flexibility-calls or contracted load-shedding is not supposed to be included in the LOL. Thus, the LOL is an indicator for the more critical situations in CPES operation and outweighs the LAR, which will be explained in the next subchapter.

Calculating the LOL can be done by aggregating the active power of all unsupplied loads once the CPES has reached a steady-state after inserting $d_{\mathrm{EX},m}$ and accounting for all available RAs. Regarding the simulative approach proposed in Chapter 5, this means that the LOL can and should be calculated whenever Phase 4 or Phase 11 is finished. This is also aligned with the process for deriving the qualitative states shown in Fig. 5.12. Thus, one LOL is obtained for the initialised system state as a reference, as well as for each $d_{\mathrm{EX},m}$ introduced into the system. Based on the simulation results available after said phases, calculating the LOL is simple as it is the difference between the reference active power demand of all loads P_{ref} and the active power actually supplied to loads in the controlled and disturbed system state P_{sup}. In this regard, P_{ref} corresponds to the pre-disturbed load situation of the initialised system, potentially modified by the activation of contracted flexibility options as a remedial action. The shedding of loads that do not participate in any means of contracted flexibility provision does not change the P_{ref}, though. With $P_{i,\mathrm{ref}}$ and $P_{i,\mathrm{sup}}$ known from simulation results for each bus i, the LOL can be calculated as follows:

$$\mathrm{LOL} = \sum_{i=1} P_{i,\mathrm{ref}} - P_{i,\mathrm{sup}} \tag{6.1}$$

The LOL can also be expressed in a normalised manner as the share of the reference load P_{int} that is currently not supplied. This normalised LOL_{n} ranges from 0 to 1 and the corresponding power system can be assumed to be in the emergency state for $0 < \text{LOL}_{\text{n}} < 0.5$ and in the blackout state for $\text{LOL}_{\text{n}} \geq 0.5$. It can be determined via

$$\text{LOL}_{\text{n}} = \sum_{i=1} \left(\frac{P_{i,\text{ref}} - P_{i,\text{sup}}}{P_{i,\text{ref}}} \right) \tag{6.2}$$

6.2 Load at Risk

In contrast to the LOL, which represents the extent of critical power system degradation and relates to the emergency and blackout states, the LAR quantifies the theoretical additional loss of loads in case of further disturbances. It therefore corresponds to the CA as described before and it represents the extent of the alert state. As a reminder, the CA comprises a set of simulations that are based on the current system state, which is oftentimes already disturbed by $d_{\text{EX},m}$ in case of this thesis. For each of the n additional, theoretical disturbances $d_{\text{CL},n}$ from the contingency list, one CA simulation is conducted. During each CA simulation, $d_{\text{CL},n}$ is introduced to the potentially already disturbed system, a power flow calculation is run, and a check for any resulting OSL-violations is conducted for all lines and buses. The LAR can be described as the 'additional loss of loads that results from the CA simulations'. Therefore, at the end of each CA simulation, all assets that violate their respective OSL, are disabled and another, final power flow calculation is executed. Note that this disabling of all assets that violate an OSL during the CA is a strong simplification that results in a potentially overly pessimistic view on the real system's behaviour. Yet, it is aligned with system operators' worst-case way of thinking. Furthermore, the CA already considers all RAs available. Therefore, the only remaining possible reaction of the power system is the protection-based shutdown of assets and shedding of loads. Assuming all overloaded assets to be disabled simultaneously can be unnecessarily extreme, because disabling some assets might already resolve the OSL-violations of other assets. The added value and increased LAR accuracy that would come from considering an optimal shedding-sequence of assets for protection systems does not justify the increased complexity of determining and implementing these sequences, though.

The unsupplied active power of all loads connected to a bus i in any of these CA-based power flow calculations is labelled $P_{i,\text{risk}}$ and is contributing to the LAR, unless they are already included in the LOL. Any load that is already lost in the current system state cannot be at risk at the same time. Furthermore, it is irrelevant if bus i is critical (and therefore shed) in one or many CA simulations, its corresponding $P_{i,\text{risk}}$ is only added to the LAR once. Hence, the LAR can be calculated via

$$\text{LAR} = \sum_{i=1}^{K} P_{i,\text{risk}} \tag{6.3}$$

with K being the set of buses that are still supplied outside of the CA but have been flagged critical at least once by the CA. As the steps required for obtaining the LOL and especially the LAR can be confusing in context of the method presented in Chapter 5.1, Fig. 6.1 summarises the corresponding process:

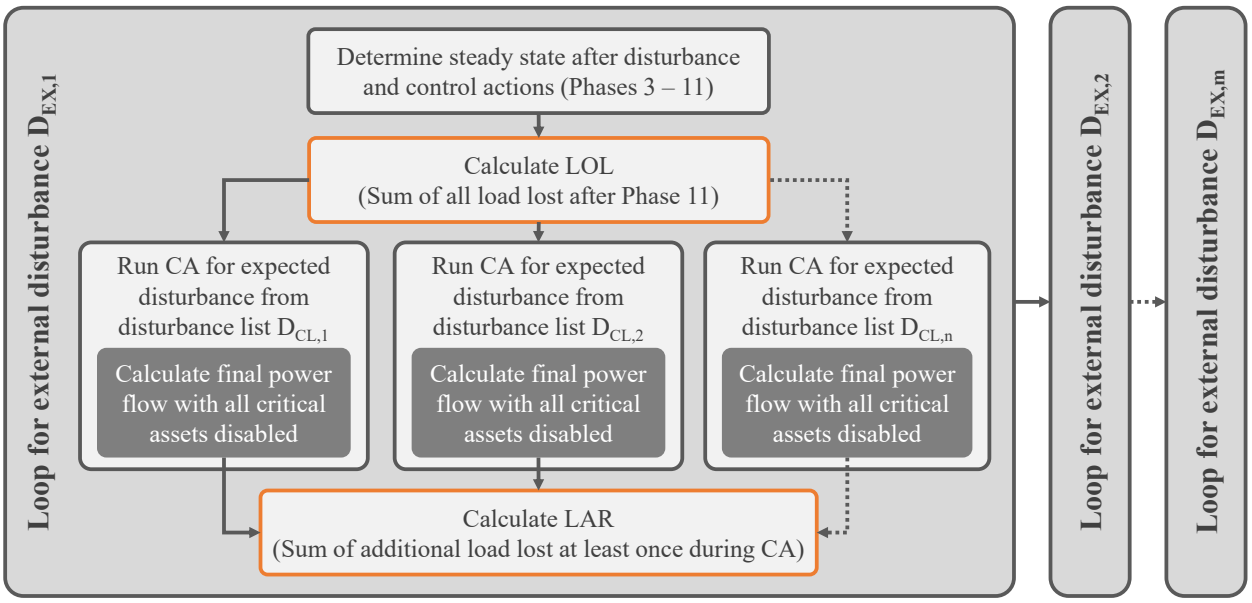


Figure 6.1: Visualisation of the process for obtaining LOL and LAR

Just like the LOL, the LAR can be expressed in a normalised manner, too, if divided by P_{ref}. This normalised LAR_n provides the relative shares of the CPES' loads at risk.

$$\text{LAR}_\text{n} = \sum_{i=1}^{K} \left(\frac{\sum_{i=1}^{K} P_{i,\text{risk}}}{P_{i,\text{ref}}} \right) \tag{6.4}$$

Compared with the previously explained qualitative state trajectories, the LOL- and LAR-based stability assessment of power systems improves on granularity and attention to detail. The securely supplied load (SSL) comprises the load that is currently supplied and not at risk, which directly corresponds to all load that is not part of the LOL or the LAR. A visual representation of this new, quantitative system state can be derived by combining LAR_n, LOL_n and the normalised counterpart of the SSL, the SSL_n in a stacked barplot. Fig. 6.2 demonstrates this with three external disturbances added sequentially to the simulated CPES. It depicts an initially growing LAR after the first disturbance has unfold, inidicating the CPES to be in the alert state. After the second disturbance, most of the LAR is actually converted to LOL while the LAR increases even further. In this case, the power system is in emergency state. Finally, the third external disturbances causes the LOL to exceed the 50 % threshold, shifting the power system to the blackout state.

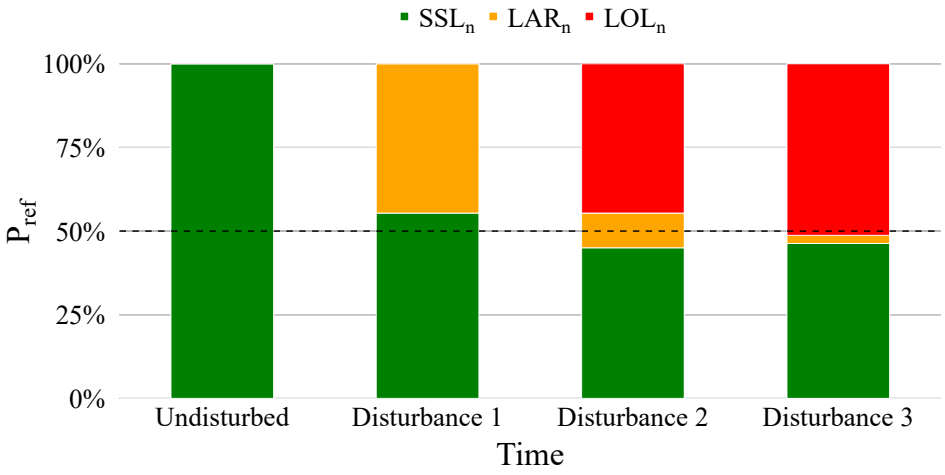


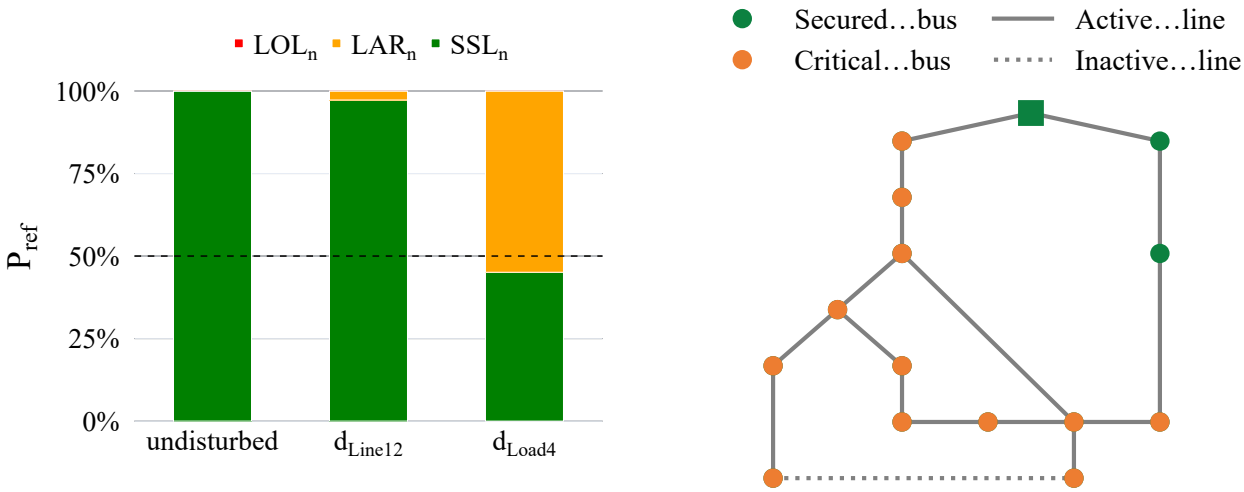
Figure 6.2: Visual representation of CPES stability with SSL_n, LAR_n, and LOL_n

6.3 Quantitative Stability Assessment Example

The application of the LOL, LAR and SSL is demonstrated in this subchapter. The corresponding case study is based on slightly modified versions of the power and communication systems previously used in Chapter 5.3.1. Therefore, the CIGRE medium voltage benchmark grid with a closed switch between Bus 8 and Bus 14 and an OLTC between Bus 0 and Bus 1 is chosen again as depicted in Fig. 5.14. As for the communication system, the same setup as shown in Fig. 5.15 is used as well and the configuration and placement of all sensors, routers, the OLTC controller, and the

SE server remain unchanged. The same goes for the placement and connections of all communication lines. Yet, the base load of all connected loads in the power system was changed as it was increased by a factor of 1.5 in order to bring the system closer to a critical situation. This increased base load is not considered as a disturbance, though, but rather the initial configuration of the power system for the case study at hand.

The following base scenario S1 comprises two external disturbances that are introduced to the CPES sequentially, so that the second disturbance happens in addition to the first one. For each external disturbance, its propagation through the CPES is asssessed as described in Chapter 5.1 considering the performances of the SE and the OLTC controller. In addition to that, the SSL_n, the LOL_n, and the LAR_nvalues are derived for the resulting CPES state after each disturbance has fully unfolded. In this scenario, the first disturbance d_{Line12} affects Line 12, which connects Bus 6 and Bus 7, and is assumed to fail. The second disturbance d_{Load4} describes a positive step in the active power demand of Load 4 by a factor of 3.5. While this is a mostly unrealistic dimension for a load step, this disturbance is considered as 'expected' by the system operator, because it is also part of the list of known contingencies and therefore regarded during the CA. The fact that this large factor is not a direct problem for the CPES' stability can also be taken from Fig. 6.3 which visualises the LOL_n, LAR_n, and SSL_n for this base scenario S1 together with an overview of the final states of all buses and lines:



(a) Load shares

(b) Final bus and line conditions

Figure 6.3: Simulation results for S1 with two cumulative uncritical disturbances

As can be seen, the undisturbed CPES results in all loads to be securely supplied, even in the face of the active power step factor of 3.5 of d_{Load4} which is considered a known risk and assessed during the CA. Therefore, the CPES can be assumed to be designed with this specific disturbance in mind. After d_{Line12} has unfold, a minor share of load is no longer securely supplied and might potentially be shed if one or multiple specific contingencies from the list of known contingencies occurred in addition to d_{Line12}. This is represented by the $\mathrm{LAR_n}$ (yellow) of approximately 3 % in the corresponding bar in Fig. 6.3. The additional introduction of d_{Load4} leads to a significant increase of the $\mathrm{LAR_n}$ to 55 % as further loads are shed in CA simulations. Still, the $\mathrm{LOL_n}$ is zero as no load has been shed. In terms of ENTSO-E system states, the undisturbed system would therefore be in its normal state, whereas the system would be in its alert state with positive $\mathrm{LAR_n}$ values but no lost load at both later points in time. This base scenario demonstrates the added value of quantitative results as the CPES stability is clearly more severely degraded once the second disturbance is introduced. Yet, with the ENTSO-E system states, this difference would be lost in the wide definition of the alert state. From a human operator's perspective, showing less detail and focusing on the most urgent, high-level information is a valid priority as critical decisions have potentially to be made on very short notice. When it comes to planning and assessing the stability of different system designs, though, the increased level of detail that comes with quantitative results can be of great value.

Next, scenarios S2 and S3 are assessed regarding their stability impact in terms of LOL and LAR. S2 is based on scenario S1 with an additional, ICT-based disturbance $d_{\mathrm{n0-oltc}}$, which is introduced in between the disturbances d_{Line12} and d_{Load4}. All disturbances are considered in a cumulative manner once again. Said new disturbance $d_{\mathrm{n0-oltc}}$ describes the failure of the communication link between Node 0, which is installed at Bus 0, and the OLTC controller, rendering the OLTC service degraded. In this state, the OLTC controller can only use locally available voltage measurements as a basis for tap change decisions. The consequences of $d_{\mathrm{n0-oltc}}$ are visualised in Fig. 6.4 as well as its impact on the unfolding of further external disturbances. Immediately after $d_{\mathrm{n0-oltc}}$ has unfold, the share of load that is potentially shed during CA is increased as more CA scenarios would require the OLTC controller to be aware of critical voltages further away from the transformers in order to maintain OSL. The $\mathrm{LAR_n}$ grows from 3 % to 9 %, indicating a lower stability. Last, d_{Load4} is introduced to S2. In comparison with S1, S2 does result in a more critical CPES state once this last disturbance has fully unfolded. With an $\mathrm{LOL_n}$ of approximately 7 %, the system is considered to be in its emergency state. Shedding this 7 % of load does lower the

remaining load of all still operational system assets, though. This in turn renders all load that is not already shed to be securely supplied as indicated by the LAR_n of 0 %.

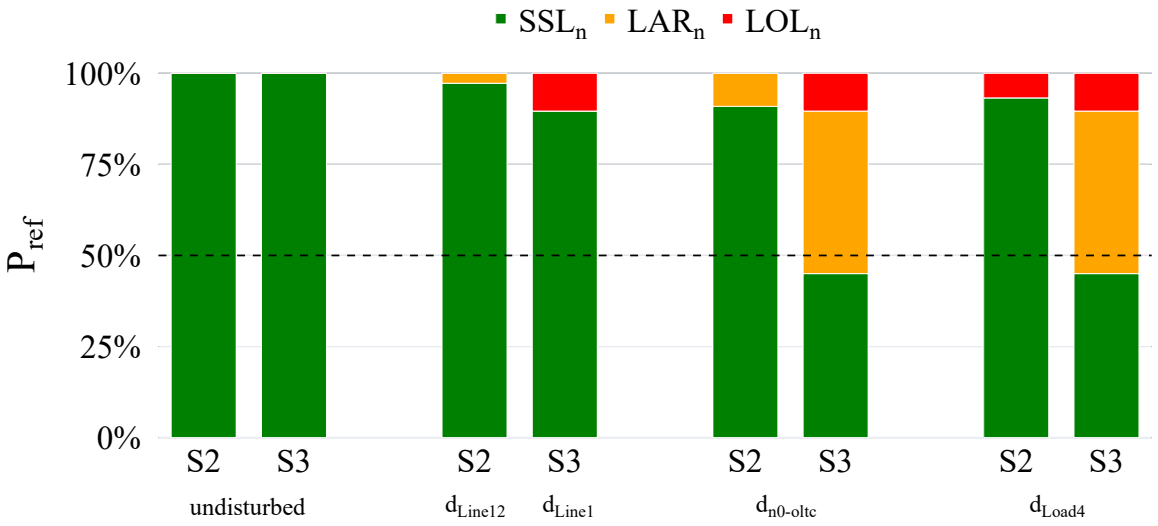
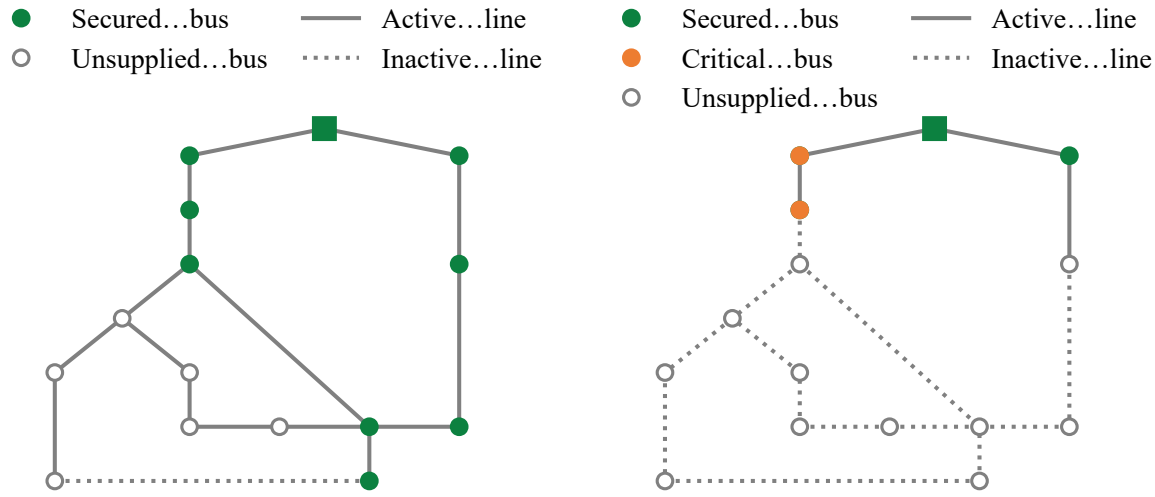


Figure 6.4: Resulting CPES stability comparison for S2 and S3 with three cumulative disturbances each

Scenario S3 differs from S2 in one detail only, namely the line that is affected by the first external disturbance. Instead of Line 12, which was assumed to fail for S1 and S2, Line 1 is affected by an external disturbance in S3. The corresponding results are included in Fig. 6.4, too, and thereby demonstrate a comparison of different disturbance scenarios and their impact on CPES stability. As Line 1 is a central asset of the analysed power system, it is assumed to be reinforced by the operator and therefore deemed extremely unlikely to fail. Hence, disturbance d_{Line1} is not included in the list of expected disturbances and the failure of Line 1 is not considered in the course of the CA. Note that in reality these contingency lists are not comprehensive lists of all possible combinations of disturbances, but a list of exceptional or critical disturbances. While it can be considered realistic for the CA to miss some disturbance scenarios, it is rather unlikely for the CA to not include a crucial asset such as Line 1. Still, d_{Line1} was chosen here in order to demonstrate the importance of a well-maintained contingency list and to further underline the added value of quantitative results. With regard to the latter, d_{Line1} leads to a significantly further degraded CPES stability than d_{Line12}, as can be seen from the LOL_n and LAR_n after the last two external disturbances have unfold. Not only is more load shed according to the final LOL_n of 10 %, but also the LAR_n with 45 % is increased dramatically. While

the CPES would be in its emergency state for both S2 and S3 after all disturbances have unfold, the stability of the CPES is lower for S3 due to the significant share of the remaining load at risk on top of the load that has already been shed. This can be confirmed by inspecting Fig. 6.5 which provides an overview of the final situation in the power system at the end of S2 and S3:



(a) Final bus and line conditions for S2 (b) Final bus and line conditions for S3

Figure 6.5: Simulated grid results for scenarios S2 and S3

The connection states of all buses and lines shown in Fig. 6.5 prove that S3 results in more buses being unsupplied and even among the remaining three supplied buses two buses are still identified as critical by the CA. While S2 also shows several shed buses, the overall situation in the grid appears healthier. A circumstance that - in the context of stability assessment and comparison of different system designs during the planning phase - is not adequately reflected by the qualitative ENTSO-E system states.

It can be taken from the results that the proposed quantitative approach provides better insight into the actual stability of the CPES and furthermore enables intuitive high-level comparisons of different CPES designs in varying disturbance scenarios. In contrast to the state-based qualitative approach, the quantitative approach is applicable for any CPES design as it omits potential problems with mapping all ICT-reliant grid services to service states. Yet, the LOL and LAR only capture the stability of the power system part of a CPES. This is why an additional assessment of quantitative stability metrics for the ICT-reliant services is strongly recommended to be considered as well, as proposed in the complementary dissertation of Ananad Narayan. As

long as service states for all considered services can be defined, the qualitative approach described in Chapter 5.2 presents a simpler approach for studies that do not require an increased level of detail.

This Chapter's Core Insights

- Compared to the qualitative state trajectories, quantitative stability indicators provide a more detailed result that improves the comparison of different CPES designs.
- Suitable power system stability indicators in context of this work are the 'Load at Risk' (LAR) and the 'Loss of Loads' (LOL):
  - The LAR represents the share of all loads' active power that is currently supplied but has been identified by the contingency analysis as potentially lost in case of a further disturbance .
  - The LOL represents the share of all loads' active power demand that has already been lost or shed.
- LOL- and LAR-based results can be used to rank the stability of system designs that would otherwise have resulted in the same qualitative state trajectories.
- While providing less detailed results, the qualitative approach with power system and service states can still be used as a simpler approach. This is especially true if an assessment demands for suitable metrics for ICT-reliant services in addition to the LOL and LAR.

7 Assessment of Dynamic Stability

The core method presented in Chapter 5 is limited to assessing static power system stability. In this light, the following chapter is about lifting this limitation and extending the method so that it also captures dynamic power system aspects and can therefore be used for dynamic stability assessments. As the number and variance of different types of analyses in this domain are vast, the scope needs to be defined first. Under consideration of the different timescales for dynamic power system phenomena, which were shown previously in Fig. 2.2 in Chapter 2.2, communication-based complications can only affect a subset of all dynamic phenomena. While local communication, for example for protection mechanisms, can be designed to happen within less than 1 ms, this work is focused on the impact of remotely controlled or coordinated actions, as protection systems are not novel to power systems and thus not part of the added complexity in CPES. Automated remote communication usually works on a timescale from a few milliseconds up to one minute in extreme scenarios. All processes that take significantly longer than 60 s to unwind are assumed to be solvable via manual communication, e.g. phone calls, in an emergency and would thus not affect CPES stability. Hence, most aspects of the electromechanical category of dynamic power system phenomena are included in the scope of dynamic CPES stability assessments. This implies a focus on rotor angle stability, frequency control and voltage control aspects as depicted in Fig. 7.1.

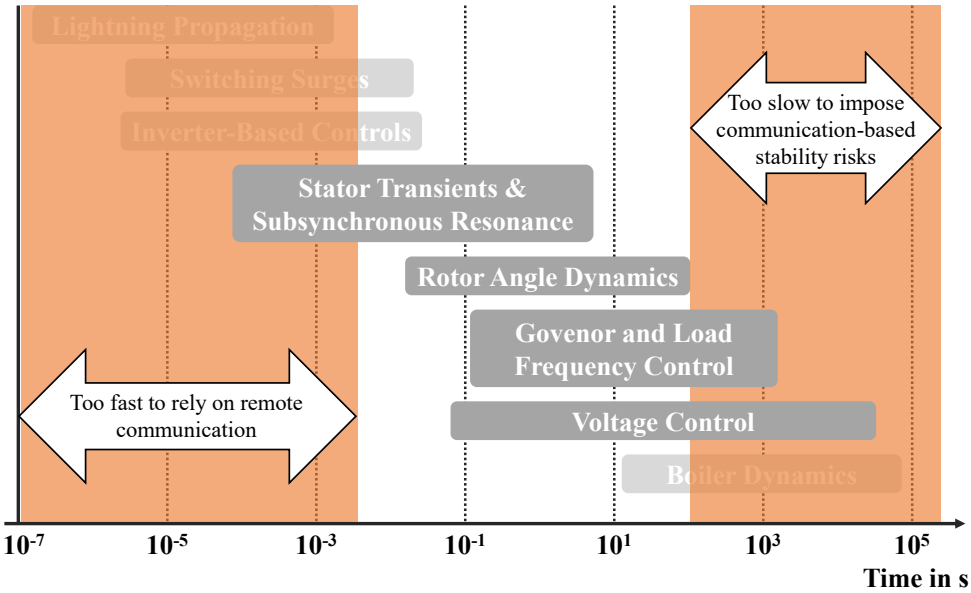


Figure 7.1: Dynamic phenomena and remote communication timescales

A more detailed overview of timescales for both stability categories and power system control mechanisms is provided in [76]. It confirms said focus on inertial response and short-term stability on the one hand and specifies (primary) voltage control and frequency restoration reserve (FRR) services as potentially relevant regarding the scope of this work on the other.

With the time scope defined, some of the phases explained in Chapter 5.1 need to be adapted to enable time-continuous power system simulations and the consideration of dynamic frequency and voltage control aspects. The resulting extension of the previously presented method is capable of not only providing a state trajectory but also information on the time of state transitions. This further improves the comparability of different system designs as they might lead to different durations of CPES state degradations while still resulting in the same sequence of states (state trajectory).

7.1 Necessary Method Adaptations

Said required changes primarily affect the power system model that is initialised in Phase 1 and used for calculations and simulations in Phases 3 and 10, but also the operator's system view and decision-making process in Phases 5 and 7, respectively. These changes are summarised in Fig. 7.2 and their details are described next.

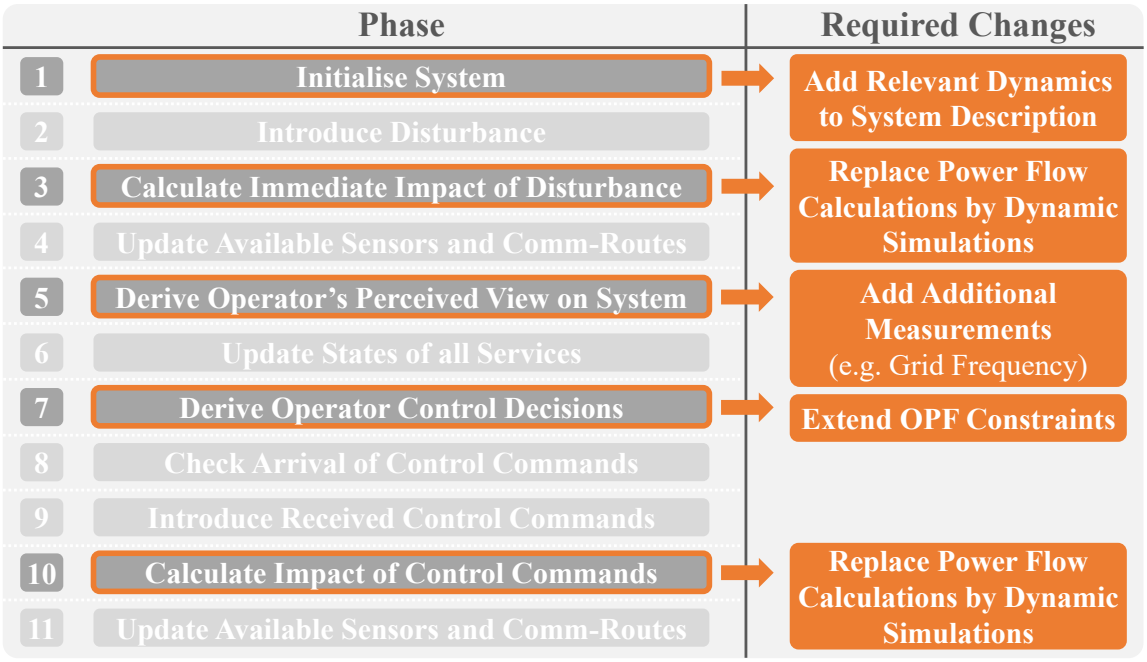


Figure 7.2: Phases that require changes for dynamic stability studies

Extended Power System Initialisation

The first necessary change affects the power system model in Phase 1. For power-flow-based static stability studies it proved sufficient to consider generation parameters, load parameters and algebraic network equations. For dynamic studies, though, the relevant dynamic behaviour of grid assets needs to be regarded, as well, as described in Chapter 2.2. Thus, those asset dynamics that are critical for the chosen dynamic stability study need to be added to the power system description in Phase 1.

One example of this could be a study concerning frequency stability. For this category of assessment, the dynamic behaviour of all synchronous generators, their turbine governors, and, optionally, their excitation systems are typically modelled and simulated. Additionally, loads can be simulated under consideration of their frequency-dependant dynamic behaviour, if desired.

Upgrade to Dynamic Simulations

Power flow calculations alone are insufficient for dynamic stability assessments. Hence, all occurrences of power flow calculations (Phases 3 & 10) need to be adapted. The proposed alternative is a set of dynamic power system simulations. As these simulations introduce a temporal component into the assessment, in contrast to steady-state analyses for static stability studies, basic scheduling needs to be defined as demonstrated by Fig. 7.3.

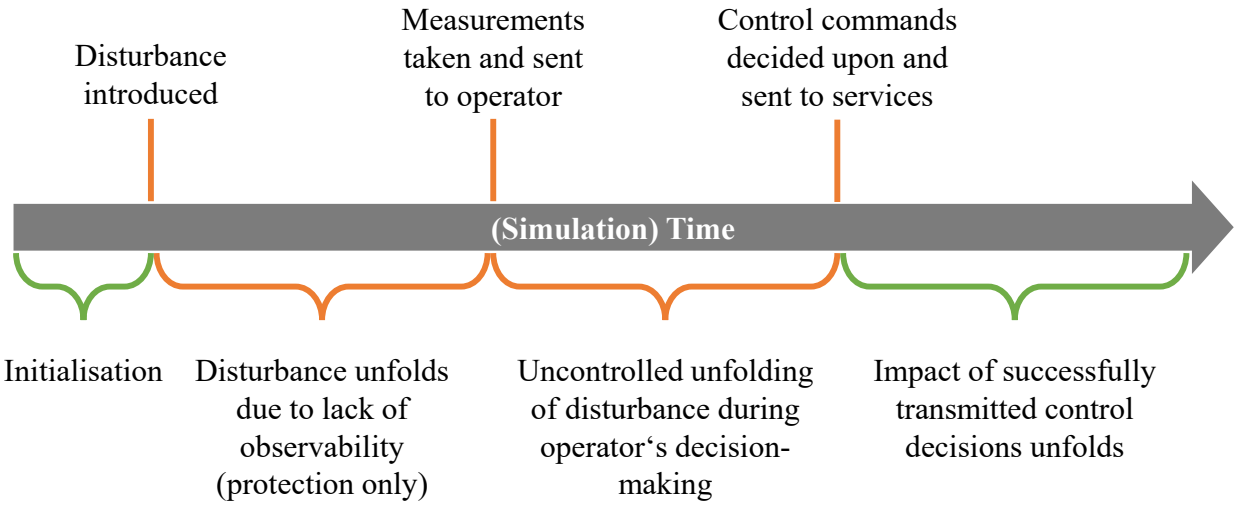


Figure 7.3: Simulation timeline for dynamic stability assessments

This exemplary schedule implies a simulation timeline split into three parts. The first part is meant for initialising the dynamic simulation, aiming to bring the power system to an initial equilibrium state of operation without oscillations. Only then the dynamic simulation is paused and a disturbance is introduced by changing power generation or consumption on affected buses or the grid topology itself, as previously explained in Chapter 5.1. The simulation can be continued until the point in time when the operator's control decisions are received by the corresponding service controllers. At some point during this simulation period, a snapshot of all measurements is taken and transmitted to the operator under consideration of communication availability. Both the time of snapshot creation and of received control commands can be predefined or dynamically triggered. After this second simulation period, those control commands that were transmitted successfully to the service controllers need to be injected into the simulation by altering the corresponding services' setpoints accordingly in Phase 9. The third simulation period is a continuation of the previous one but with potentially changed service setpoints and is meant to calculate the impact of the operator's control decisions.

Altered Decision-Making Process

Depending on the chosen dynamic stability study, additional measurements can be considered available to the system operator. This is indisputably relevant for all studies focusing on frequency stability under consideration of remotely coordinated control reserve services. The operator's view on the power system, which is derived in Phase 5, must therefore be extended accordingly. Regarding frequency analyses, generator frequencies can be considered to be measured at the plants' sites directly and transmitted to the operator's control room. As frequency measurements are not used in SE algorithms, they can rather be considered an additional, dedicated set of measurements that can still be affected by impaired ICT performance.

With the additional measurements available to the operator, its decision-making process can be extended so that it allows for more selective activation of services in specific situations. One example of this would be the activation of flexibilities that provide FRR. These flexibilities should only be considered in the OPF-based decision-making process if the monitored situation shows frequency deviations. The change from power flow calculations to dynamic simulations renders frequency measurements potentially available. Thus, the flexibility range of each bus can be divided into several flexibility pools. For example, the majority of flexible assets on one specific grid bus might

participate in redispatch services while a smaller share participates in FRR provision only. The flexibility range of the latter should only be considered available to the operator in cases of frequency-related problems. The corresponding modification of OPF constraints, therefore, needs to regard additional measurements in general and frequency measurements in this specific example. Concerning Fig. 5.10, the first two steps 'Inputs' and 'Define Constraints' would need to be extended. The frequency measurements need to be added to the perceived view as an additional input that is furthermore compared with the operational limits. If the perceived frequency violates any frequency limits, flexibility ranges of loads and generators can be adapted for all considered FRR providers. To give a better overview, the extended process for OPF preparations is illustrated in Fig. 7.4, an updated version of Fig. 5.10 with added or changed aspects highlighted in green. Note that for various dynamic stability studies the operator's centralised decision-making process should rather be implemented with an AC-OPF instead of a DC-OPF. Otherwise, the fundamental DC-OPF assumptions shown in [77] such as 'all bus voltages set to 1 $p.u.$' and 'all voltage angle differences between branches being negligible' render effective decision-making impossible.

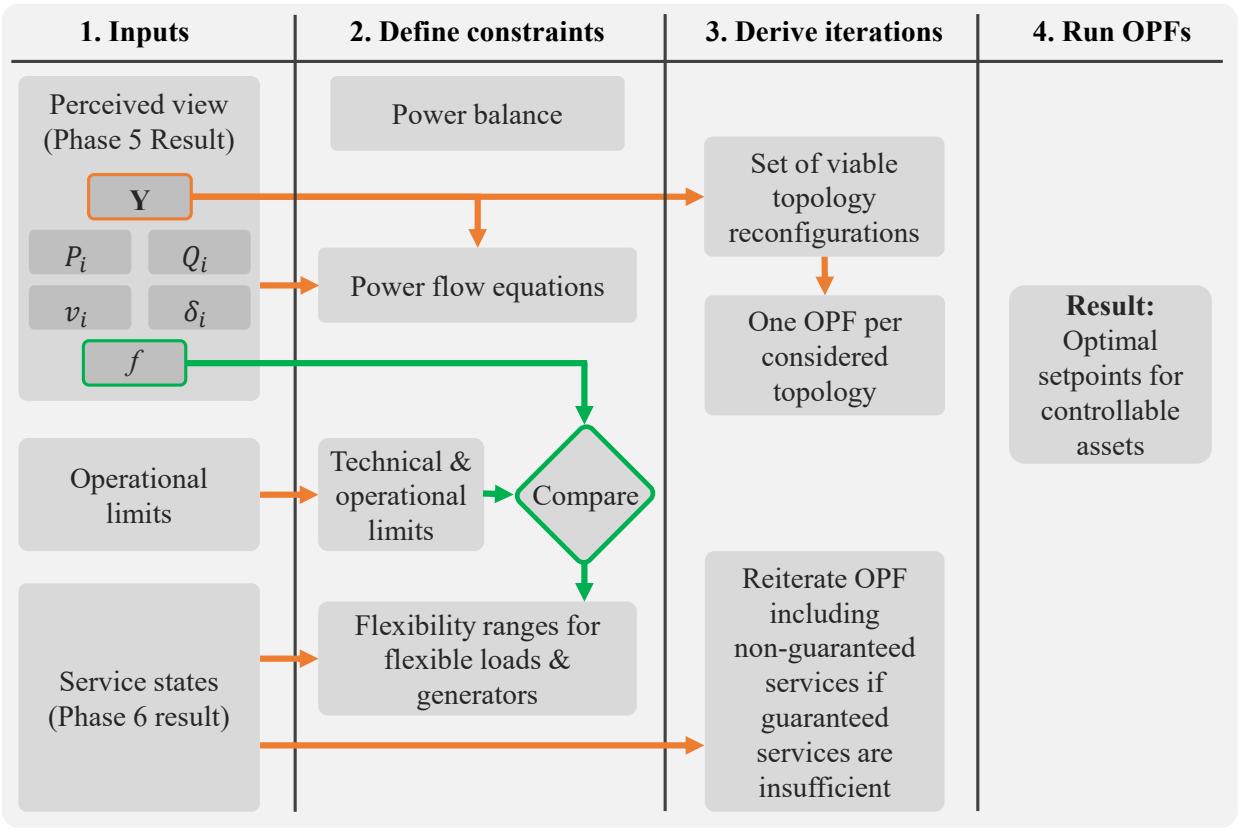


Figure 7.4: Extended OPF preparations considering frequency (green)

7.2 Dynamic Adaptation Example

In order to demonstrate the previously described required changes for dynamic stability assessments next, a simple scenario is presented along with the corresponding simulation results. Said scenario concerns the IEEE 14-bus benchmark grid, local FCR controllers at each synchronous generator as well as centrally coordinated, OPF-based redispatch and FRR services. It is meant to showcase the coupling of dynamic power system simulations with OPF-based decision-making as a valid approach for integrating dynamic aspects into the method described in Chapter 5. Here, pandapower was chosen again to handle the static operator's system view on the power system and the OPF, while the Python-based simulation framework ANDES was tasked with running the dynamic power system simulations [78]. The previously mentioned IEEE 14-bus benchmark grid is used here because corresponding models are available and validated for both pandapower and ANDES. Fig. 7.5 shows a plot of the IEEE 14-bus system with five synchronous generators at Buses 1, 2, 3, 6, and 8 and three transformers which connect the 69 kV area comprising Buses 1-5 with the 138 kV area.

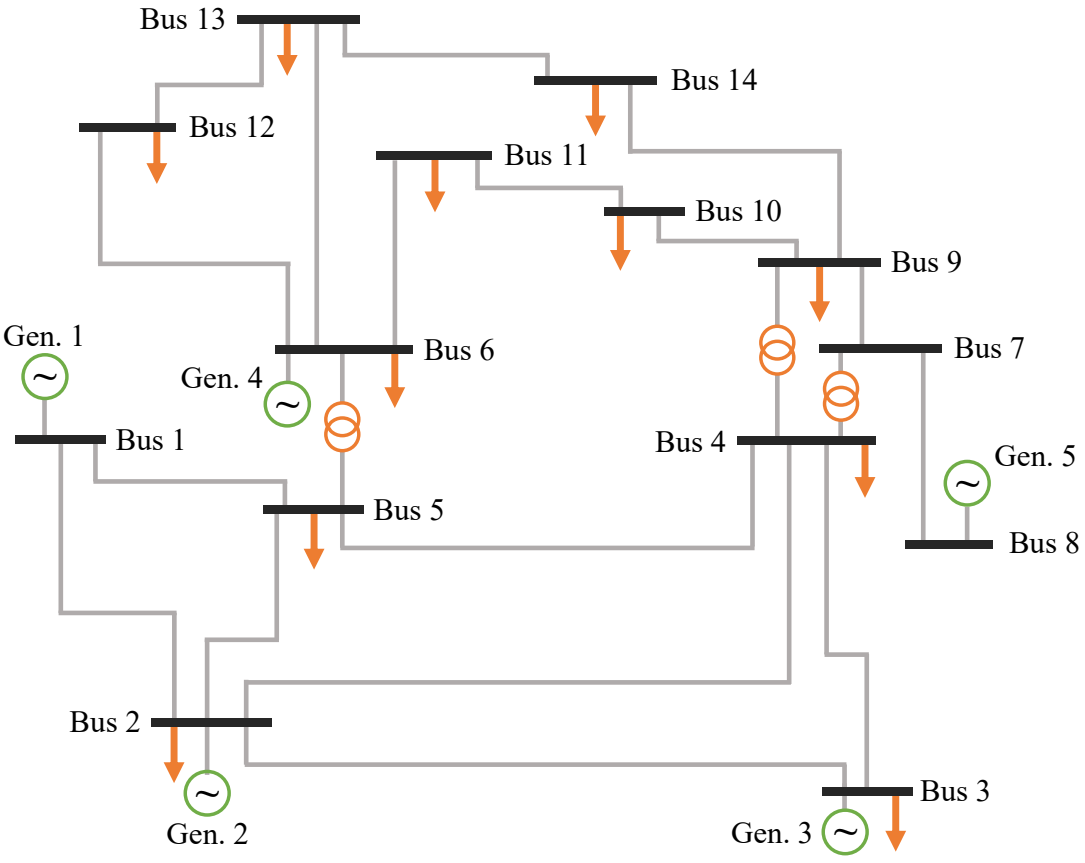


Figure 7.5: The IEEE 14-bus benchmark system

The interface designed to update the pandapower network with the most recent dynamic simulation results and map the OPF results back onto the ANDES network needed to be custom-made, though. As for the dynamic models used for the simulation, all generators were modelled according to the GENROU[8] model and their turbine governors are based on the TGOV1[9] model. In addition to that, the EXST1[10] and IEEET1[11] models are used for the generator exciters. The tasks of the ANDES and pandapower modules, as well as their interactions, are depicted in Fig. 7.6 in the chronological order proposed in Fig. 7.3.

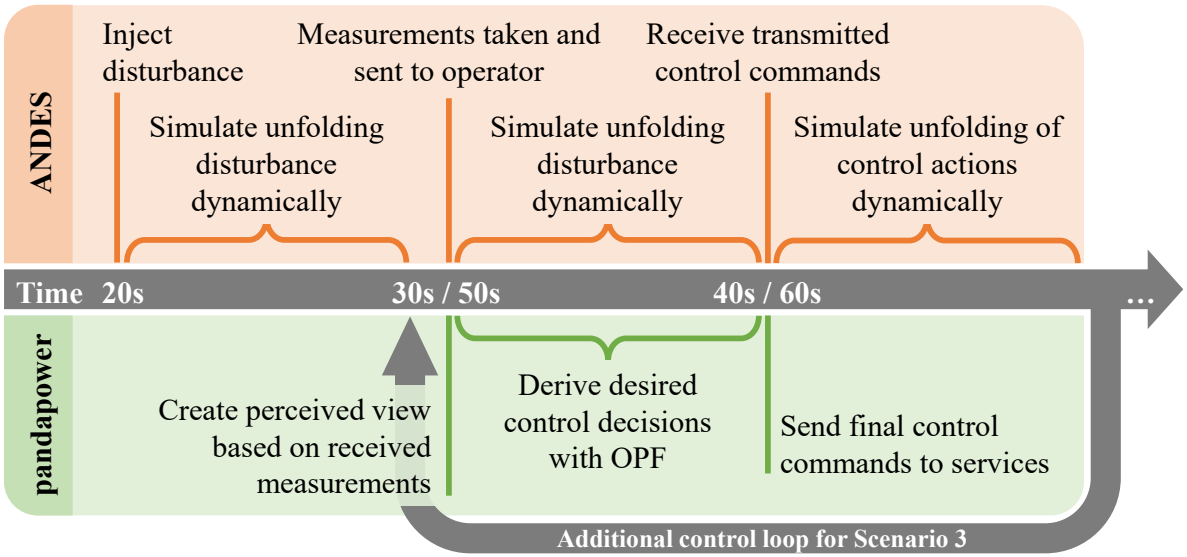


Figure 7.6: Simulation process and interactions between ANDES and pandapower

Note that the ICT network and data flow is not simulated for this demonstration. Instead, delayed and missing measurement or control data is predefined manually and implemented directly into the power system controller simulations where needed since the focus of this demonstration lies on changes required for dynamic power system assessments. While out of scope for the thesis at hand, the core method presented in this work could also be rearranged so that it reflects dynamic changes to ICT services or the communication system, too.

[8] https://docs.andes.app/en/latest/groupdoc/SynGen.html#genrou
[9] https://docs.andes.app/en/latest/groupdoc/TurbineGov.html#tgov1
[10] https://docs.andes.app/en/latest/groupdoc/Exciter.html#exst1
[11] https://docs.andes.app/en/latest/groupdoc/Exciter.html#ieeet1

7.2.1 Scenario 1: No Communication

Scenario 1 (S1) is the reference case with a positive step of the active power consumption on Bus 6 but no coordinated RAs. For any such load step to have a noticeable impact on the system's frequency, the slack bus at Bus 1 needs to be replaced by a synchronous generator. With Fig. 7.3 in mind, the first 20 seconds of the simulated timeline are used as an initialisation phase for the power system, during which all initial oscillations settle. At $t = 20s$, the power consumption step is introduced into the simulation. The impact of this disturbance on bus voltages, generator rotor speed, and turbine output is simulated until $t = 90s$.

Fig. 7.7 indicates an acceptably stable voltage behaviour. Both during and after the system's adaption to the load step all bus voltages remain within the tolerance band between $0.9\,p.u.$ and $1.1\,p.u.$ at all times.

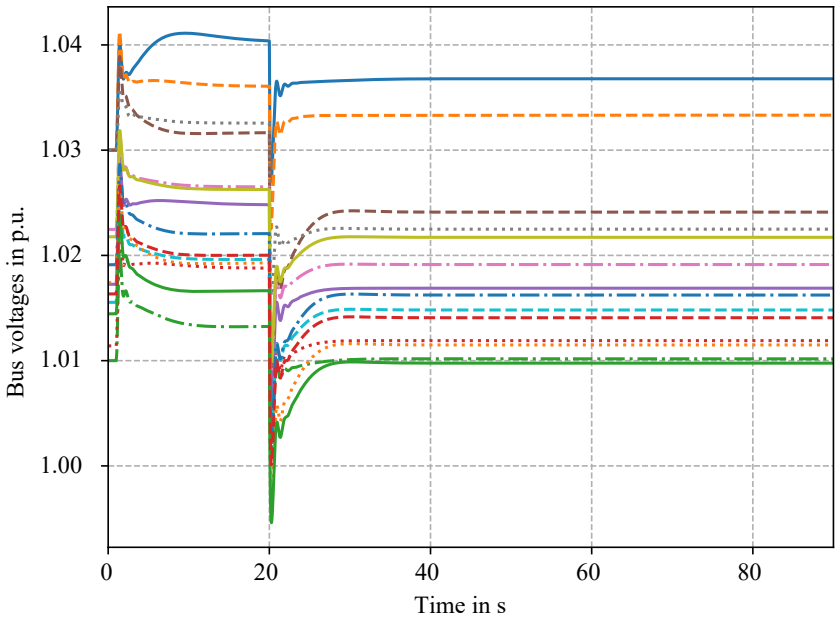


Figure 7.7: Simulated bus voltages for S1

Regarding the generator frequencies, represented by the synchronous generator rotor speeds ω in Fig. 7.8, the local FCR controllers manage to successfully contain the disturbance-injected frequency drop, but the terminal frequencies of slightly less than $0.996\,p.u.$ are too low. As stated in [30], the allowed maximum terminal frequency deviation is $\pm 200\,mHz$, which corresponds to $\pm 0.004\,p.u.$. Thus, while not causing any direct system instability, the frequency behaviour is violating regulations.

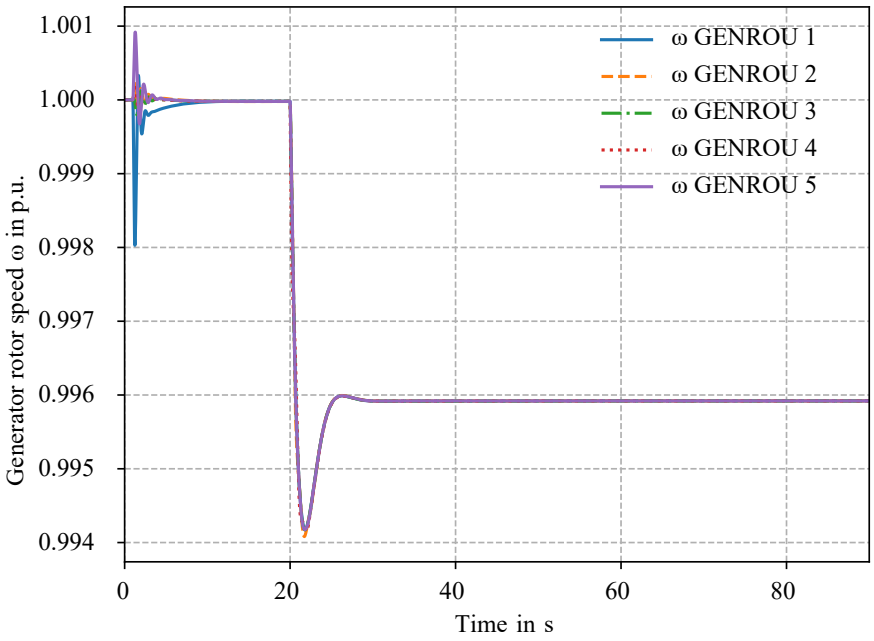


Figure 7.8: Simulated generator rotor speed ω for S1

A scenario without any FRR is not realistic and merely serves as a reference case. In that light, Scenario 1 demonstrates two important parts of frequency control: For one, within the first milliseconds after the disturbance occurs, the frequency of all generators drops as the required energy to supply the increased electrical load is taken and converted from the kinetic energy stored in the generators' rotational inertia. Secondly, to compensate for the increased load, the turbine governors increase their output setpoint for all turbines so that the mechanical input power and electrical output power of the generators are temporarily balanced again. The equal contribution of all generators after $t = 20s$ to FCR, which is not subject to economic optimisation, can be taken from Fig. 7.9.

Even though the shown FCR process successfully contains the frequency drop, an acceptable frequency must still be restored and the resources that enable the provision of FCR need to be made available again in case of further disturbances.

7.2.2 Scenario 2: Ideal Communication

In Scenario 2 (S2), a positive step in the active power consumption on Bus 6 of the power system is chosen as the main disturbance once again. In contrast to S1, all

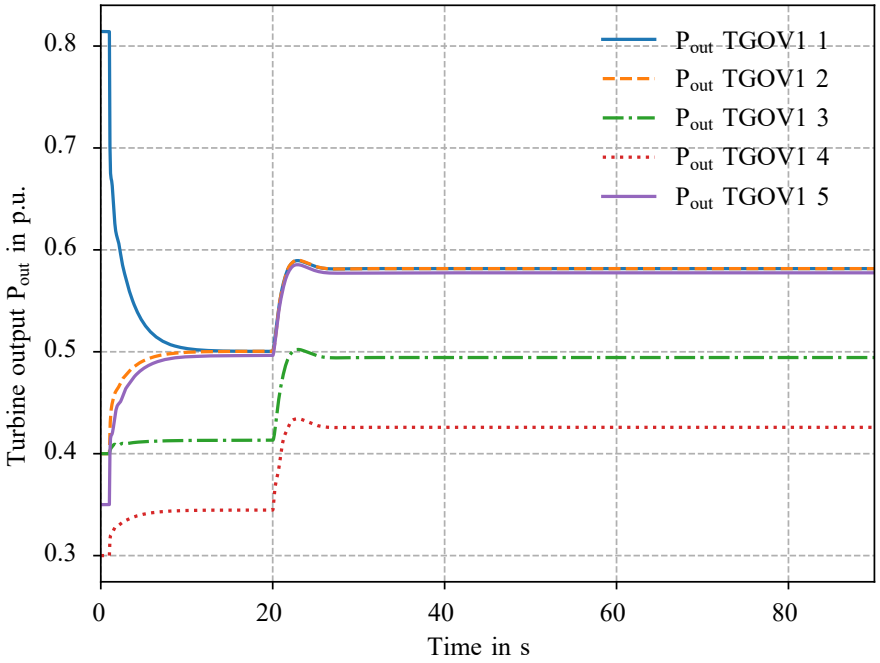


Figure 7.9: Simulated turbine output P_{out} for S1

generators are set to also provide FRR upon a centrally coordinated activation call that is assumed to be transmitted successfully, here. The first $30s$ of the simulation are set up identically to S1. At $t = 30s$ measurements are taken and forwarded to the decision-making instance. This instance is implemented based on an AC-OPF as previously suggested. At $t = 40s$, the setpoints for the generators' active power output and voltage that result from the OPF are fed back into the dynamic simulation. Both, the time until the first set of measurements is taken and the duration of the communication and decision-making processes have been chosen arbitrarily here. Finally, the dynamic simulation is continued for another 50 seconds. The resulting generator rotor speed and turbine output are plotted in Fig. 7.10 and Fig. 7.11, respectively:

As Scenario 1 indicated, FCR alone is inadequate and not designed to handle disturbances without further actions, which is why providers of FRR are activated next. This can be seen at $t = 40s$ in the plots. The OPF and the measurement and control data, which are assumed to be transmitted successfully in this scenario, resulted in new setpoints for all generators' active power output and voltages. The fact that all generators operate at their nominal frequency again from $t \approx 50s$ onward proves the OPF-based and centrally coordinated FRR service to work as intended assuming ideal communication.

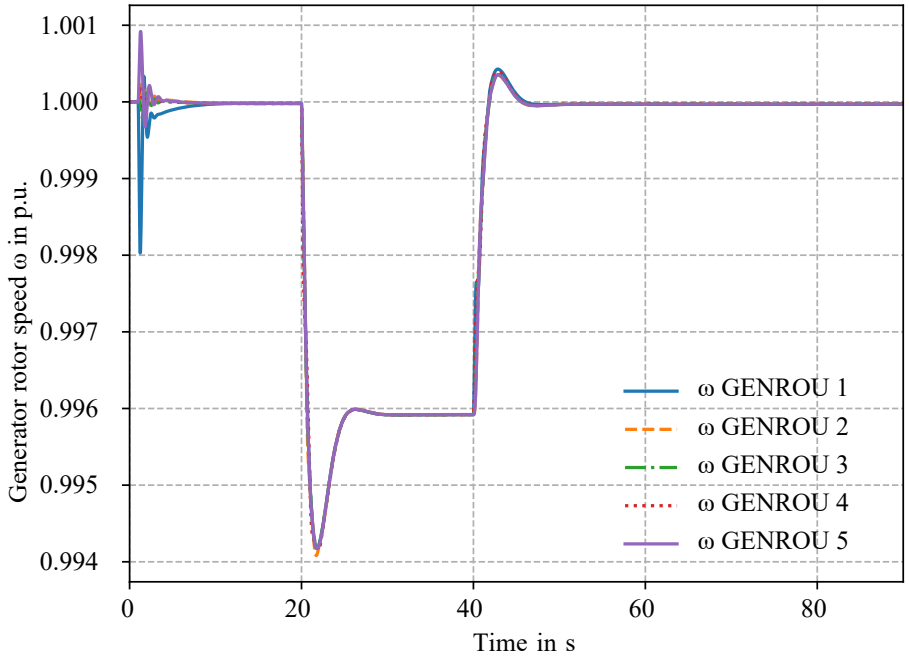


Figure 7.10: Simulated generator rotor speed ω for S2

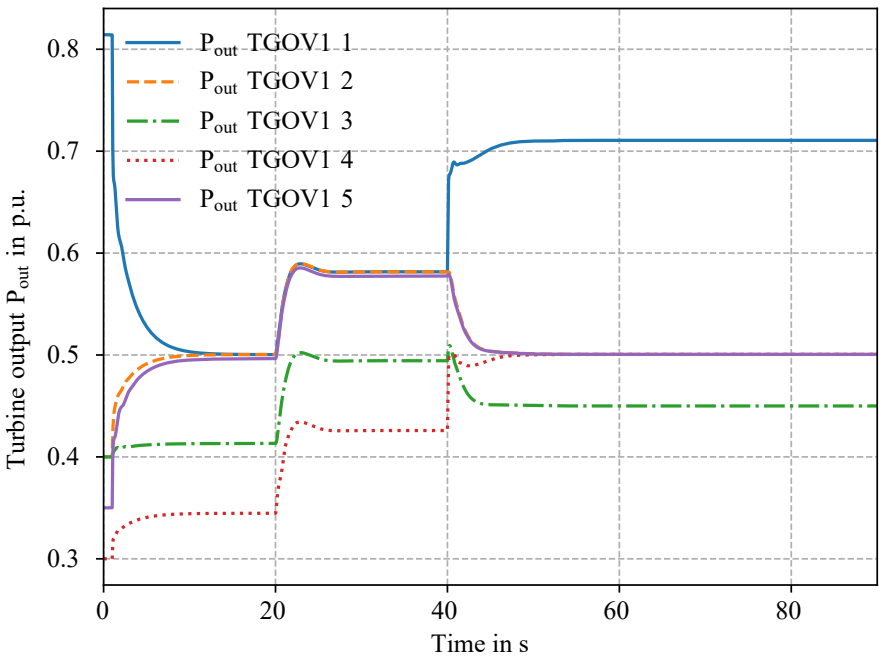


Figure 7.11: Simulated turbine output P_{out} for S2

7.2.3 Scenario 3: Degraded Communication

As a follow-up to the previous scenario, a communication-based problem is added to the otherwise unchanged setup. More specifically, it is assumed that TGOV1 4, the turbine governor of synchronous generator GENROU 4, is not receiving the OPF-based FRR-activation call at $t = 40s$, leading to this one generator not providing FRR. While this can theoretically be considered a potential consequence of data loss, it is also an artificial scenario assuming an unrealistically poorly designed communication system and protocols. Scenario 3 is split into two parts with different system behaviours. For the first sub-scenario (S3A), the communication problem is assumed to be temporary and will therefore only affect the first set of transmitted setpoints to GENROU 4. A second iteration of the operator's decision and control process is introduced to address the inadequate performance of the first FRR-activation call and activate the FRR-provision of GENROU 4. As in Scenario 2, detecting the mismatch in FRR at $t = 50s$ and retransmitting the activation call is assumed to take another $20s$. Thus, the second activation call is ultimately received by GENROU 4 at $t = 60s$. The resulting generator rotor speed can be taken from Fig. 7.12.

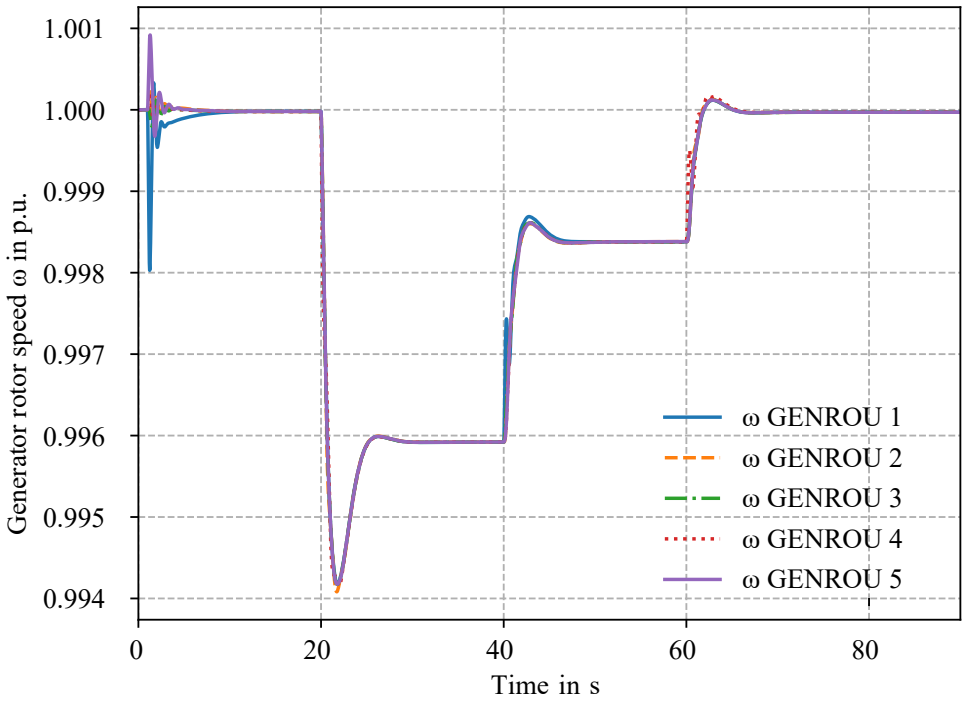


Figure 7.12: Simulated generator rotor speed ω for S3

At $t \approx 65s$, the generators are successfully brought back to nominal operation frequency approximately five seconds after the updated setpoints were received. This meets the expectations and indicates a sufficiently stable operation of the system. Yet, a more substantial delay in the activation call's retransmission might exacerbate problems. Fig. 7.13 presents acceptable voltage levels on all busses and at all times, once again for S3A.

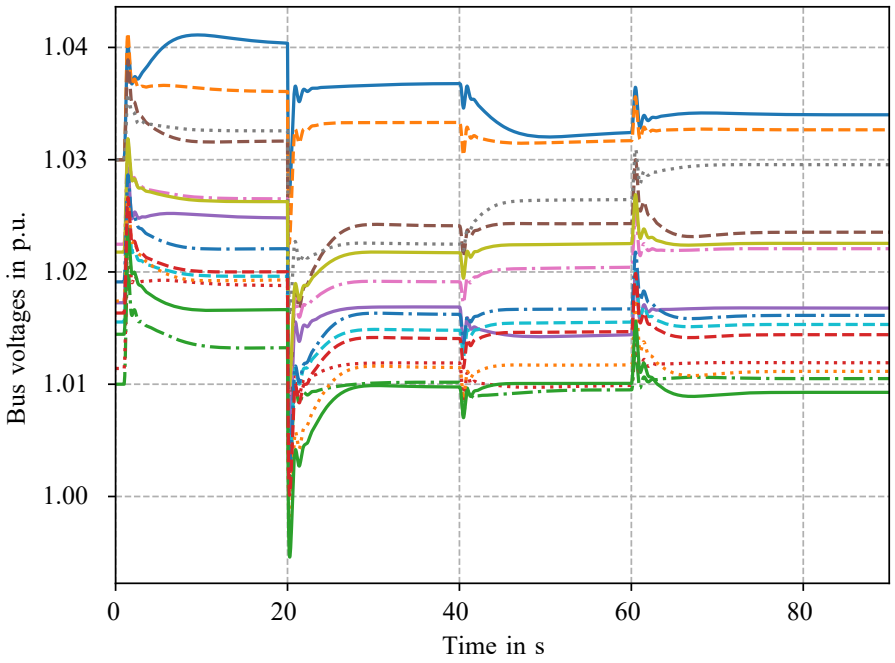


Figure 7.13: Simulated bus voltages for S3A

For the second sub-scenario (S3B), the communication route to GENROU 4 is assumed to be permanently broken but the operator's awareness of this issue is given, too. The OPF is changed in order to capture the uncontrollability of the affected generator by fixing its setpoints to the last known value and reducing its flexibility range to zero. The expected outcome of this case is for other generators to compensate for the unresponsive generator. Comparing the generators' simulated turbine outputs for S3A and S3B, this expectation can be confirmed. While Fig. 7.14 shows the expected activation delay of TGOV1 4, Fig. 7.15 indicates TGOV1 1 compensating for the lack in provided FRR. The simulated frequencies and voltages for S3B are very similar to those for S3A. The according plots are omitted as they would be visually identical to Fig. 7.12 and Fig. 7.13, respectively and would not provide relevant information in the context of these demonstrations.

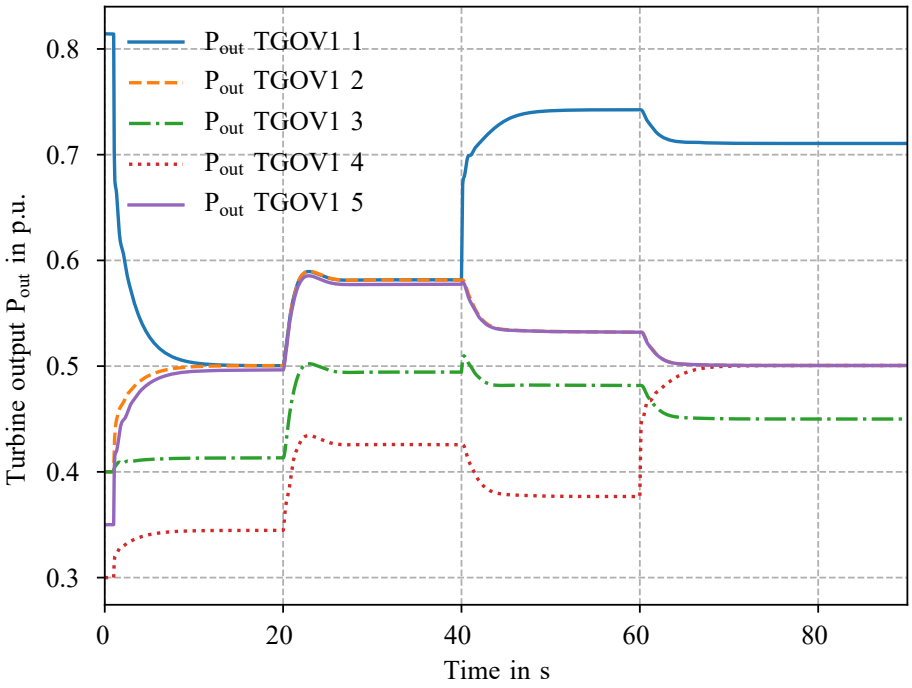


Figure 7.14: Simulated turbine output P_{out} for S3A

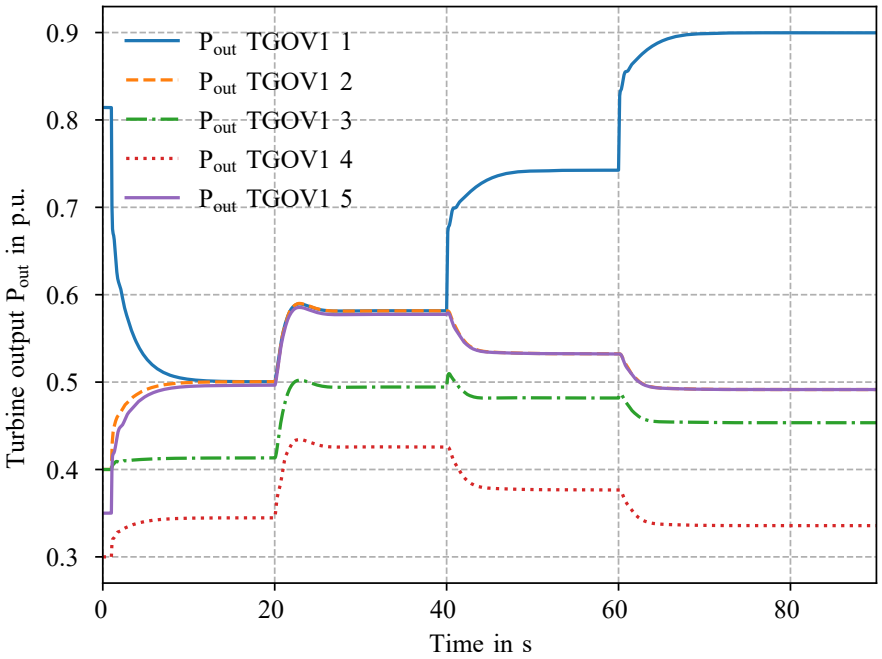


Figure 7.15: Simulated turbine output P_{out} for S3B

7.3 Relevance of Dynamic Phenomena in CPES Stability Studies

The previously shown examples S1 - S3 are meant to demonstrate the changes outlined in Chapter 7.1 to work as intended. This is why – in this case – arbitrarily chosen fixed delay times for communication and data processing are acceptable. While FRR providers are required to start their provision within 30 seconds after the activation call, the demanded full activation time is 5 minutes. Within the scope of ICT-based stability risks, neither of these requirements is threatened by typical communication delays or even retransmission attempts as shown in S3A. While specific hard- or software faults might still cause data processing times to push the activation time for some generators beyond the 30-second threshold, imminent power system instability is not to be expected under realistic circumstances assuming adequate system designs. Instead, generator protection mechanisms concerning under- and over-frequency protection must be checked against the resulting activation time and the share of delayed FRR. In scenarios with one tripping generator triggering a tripping cascade due to sustained frequency deviations, delay-focused analyses might turn relevant, though. According to [79], an initial tripping event can be triggered within seconds to minutes, depending on the magnitude of the sustained deviation. Furthermore, the tighter timing requirements for FCR provision would theoretically impose a more substantial threat to power system stability. In nowadays power systems, though, FCR provision does not only work without the exchange of data but remote communication is typically avoided completely by design to mitigate all communication-based risks. Thus, similar conclusions can be drawn for all three ICT error categories. Only if this design principle was to change, the relevance of ICT-focused FCR analyses in the context of ICT-degradation would increase. While this change is unlikely, it might come as a consequence of decentralisation and the resulting increase in unit coordination complexity. For example, taking sufficiently exact frequency measurements for FCR requires expensive hardware. Hence, most small-scale DERs might only be able to contribute to FCR via remotely communicated measurements or activation calls as shown in Chapter 7.2. It is unclear, though, whether this inclusion of small-scale DERs will even be necessary for the stable operation of future energy systems in the first place. Despite being a rather unlikely scenario, particularly in the in the near future, other technologies such as a new generation of nuclear (fusion) reactors, might render the necessity for DER-coordination and automation obsolete.

About voltage stability and voltage control, similar results are expected: Voltage collapses that unfold within a few seconds can theoretically come as a consequence of temporarily supportive transformer and load behaviour after a disturbance. For example, an OLTC in a low-voltage grid might take some seconds to readjust its tap position after an external voltage drop, leading to all voltage-dependent loads connected to the low-voltage area to mitigate consequences until the OLTC has reached the new tap position. This dynamic voltage-depending behaviour of loads has been shown for example in [80]. The resulting timescale for such a potential voltage collapse to unfold can be as short as a few seconds. Theoretically, this would place this type of voltage collapse on the correct timescale for communication-based risk assessments. Yet, in real power systems, automated voltage regulators would not rely on any remote communication and would still react appropriately and sufficiently fast. One could argue again, that with increasing decentralisation the responsibility for maintaining voltage levels might move to DERs. Assuming these DERs to be a less adequate substitute for conventional power plants would imply improper and unreasonable system design, though. Still, if DERs are to become the main contributors to voltage control and if their control schemes are to depend on remote communication, ICT-based risk analyses would be due.

In general, ICT-induced risks to dynamic power system stability primarily unfold on the service level, as shown in Chapter 4.1.1. On the power system level, dynamic phenomena are conventionally met with autonomous control systems that do not rely on remote communication by design. If this is to change, dynamic stability assessments in the context of ICT-based risks become relevant. Until then, assessing a service's sensitivity to ICT errors under consideration of dynamic system behaviour and considering the resulting performance degradation via service states in static stability studies is sufficient.

Yet, there might be another positive aspect to using the dynamic simulations in the context of this work's method: The state trajectories that result from static analyses are bound to be interpreted as event-based updates of the CPES because there is no information about the absolute time between state snapshots. In contrast to that, the method for dynamic phenomena provides time-continuous simulation results. These allow for much more frequently updated system and service states and therefore a severely increased level of detail. This quasi-continuous state trajectory can then be used to derive quantitative robustness or resilience metrics instead of the previously described qualitative comparisons based on time-discrete state trajectories. Such

metrics have been the focus of recent research works as for example shown in [81, 82] or [83]. The authors of these works either propose metrics that partially leverage the added information provided by time-continuous simulations or at least confirm the potential value of doing so. While most robustness and resilience metrics focus on the temporary unavailability or failure and repair rates of systems' components, the more abstract concept of CPES and service states, especially under consideration of dynamics, might be a good fit for a new type of metric.

This Chapter's Core Insights

- The previously presented method for static CPES stability analyses can be extended to also capture dynamic behaviour in power system stability assessments.
- Additional measurements, such as generator rotor speeds representing grid frequency, can be used as extended input for operator decision-making.
- The relevance of dynamic considerations with regard to communication problems is low in current energy systems, though. Considering dynamic aspects on the service level only and conducting static stability assessments with appropriate service states as input is sufficient.
- The relevance of dynamic considerations might increase with changes in future power systems due to their increased dependence on distributed flexibility services and their timely response.
- The resulting time-continuous state trajectories might still be beneficial for the development of new, less component-focused resilience metrics for CPES.

8 Conclusion

8.1 Summary

In this thesis, the origin and extent of ICT-based stability risks in CPESs have been investigated. This is done in light of the growing total demand for electrical energy on the one side and the increasing complexity of future power systems with decentralised generation and more frequent grid congestions on the other. As physical grid expansion is expected to be too expensive as the sole solution to these challenges, operators and regulators strive for improved coordination of modern assets as a complementary approach and a means to secure the future provision of ancillary services. This coordination relies on the successful exchange and processing of data in many cases. Hence, the very services that are supposed to become increasingly important for the stability of power systems will also be increasingly vulnerable to ICT-induced risks.

The first core result and answer to the first research question of this work lie in the cyber-physical services that have been identified as the primary driver of interdependence in CPESs in Chapter 3. While these services provide increasingly critical functionalities to power system operators, their performance is directly tied to the availability, timeliness and correctness of remotely exchanged data. This dependency on data in general as well as a state description for evaluating the expected service response based on ICT performance indicators have been explained and demonstrated in Chapter 4.

Next, the second research question and thus the effect of degraded service performance on a power system's stability was addressed. In this regard, a modular method comprising eleven steps has been presented and described in detail in Chapter 5. This method takes in a power system, an ICT system, disturbances that are supposed to stress the combined CPES, and, finally, a set of centrally coordinated services meant to handle said disturbances. From these inputs, the immediate physical response of the power system is evaluated first. Then, the operator's perceived system view, which is potentially flawed by bad measurements, is derived and the decision-making process is emulated under consideration of all information assumed available to the operator, including SE results and service states. Finally, the operator's centrally coordinated control decisions for all services are reintroduced into the power system simulation

with regard to a potentially degraded ICT system performance. Not only can this method be applied to assess static power system stability under consideration of ICT errors, but with the extensions presented in Chapter 7, dynamic stability phenomena can be included, as well.

When both the operational state of the power system as well as the states of all services are assessed at specific steps of the method, the so-called state trajectory can be derived. Such a state trajectory qualitatively summarises the CPES stability or threat level and overall robustness against the introduced disturbances. State trajectories from different simulations with varying system designs and service setups can be used to compare these configurations and their impact on the CPES's stability in a qualitative manner as demonstrated by the case study in Chapter 5.3.1. The process of comparing and evaluating different CPES configurations was then improved with the introduction of the quantitative CPES stability metrics in Chapter 6. These metrics are based on the loss of load (LOL) and load at risk (LAR), which are calculated at different points in time and provide a quantitative alternative to the previously introduced CPES state trajectory. Thereby, the third and last research question which focused on how to compare different CPES system designs regarding their stability was addressed, too.

The resulting method can generally be applied in CPES planning for assessing alternative system and service configurations and their impact on the CPES' stability. This includes the comparison of different communication technologies, networks and control schemes on the one hand, but also different conventional power system expansions like additional lines or upgraded transformers on the other. The results can, among others, be used to decide where higher investment costs might be justified with regard to the corresponding system stability improvement. Hence, they can also be used as an indicator of where increased control and coordination capacities are sufficient and where conventional grid expansion is inevitable. Furthermore, the proposed service states can theoretically be introduced in CPES operation and be visualised and frequently updated for human operators. The added information can serve as an early warning signal for impending system threats or at least prepare the operator for degraded service performance.

8.2 Critical Acclaim

As claimed in Chapter 1.3, the method presented in this work introduces a high level of abstraction in order to enable broad application while retaining sufficient details regarding the interconnections between ICT and power system domains. It does so by combining the results of both bottom-up and top-down approaches. More specifically, the service-specific in-depth studies allow for the interdependencies to be captured and considered in high detail. The introduced service states then enable an improved level of abstraction and generalisation on the one hand and a way to integrate the knowledge about service-based interdependencies into conventional, scalable stability assessment approaches, on the other. Yet, said abstraction is based on a set of assumptions and simplifications which imply several limitations for the presented method, as well. The four most critical limitations and drawbacks are outlined next.

The abstraction of ICT details on a service level into service states not only allows researchers to isolate the assessment of dynamic stability assessments and thereby avoid dynamic co-simulations, but it also implies two problems: For one, it can be challenging to map complex services and their various levels of degraded performance to the proposed three service states. In this thesis, services were simplified into generic providers of flexibilities in many cases. While this might ultimately be close to what the majority of future services will behave like, there are also completely different services. Two examples of such different services are the SE and OLTC-based voltage control shown in Chapter 4.3.1. Yet, for other services, the mapping from basic ICT performance indicators like latency to an aggregated state for the expected service performance might be more challenging or even impossible. The second problem with this simplification concerns the effort required for running bigger-scale analyses with many different services in different grids. In Chapter 4.1, it is said that all services' sensitivities to ICT errors need to be known or assessed individually before an aggregated assessment on the CPES-level can be conducted. This requirement poses a challenge if large systems with many different services and implementations are being considered. Having to analyse all services' sensitivities upfront therefore limits the scalability of the method.

A further simplification is about the demonstrated emulation of the operator's decision-making process via OPF. The OPF was introduced as a mere example of how to implement this decision-making and this comes with some limitations on its own: First, using an OPF implies optimal economic acting while disregarding many criti-

cal market mechanisms. Second, not all service actions might be able to be translated into OPF changes. In this work, only changes that affect the power flow at specific buses and very basic topology changes have been considered and the latter already results in an increased amount of OPF iterations and therefore a scalability problem. This simplification furthermore means that the OPF can only make decisions based on static stability considerations. This limitation can be partially lifted by manual consideration of frequency measurements and an accordingly adapted OPF as shown in Chapter 7.1, but this workaround is not guaranteed to work for all dynamic phenomena.

The third major drawback of the presented approach originates from the questionable relevance of dynamic stability assessments in the context of ICT-based risks in today's power systems. This issue, which might be resolved with a change in future power systems' requirements, has been discussed in detail in Chapter 7.3.

The final noteworthy simplification does not affect the core method but the subsequent quantification approach presented in Chapter 6. More specifically, the suggested process for deriving the LAR implies that all buses and lines that are identified as critical in contingency analysis are assumed to shut down simultaneously. This, of course, is only rarely required in reality because the shedding of some load would already improve the condition of most remaining critical assets. Yet, the chosen approach is aligned with the operators' worst-case way of thinking and is sufficiently accurate for comparing different CPES designs in diverse disturbance scenarios.

8.3 Outlook

As for future consecutive work, the main open task is to validate the claims on the general applicability of the presented method. While the provided examples and case studies concern different power systems and services, they are only meant to demonstrate the method as proof of concept and indicate basic adaptivity, but they do not validate the method's general applicability.

Additionally, a more detailed way to quantify the impact of different CPES designs on the system's stability would be a great contribution to this field of research. On the level of services, this task is addressed by Anand Narayan's PhD thesis. Yet, on the higher CPES-level, the presented metrics LOL and LAR can be considered too focused on the electrical load aspect of the CPES. The definition of more comprehensive stability and resilience metrics is an ongoing task and could benefit from the

presented concepts of the more abstract CPES and service states as well as from the consideration of power system dynamics, as briefly outlined in Chapter 7.3.

Furthermore, in all examples in this work, the sensitivity of services to ICT errors was assessed with a single error type at a time. It stands to reason, though, that a combination of multiple simultaneous ICT errors, e.g. data loss and corruption, might lead to a service's performance deteriorating long before a single error type would. Hence, analyses for combined ICT error types and their impact on the performance of services are recommended for future work, too.

Last, this work focuses on simulation-based stability assessments of CPESs. An analytical approach for including service-based interdependencies in established dynamic stability studies could be another logical next step. While corresponding first attempts based on modelling CPES and cyber-physical services as a combination of hybrid and finite-state automata have been presented in [MK7], the full analytical approach outgrew the scope of this work due to its late stage and the high level of complexity.

References

[1] IEA - International Energy Agency. "World Energy Outlook 2019". In: *International Energy Agency, Paris* (2019). URL: iea.blob.core.windows.net/assets/98909c1b-aabc-4797-9926-35307b418cdb/WEO2019-free.pdf (cit. on p. 1).

[2] O. Ruhnau, S. Bannik, S. Otten, A. Praktiknjo, and M. Robinius. "Direct or indirect electrification? A review of heat generation and road transport decarbonisation scenarios for Germany 2050". In: *Energy* 166 (2019), pp. 989–999 (cit. on p. 1).

[3] P. J. Baruah, N. Eyre, M. Qadrdan, M. Chaudry, S. Blainey, J. W. Hall, N. Jenkins, and M. Tran. "Energy system impacts from heat and transport electrification". In: *Proceedings of the Institution of Civil Engineers-Energy* 167.3 (2014), pp. 139–151 (cit. on p. 1).

[4] S. Bellocchi, M. Manno, M. Noussan, M. G. Prina, and M. Vellini. "Electrification of transport and residential heating sectors in support of renewable penetration: Scenarios for the Italian energy system". In: *Energy* 196 (2020) (cit. on p. 1).

[5] M. Buck, A. Graf, and P. Graichen. "Agora Energiewende (2019): European Energy Transition 2030: The Big Picture". In: (2019) (cit. on pp. 1–2).

[6] K. Rauma, A. Funke, T. Simolin, P. Järventausta, and C. Rehtanz. "Electric Vehicles as a Flexibility Provider: Optimal Charging Schedules to Improve the Quality of Charging Service". In: *Electricity* 2.3 (2021), pp. 225–243. DOI: 10.3390/electricity2030014 (cit. on p. 1).

[7] F. Salah, J. P. Ilg, C. M. Flath, H. Basse, and C. Van Dinther. "Impact of electric vehicles on distribution substations: A Swiss case study". In: *Applied Energy* 137 (2015), pp. 88–96 (cit. on p. 1).

[8] C.-H. Lo and N. Ansari. "Decentralized Controls and Communications for Autonomous Distribution Networks in Smart Grid". In: *IEEE Transactions on Smart Grid* 4.1 (2013), pp. 66–77. DOI: 10.1109/TSG.2012.2228282 (cit. on p. 1).

[9] G. Joos, B. Ooi, D. McGillis, F. Galiana, and R. Marceau. "The potential of distributed generation to provide ancillary services". In: *2000 Power Engineering Society Summer Meeting*. Vol. 3. 2000, 1762–1767 vol. 3. DOI: 10.1109/PESS.2000.868792 (cit. on p. 1).

[10] K. E. Bakari and W. L. Kling. "Virtual power plants: An answer to increasing distributed generation". In: *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*. 2010, pp. 1–6. DOI: 10.1109/ISGTEUROPE.2010.5638984 (cit. on p. 1).

[11] *Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU*. Accessed: March 14, 2023. URL: data.europa.eu/eli/dir/2019/944/oj (cit. on pp. 1, 20).

[12] CEDEC, EDSOE, ENTSO-E, Eurelectric, and G. TSO-DSO. *TSO-DSO Report. An Integrated Approach to Active System Management*. 2019 (cit. on p. 2).

[13] I. Dumitrache, N. Constantin, and O. Stoica. "Some Challenges for the Cyber – Physical Energy System". In: *IFAC Proceedings Volumes* 46.6 (2013). 2nd IFAC Workshop on Convergence of Information Technologies and Control Methods with Power Systems, pp. 1–6. DOI: https://doi.org/10.3182/20130522-3-RO-4035.00045 (cit. on p. 2).

[14] I. A. Tøndel, J. Foros, S. S. Kilskar, P. Hokstad, and M. G. 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. DOI: https://doi.org/10.1016/j.aci.2017.01.001 (cit. on pp. 2, 4).

[15] Y.-K. Wu, S. M. Chang, and Y.-L. Hu. "Literature review of power system blackouts". In: *Energy Procedia* 141 (2017), pp. 428–431 (cit. on p. 2).

[16] P. Kundur. "Power system stability". In: *Power system stability and control* (2007), pp. 7–1 (cit. on pp. 3, 9).

[17] E. Handschin and A. Petroianu. *Energy management systems: operation and control of electric energy transmission systems*. Springer Science & Business Media, 2012 (cit. on p. 3).

[18] J.-C. Laprie, K. Kanoun, and M. Kaâniche. “Modelling Interdependencies Between the Electricity and Information Infrastructures”. In: *Computer Safety, Reliability, and Security*. Ed. by F. Saglietti and N. Oster. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 54–67. ISBN: 978-3-540-75101-4 (cit. on p. 3).

[19] M. Panteli and D. S. Kirschen. “Assessing the effect of failures in the information and communication infrastructure on power system reliability”. In: *2011 IEEE/PES Power Systems Conference and Exposition*. 2011, pp. 1–7. DOI: 10.1109/PSCE.2011.5772565 (cit. on pp. 3–4, 31).

[20] M. Panteli, P. A. Crossly, and D. S. Kirschen. “A multi-state model for assessing the impact of insufficient Wide-area Situational Awareness”. In: *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*. 2012, pp. 1–6. DOI: 10.1049/cp.2012.0031 (cit. on p. 4).

[21] M. Panteli, P. A. Crossley, D. S. Kirschen, and D. 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. DOI: 10.1109/TPWRS.2013.2240705 (cit. on pp. 4–5).

[22] J. Wäfler and P. E. Heegaard. “Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability”. In: *Advances in Communication Networking*. Ed. by T. Bauschert. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 185–196. ISBN: 978-3-642-40552-5 (cit. on pp. 4, 29, 43).

[23] J. Wäfler and P. E. Heegaard. “A Combined Structural and Dynamic Modelling Approach for Dependability Analysis in Smart Grid”. In: SAC ’13. Coimbra, Portugal: Association for Computing Machinery, 2013, 660–665. ISBN: 9781450316569. DOI: 10.1145/2480362.2480489 (cit. on p. 4).

[24] J. Wäfler and P. E. Heegaard. “Interdependency in smart grid recovery”. In: *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. 2015, pp. 201–207. DOI: 10.1109/RNDM.2015.7325230 (cit. on p. 4).

[25] J. Wäfler. “Modeling and Analysis of Dependability and Interdependency Failures in Smart Grids: Study on how the wide usage of ICT changes the Dependability in the future Power Grid”. In: (2016) (cit. on p. 4).

[26] "Historical Reliability Data for IEEE 3006 Standards: Power Systems Reliability". In: *3006HistoricalData-2012 Historical Reliability Data for IEEE 3006 Standards* (2012), pp. 1–303. DOI: 10.1109/IEEESTD.2012.6745993 (cit. on p. 5).

[27] J. A. Hussein and A. R. Majeed. "Reliability Study of Regional Power Network Communication". In: *2006 IEEE/PES Transmission & Distribution Conference and Exposition: Latin America*. 2006, pp. 1–6. DOI: 10.1109/TDCLA.2006.311632 (cit. on p. 5).

[28] K. Heussen and M. Lind. "Decomposing objectives and functions in power system operation and control". In: *2009 IEEE PES/IAS Conference on Sustainable Alternative Energy (SAE)*. 2009, pp. 1–8. DOI: 10.1109/SAE.2009.5534873 (cit. on p. 9).

[29] K. Kollenda, A. Schrief, C. Biele, M. Lindner, N. Sundorf, A. Hoffrichter, A. Roehder, A. Moser, and C. Rehtanz. "Curative measures identification in congestion management exploiting temporary admissible thermal loading of overhead lines". In: *IET Generation, Transmission & Distribution* (2022) (cit. on pp. 10, 13).

[30] *European Union (EU) Commission Regulation 2017/1485 - Establishing a Guideline on Electricity Transmission System Operation*. Accessed: March 14, 2023. URL: data.europa.eu/eli/reg/2017/1485/oj (cit. on pp. 10, 16, 18–19, 33, 39, 98).

[31] *E DIN EN 50160:2022-10*. DIN e.V., 2022 (cit. on p. 11).

[32] *UCTE Operations Handbook - Appendix 1: Load-Frequency Control and Performance*. UCTE, 2004. URL: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/Operation_Handbook/Policy_1_Appendix\%20_final.pdf (cit. on p. 11).

[33] *Commission Regulation (EU) 2016/631 of 14 April 2016 establishing a network code on requirements for grid connection of generators (Text with EEA relevance)*. 2016 (cit. on p. 11).

[34] "Manual on System Restoration". In: (2022). URL: https://www.pjm.com/-/media/documents/manuals/m36.ashx (cit. on p. 11).

[35] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal. "Definition and classification of power system stability IEEE". In: *IEEE Transactions on Power Systems* 19.3 (2004), pp. 1387–1401. DOI: 10.1109/TPWRS.2004.825981 (cit. on pp. 12, 15).

[36] N. Hatziargyriou, J. Milanović, C. Rahmann, V. Ajjarapu, C. Cañizares, I. Erlich, D. Hill, I. Hiskens, I. Kamwa, B. Pal, P. Pourbeik, J. Sanchez-Gasca, A. Stanković, T. Van Cutsem, V. Vittal, and C. Vournas. *Stability definitions and characterization of dynamic behavior in systems with high penetration of power electronic interfaced technologies*. English. IEEE PES Technical Report PES-TR77. IEEE, April 2020. URL: https://resourcecenter.ieee-pes.org/ (cit. on p. 12).

[37] N. Hatziargyriou, J. Milanovic, C. Rahmann, V. Ajjarapu, C. Canizares, I. Erlich, D. Hill, I. Hiskens, I. Kamwa, B. Pal, et al. "Definition and classification of power system stability–revisited & extended". In: *IEEE Transactions on Power Systems* 36.4 (2020), pp. 3271–3281 (cit. on pp. 12–14).

[38] P. Sauer and M. Pai. "Power system dynamics and stability". In: *SERBIULA (sistema Librum 2.0)* (Jan. 2008) (cit. on p. 13).

[39] H. K. Khalil. *Nonlinear systems; 3rd ed.* The book can be consulted by contacting: PH-AID: Wallet, Lionel. Upper Saddle River, NJ: Prentice-Hall, 2002. URL: https://cds.cern.ch/record/1173048 (cit. on p. 15).

[40] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter. "Bad data analysis for power system state estimation". In: *IEEE Transactions on Power Apparatus and Systems* 94.2 (1975), pp. 329–337. DOI: 10.1109/T-PAS.1975.31858 (cit. on p. 17).

[41] A. Abur and A. G. Exposito. *Power system state estimation: theory and implementation*. CRC press, 2004 (cit. on p. 17).

[42] *Systemschutzplanplan der vier deutschen Übertragungsnetzbetreiber*. 50hertz, Amprion, Tennet, Transnet BW. 2021 (cit. on pp. 17, 64).

[43] *European Union (EU) Commission Regulation 2017/2196 - Establishing a Network Code on Electricity Emergency and Restoration*. Accessed: March 14, 2023. URL: data.europa.eu/eli/reg/2017/2196/oj (cit. on pp. 18–19, 64).

[44] V. Aravinthan, T. Balachandran, M. Ben-Idris, W. Fei, M. Heidari-Kapourchali, A. Hettiarachchige-Don, J. N. Jiang, H. Lei, C.-C. Liu, J. Mitra, M. Ni, M. Papic, M. Parvania, M. Sephary, C. Singh, A. Srivastava, A. Stefanov, H. Sun, and S. Tindemans. "Reliability Modeling Considerations for Emerging Cyber-Physical Power Systems". In: *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. 2018, pp. 1–7. DOI: 10.1109/PMAPS.2018.8440331 (cit. on p. 21).

[45] *Network Code on Emergency and Restoration - Implementation Guide for the Communication Systems Requirements*. ENTSO-E, 2018 (cit. on p. 22).

[46] T. Sauter and M. Lobashov. "End-to-End Communication Architecture for Smart Grids". In: *IEEE Transactions on Industrial Electronics* 58.4 (2011), pp. 1218–1228. DOI: 10.1109/TIE.2010.2070771 (cit. on pp. 22, 35).

[47] V. Gungor and F. Lambert. "A survey on communication networks for electric system automation". In: *Computer Networks* 50.7 (2006), pp. 877–897. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2006.01.005 (cit. on pp. 23, 26).

[48] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. "A Survey on Cyber Security for Smart Grid Communications". In: *IEEE Communications Surveys & Tutorials* 14.4 (2012), pp. 998–1010. DOI: 10.1109/SURV.2012.010912.00035 (cit. on pp. 23, 26).

[49] "Schutz- und Automatisierungstechnik in aktiven Verteilnetzen". In: (2016) (cit. on p. 23).

[50] G. López, J. Matanza, D. De La Vega, M. Castro, A. Arrinda, J. I. Moreno, and A. Sendin. "The Role of Power Line Communications in the Smart Grid Revisited: Applications, Challenges, and Research Initiatives". In: *IEEE Access* 7 (2019), pp. 117346–117368. DOI: 10.1109/ACCESS.2019.2928391 (cit. on p. 26).

[51] A. Colella, A. Castiglione, and C. M. Colombini. "Industrial Control System Cyber Threats Indicators in Smart Grid Technology". In: *2014 17th International Conference on Network-Based Information Systems*. 2014, pp. 374–380. DOI: 10.1109/NBiS.2014.129 (cit. on p. 26).

[52] S. Saadat, S. Bahizad, T. Ahmed, and S. Maingot. “Smart Grid and Cyber-security Challenges”. In: *2020 5th IEEE Workshop on the Electronic Grid (eGRID)*. 2020, pp. 1–8. DOI: 10.1109/eGRID48559.2020.9330660 (cit. on p. 26).

[53] M. Wagner, M. Kuba, and A. Oeder. “Smart grid cyber security: A German perspective”. In: *2012 International Conference on Smart Grid Technology, Economics and Policies (SG-TEP)*. 2012, pp. 1–4. DOI: 10.1109/SG-TEP.2012.6642389 (cit. on p. 26).

[54] S. Clements and H. Kirkham. “Cyber-security considerations for the smart grid”. In: *IEEE PES General Meeting*. 2010, pp. 1–5. DOI: 10.1109/PES.2010.5589829 (cit. on p. 27).

[55] J. M. Simmons. *Optical network design and planning*. Springer, 2014 (cit. on p. 27).

[56] A. Narayan, B. H. Hassan, S. Attarha, C. Krüger, D. Babazadeh, and S. Lehnhoff. “Grid Function Virtualization for Reliable Provision of Services in Cyber-Physical Energy Systems”. In: *2020 IEEE Power & Energy Society General Meeting (PESGM)*. 2020, pp. 1–5. DOI: 10.1109/PESGM41954.2020.9282006 (cit. on p. 29).

[57] S. Dalhues, L. Robitzky, U. Häger, N. Dorsch, F. Kurtz, and C. Wietfeld. “Analysis of real-time coordination of distributed power flow controllers using software-defined networking communication”. In: *2018 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 2018, pp. 1–5. DOI: 10.1109/ISGT.2018.8403388 (cit. on pp. 29, 66).

[58] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu. “Opportunities and challenges of wireless communication technologies for smart grid applications”. In: *IEEE PES General Meeting*. 2010, pp. 1–7. DOI: 10.1109/PES.2010.5589988 (cit. on p. 35).

[59] T.-T. Tay, I. Mareels, and J. B. Moore. “Adaptive-Q Application to Nonlinear Systems”. In: *High Performance Control*. Springer, 1998, pp. 205–240 (cit. on p. 36).

[60] S. Meinecke, D. Sarajlić, S. R. Drauz, A. Klettke, L.-P. Lauven, C. Rehtanz, A. Moser, and M. Braun. “SimBench—A Benchmark Dataset of Electric Power Systems to Compare Innovative Solutions Based on Power Flow Analysis”. In: *Energies* 13.12 (2020). DOI: 10.3390/en13123290 (cit. on p. 37).

[61] P. Kansal and A. Bose. "Bandwidth and latency requirements for smart transmission grid applications". In: *2013 IEEE Power & Energy Society General Meeting*. 2013, pp. 1–1. DOI: 10.1109/PESMG.2013.6672081 (cit. on p. 45).

[62] M. Kuzlu, M. Pipattanasomporn, and S. Rahman. "Communication network requirements for major smart grid applications in HAN, NAN and WAN". In: *Computer Networks* 67 (2014), pp. 74–88. DOI: https://doi.org/10.1016/j.comnet.2014.03.029 (cit. on p. 45).

[63] C. Oerter and N. Neusel-Lange. "LV-grid automation system — A technology review". In: *2014 IEEE PES General Meeting | Conference & Exposition*. 2014, pp. 1–5. DOI: 10.1109/PESGM.2014.6939827 (cit. on p. 48).

[64] R. Palaniappan, B. Bauernschmitt, D. Hilbrich, and C. Rehtanz. "An Intelligent Measurement and Control Device for Active Distribution Grids". In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. 2020, pp. 975–979. DOI: 10.1109/ISGT-Europe47291.2020.9248862 (cit. on p. 48).

[65] S. N. Salih and P. 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 (2016), pp. 4026–4035. DOI: 10.1109/TPWRS.2015.2501433 (cit. on p. 49).

[66] M. Panteli. *Impact of ict reliability and situation awareness on power system blackouts*. The University of Manchester (United Kingdom), 2013 (cit. on p. 53).

[67] S. Frank, I. Steponavice, and S. Rebennack. "Optimal power flow: a bibliographic survey I". In: *Energy systems* 3.3 (2012), pp. 221–258 (cit. on p. 62).

[68] M. AlRashidi and M. El-Hawary. "Applications of computational intelligence techniques for solving the revived optimal power flow problem". In: *Electric Power Systems Research* 79.4 (2009), pp. 694–702. DOI: https://doi.org/10.1016/j.epsr.2008.10.004 (cit. on p. 65).

[69] N. Dorsch, F. Kurtz, S. Dalhues, L. Robitzky, U. Häger, and C. Wietfeld. "Intertwined: Software-defined communication networks for multi-agent system-based Smart Grid control". In: *2016 IEEE international conference on smart grid communications (SmartGridComm)*. IEEE. 2016, pp. 254–259 (cit. on p. 66).

[70] Y. Wu, L. Nordström, and D. 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. 71).

[71] B. Moussa, P. Akaber, M. Debbabi, and C. 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 p. 71).

[72] L. Thurner, A. Scheidler, F. Schäfer, J. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun. "pandapower — An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems". In: *IEEE Transactions on Power Systems* 33.6 (2018), pp. 6510–6521. DOI: 10.1109/TPWRS.2018.2829021 (cit. on p. 75).

[73] S. Afzal, H. Mokhlis, H. A. Illias, N. N. Mansor, and H. Shareef. "State-of-the-art review on power system resilience and assessment techniques". In: *IET Generation, Transmission & Distribution* 14.25 (2020), pp. 6107–6121. DOI: https://doi.org/10.1049/iet-gtd.2020.0531 (cit. on p. 81).

[74] P. Paliwal, N. P. Patidar, and R. K. Nema. "Probabilistic indices for analysing the impact of penetration of distributed energy resources on system reliability". In: *IET Renewable Power Generation* 14.12 (2020), pp. 2154–2165. DOI: https://doi.org/10.1049/iet-rpg.2019.1214 (cit. on p. 81).

[75] "IEEE Guide for Electric Power Distribution Reliability Indices". In: *IEEE Std 1366-2003 (Revision of IEEE Std 1366-1998)* (2004), pp. 1–50. DOI: 10.1109/IEEESTD.2004.94548 (cit. on p. 81).

[76] P. Tielens and D. Van Hertem. "The relevance of inertia in power systems". In: *Renewable and Sustainable Energy Reviews* 55 (2016), pp. 999–1009. DOI: https://doi.org/10.1016/j.rser.2015.11.016 (cit. on p. 92).

[77] H. Liu, L. Tesfatsion, and A. A. Chowdhury. "Locational marginal pricing basics for restructured wholesale power markets". In: *2009 IEEE Power & Energy Society General Meeting*. 2009, pp. 1–8. DOI: 10.1109/PES.2009.5275503 (cit. on p. 95).

[78] H. Cui, F. Li, and K. Tomsovic. “Hybrid Symbolic-Numeric Framework for Power System Modeling and Analysis”. In: *IEEE Transactions on Power Systems* 36.2 (2021), pp. 1373–1384. DOI: 10.1109/TPWRS.2020.3017019 (cit. on p. 96).

[79] Z. Song, Y. Lin, C. Liu, Z. Ma, and L. Ding. “Review on over-frequency generator tripping for frequency stability control”. In: *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. 2016, pp. 2240–2243. DOI: 10.1109/APPEEC.2016.7779886 (cit. on p. 105).

[80] S. Liemann and C. Rehtanz. “Power Response and Modelling Aspects of Power Electronic Loads in Case of Voltage Drops”. In: *11th Bulk Power Systems Dynamics and Control Symposium (IREP 2022)*. 2022. arXiv: 2207.03965 (cit. on p. 106).

[81] A. Stanković et al. “Methods for Analysis and Quantification of Power System Resilience”. In: *IEEE Transactions on Power Systems* (2022), pp. 1–14. DOI: 10.1109/TPWRS.2022.3212688 (cit. on p. 107).

[82] A. Umunnakwe, H. Huang, K. Oikonomou, and K. Davis. “Quantitative analysis of power systems resilience: Standardization, categorizations, and challenges”. In: *Renewable and Sustainable Energy Reviews* 149 (2021). DOI: https://doi.org/10.1016/j.rser.2021.111252 (cit. on p. 107).

[83] A. A. Ganin, E. Massaro, A. Gutfraind, N. Steen, J. M. Keisler, A. Kott, R. Mangoubi, and I. Linkov. “Operational resilience: concepts, design and analysis”. In: *Scientific reports* 6.1 (2016), pp. 1–12 (cit. on p. 107).

Publications

[MK1] M. Klaes, A. Narayan, A. D. Patil, J. Haack, M. Lindner, C. Rehtanz, M. Braun, S. Lehnhoff, and H. de Meer. "State description of cyber-physical energy systems". In: *Energy Informatics* 3.1 (2020), pp. 1–19. DOI: 10.1186/s42162-020-00119-3 (cit. on pp. 18, 43, 45, 47–49, 61).

[MK2] A. Narayan, M. Klaes, D. Babazadeh, S. Lehnhoff, and C. Rehtanz. "First Approach for a Multi-dimensional State Classification for ICT-reliant Energy Systems". In: *International ETG-Congress 2019; ETG Symposium*. 2019, pp. 1–6. URL: https://ieeexplore.ieee.org/document/8835986 (cit. on p. 28).

[MK3] J. Zwartscholten, M. Klaes, D. M. Gonzalez, F. Subhan, A. Narayan, and C. Rehtanz. "Impact of Increased ICT Latency on Active Distribution Network Control". In: *2020 6th IEEE International Energy Conference (ENERGYCon)*. 2020, pp. 864–869. DOI: 10.1109/ENERGYCon48941.2020.9236511 (cit. on pp. 36, 42).

[MK4] M. Klaes, J. Zwartscholten, A. Narayan, S. Lehnhoff, and C. Rehtanz. "Impact of ICT Latency, Data Loss and Data Corruption on Active Distribution Network Control". In: *IEEE Access* 11 (2023), pp. 14693–14701. DOI: 10.1109/ACCESS.2023.3243255 (cit. on pp. 36, 44–45).

[MK5] B. H. Hassan, A. Narayan, D. Babazadeh, M. Klaes, and S. Lehnhoff. "Performance Assessment of State Estimation in Cyber-Physical Energy Systems". In: *2021 IEEE Madrid PowerTech*. 2021, pp. 1–6. DOI: 10.1109/PowerTech46648.2021.9494760 (cit. on pp. 45–46, 61, 73).

[MK6] A. Narayan, M. Klaes, S. Lehnhoff, and C. 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)*. 2021, pp. 522–529. DOI: 10.1109/EPEC52095.2021.9621496 (cit. on pp. 53, 71).

[MK7] J. Haack, A. Narayan, A. Patil, M. Klaes, M. Braun, S. Lehnhoff, H. de Meer, and C. Rehtanz. "A Hybrid Model for Analysing Disturbance Propagation in Cyber–Physical Energy Systems". In: *Electric Power Systems Research* 212 (2022), p. 108356. DOI: https://doi.org/10.1016/j.epsr.2022.108356 (cit. on pp. 53, 56, 71, 113).

List of Abbreviations

ADN Active Distribution Network

CA Contingency Analysis

CPES Cyber-Physical Energy System

DER Distributed Energy Resource

DSO Distribution System Operator

FCR Frequency Containment Reserve

FRR Frequency Restoration Reserve

ICT Information and Communications Technology

LAR Load at Risk

LOL Loss of Load

LV Low Voltage

OPF Optimal Power Flow

OSL Operational Security Limit

RA Remedial Action

SSL Securely Supplied Loads

SE State Estimation

TSO Transmission System Operator

List of Figures