

RESEARCH

Open Access



Quantifying the resilience of ICT-enabled grid services in cyber-physical energy system

Anand Narayan^{1,2*}, Michael Brand² and Sebastian Lehnhoff^{1,2}

From The 12th DACH+ Conference on Energy Informatics 2023
Vienna, Austria. 4-6 October 2023. <https://www.energy-informatics2023.org/>

*Correspondence:
anand.narayan@offis.de

¹ Carl von Ossietzky University
of Oldenburg, Ammerländer
Heerstraße 114-118,
26129 Oldenburg, Germany
² OFFIS-Institute for Information
Technology, Escherweg 2,
26121 Oldenburg, Germany

Abstract

Information and Communication Technology (ICT) is vital for the operation of modern power systems, giving rise to Cyber-Physical Energy Systems (CPEs). ICT enables the grid services (GSs) needed for monitoring and controlling the physical parameters of the power system, especially for remedying the impact of disturbances. But the ICT integration makes the overall system more complex, leading to new and unforeseen disturbances. This motivates the need for a resilient system design capable of absorbing and recovering from such disturbances. The current state of the art lacks a comprehensive resilience assessment of ICT-enabled GSs in CPEs. To address this, a novel method and metrics to assess the resilience of GSs in CPEs are presented in this paper. An operational state model of a GS, with three states, i.e., normal, limited and failed, is used to capture its performance, which is essential for quantifying its resilience. Sequential Monte Carlo simulations are performed with the model to capture the behaviour of ICT components to compute the operational state trajectory of the GSs. Metrics are then derived to quantify the resilience and its constituting phases. The method is demonstrated using two ICT system designs for the CIGRE MV benchmark grid, considering the state estimation as an exemplary GS. The simulation results show that the proposed method can capture the differences between ICT system designs with regard to resilience metrics. The contribution can, therefore, be used to analyse, compare and potentially improve the resilience of ICT system designs for CPEs.

Keywords: ICT-enabled grid services, Operational states, Monte carlo simulation, Resilience quantification

Introduction

Motivation

Modern power systems are characterized by increased uncertainties due to the penetration of distributed energy resources. Information and Communication Technology (ICT) plays a vital role in such systems as it enhances the monitoring, decision making and control, required for their safe and reliable operation (Tøndel et al. 2018). This results in a strong interdependency between power and ICT systems giving rise to

Cyber-Physical Energy Systems (CPESs). The operation of such a system is carried out using the so-called Grid Services (GSs), which use the ICT hardware and software for sensing, actuation, data transfer and processing. These GSs aid in the detection and remedying of power system disturbances such as line failures, generation fluctuations and over/under voltages. Examples of such ICT-enabled GSs are state estimation (SE), voltage control, congestion management and redispatch (Narayan et al. 2019).

The strong interdependencies between power and ICT systems not only increase the overall complexity of CPESs but can also introduce new threats and vulnerabilities (Jimada-Ojuolape and Teh 2020; Tøndel et al. 2018). Past events have already shown that ICT disturbances can either cause or aggravate disturbances in the power system via the GSs. For example, the 2003 North American blackout was caused by a software problem in the SE service. This gave incorrect situational awareness to the operator leading to incorrect decisions (NERC 2004). The 2013 *Kreisläufer problem* in Austria was caused by large amounts of broadcast data from faulty controllers, causing congestion in the ICT network. This hindered further transmission of measurements and control commands (Schossig and Schossig 2014). The 2015 and 2017 Ukraine blackouts happened due to cyber-attacks targeting the critical GSs in the control room (Whitehead et al. 2017). These events demonstrate that, in addition to power system disturbances, modern CPESs face a wide range of new ICT disturbances, which can impact the performance (or functionality) of GSs and, consequentially, the performance of the whole CPES. This makes it necessary to consider the ICT system and the GSs in the planning and operation of CPESs.

As a safety-critical system, a CPES should be designed to survive, among others, power and ICT disturbances. In this regard, resilience is an emerging concept (acatech/Leopoldina/Akademienunion 2021). In contrast to traditional systems designed to be robust, i.e., to withstand only known and highly probable disturbances, a resilient system should be able to absorb (without failing) and then recover from new and unforeseen disturbances as well (Stanković et al. 2022). This is essential as it is infeasible and costly to harden the CPES against the wide range of disturbances it faces is infeasible and costly. This paper contributes to the design of resilient ICT systems for CPESs by proposing a method to assess the resilience of the ICT-based GSs in CPES.

Related work and research gap

Due to their strong interdependencies, the performance of power and ICT subsystems impacts the performance of the overall CPES (Tøndel et al. 2018). Therefore, designing resilient individual subsystems will improve the resilience of the whole CPES. In acatech/Leopoldina/Akademienunion (2021), Stanković et al. (2022), the concept of CPES resilience is discussed, and ICT-based GSs are identified as one of the important aspects for improving the resilience of CPESs. A comprehensive summary of resilience assessment methods, quantification metrics and improvement strategies are presented in Stanković et al. (2022), Bhusal et al. (2020) and Afzal et al. (2020). They conclude that the quantification and assessment of resilience is still nascent research, which includes a wide range of subtopics such as reliability, robustness, risk and security. Although there exist several resilience metrics and assessment methods in the literature, they are yet to be universally accepted or standardized for CPESs (Bhusal et al. 2020).

Nan and Sansavini (2017) proposed a quantitative resilience assessment using an area-under-curve metric called *measure of performance*. A use case of a Swiss high-voltage grid is presented with available power lines and power demand served as measures of performance. In Nichelle'Le et al. (2021), a resilience metric is derived based on the states of components. These works, however, focus only on the power system and do not explicitly consider the ICT system. ICT components (e.g., smart meters, routers, software) have a faster innovation cycle compared to power system components, because of which ICT components undergo modifications more frequently (Panteli and Mancarella 2015). Consequentially, there exists plenty of options to design ICT systems for CPES. Some design options are summarized in Kuzlu et al. (2014). They include different communication technologies (e.g., cellular, Ethernet, Internet), types of control and decision-making (e.g., central, hierarchical, distributed) and network topology (e.g., radial, meshed, ring). This necessitates investigating the resilience of ICT systems, especially considering different design options.

Regarding the resilience of ICT systems, the authors of Sterbenz et al. (2010) present the ResiliNets framework, where resilience is defined as the area under the curve of a 3×3 state space consisting of operational states and service parameters. However, this is purely conceptual without practical use cases. Patil et al. (2020) uses the ResiliNets framework for analysing the resilience of a CPES. Here, the number of overloaded power lines and the availability of ICT components are used as metrics for the aforementioned service parameter of both power and ICT systems. The authors of Samarajiva and Zuhyle (2013) discuss ICT resilience during natural disasters using metrics such as the number of damaged telecommunication lines and base transceiver stations. Resilience in interdependent power and ICT systems is surveyed in Liu et al. (2020). Here, metrics such as the probability of wireless transmission failure and change in telecommunication Quality of Service are discussed. These works, however, focus only on ICT infrastructure aspects with an emphasis on data transfer. They do not consider the GSs mentioned above, which have a direct impact on the grid operation and, consequentially, the overall CPES.

To summarize, there is a lack of methods and metrics to quantify the resilience of ICT-enabled GSs in CPES. The ICT system should be designed such that the GSs it enables are resilient, i.e., they should bounce back from disturbances without collapsing. This mandates a comparison of the resilience of the ICT design options. Furthermore, the existing area-under-curve metrics have unbounded domains (e.g., from zero to large values), making them hard to comprehend and challenging to use for comparing systems.

Contribution

This paper presents a novel methodology and metrics to quantify the resilience of ICT-enabled GSs in a CPES. A formal operational state model of GSs from preceding work (Haack et al. 2022) is used to capture the performance of GSs, which is an essential aspect of resilience assessment. The input to the model is generated using the sequential Monte Carlo method, which simulates the behaviour of the ICT system components in their *useful life*. The output of the model is a state trajectory of each GS considered. Based on this, metrics are proposed to quantify the individual phases of resilience, which are then aggregated to calculate the *probability of resilient behaviour* of an ICT-enabled

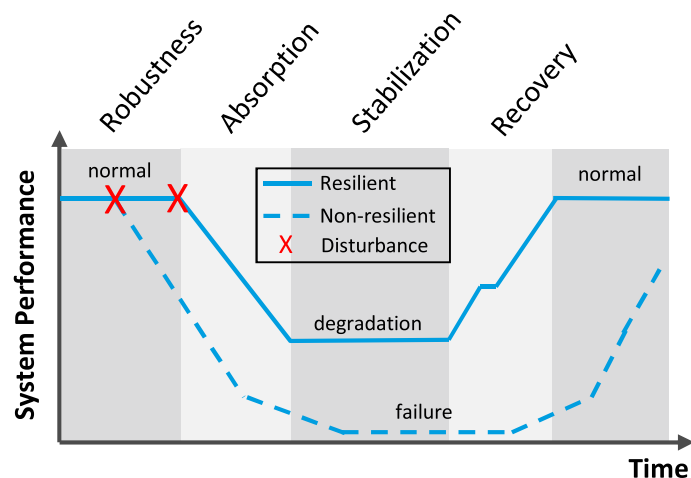


Fig. 1 Resilience bathtub curve with behaviours of resilient and non-resilient systems

GS. Another metric to quantify the aggregated *performance of a GS* from a resilient viewpoint is also proposed. The developed method and metrics are then demonstrated using a CPES consisting of the CIGRE medium voltage benchmark grid, a corresponding ICT system and SE as an exemplary service. The results can be used to analyse the resilience of existing ICT systems as well as to compare different ICT design options for CPES based on the resilience of GSs.

This paper is structured as follows: “[Theoretical background](#)” section provides the necessary background, namely, system resilience and the operational states of GSs. This is followed by the main contribution in “[Proposed methodology](#)” section, i.e., the proposed methodology and metrics to assess the resilience of ICT-enabled GSs. “[Scenario design](#)” and “[Results and discussion](#)” sections present the considered simulation scenarios and the corresponding results, respectively.

Theoretical background

This section presents the concepts used in this paper. After a brief discussion of system resilience, the operational states of ICT-enabled GSs are described.

System resilience

In this paper, the notion of resilience from the German *Energy Systems of the Future* initiative (acatech/Leopoldina/Akademienunion 2021) is used. Here, resilience is defined as the *ability of the system to absorb the impact of disturbances without collapsing and then return to normal operation*. Figure 1, also known as the resilience bathtub curve, shows the exemplary performance over time of resilient and non-resilient systems. When faced with a disturbance, a non-resilient system fails/collapses (i.e., near zero performance). In contrast, a resilient system stabilises at a lower level of performance (i.e., degrades) and quickly returns to normal performance without completely failing. The behaviour of a resilient system has four constituting phases which are as follows:

- 1 **Robustness** is the ability of the system to withstand disturbances without performance degradation. In Fig. 1, it can be seen that the resilient system is robust against

the first disturbance. In contrast, the performance of the non-resilient system is reduced to nearly zero as a result of the same disturbance.

- 2 **Absorption** is the ability of the system to respond to a disturbance by moving to a lower level of performance without collapsing. In Fig. 1, it can be seen that the resilient system absorbs the second disturbance, i.e., it moves from normal to degraded performance.
- 3 **Stabilization** is the ability of the system to maintain itself in the lower level of performance without further degradation. The resilient system in Fig. 1 shows a stable operation with degraded performance.
- 4 **Recovery** is the ability of the system to restore to normal operation. The resilient system in Fig. 1 is recovered from a degraded to normal performance faster than the non-resilient system. Recovery can either be through the system's innate response or via repair actions.

Since a system could potentially absorb a disturbance and instantly recover from it, the stabilization phase can be considered optional from a resilience viewpoint. While there exists a consensus in the literature about the last three phases, some authors such as acatech/Leopoldina/Akademienunion (2021), (Sterbenz et al. 2010) consider robustness as a part of resilience, whereas other authors (Stanković et al. 2022; Nan and Sansavini 2017) do not. Furthermore, the state after recovery is often referred to as *improved normal* as a resilient system is expected to learn and improve from disturbances (Panteli and Mancarella 2015). This, however, is beyond the scope of this paper. In summary, absorption and recovery are mandatory phases for a resilient system, whereas robustness and stabilization are optional.

Operational states of ICT-enabled grid services

The ICT system in a CPES consists of hardware and software components for data acquisition, actuation, computation and data transfer. Hardware includes sensors (e.g., remote terminal units and smart meters), controllers (e.g., intelligent electronic devices, routers, communication links (e.g., fibre optic, DSL, cellular) and servers. Whereas, the software includes algorithms for processing and decision-making (Narayan et al. 2019). Each GS requires a specific combination of hardware and software from the ICT system, and an ICT system can host several GSs, which may share the ICT components. For example, a server may host SE as well as contingency assessment services. In addition to hardware and software requirements, certain GSs may also depend on the results of other GS. For example, a coordinated dispatch from the control room uses the results of SE (Klaes et al. 2020). The main goal of the ICT system in CPES is to enable the GS, and therefore, the ICT system should be designed to ensure the proper functionality of the GSs.

Since resilience is represented as performance over time (cf. "System resilience"), a prerequisite for assessing the resilience of GSs is determining their performance. In this regard, the operational states of GSs, which represent their performance, are used. This concept is published in Klaes et al. (2020) followed by its modelling and validation in Haack et al. (2022). SE and voltage control are presented as exemplary GSs in these papers.

Based on three properties of the ICT system, namely the availability of components, timeliness of data transfer and correctness of data (i.e., measurements and control commands), the performance of a GS can be classified into one of the following three states (Narayan et al. 2021):

- Normal state: In this state, the GS is fully functional (ideal performance) and can be used by the system operator as intended. Here, coordinated decision-making is possible with low uncertainties since the required data is available and is transmitted correctly in time. A GS is said to be in *normal* state if either no disturbance has occurred or if the occurred disturbance does not result in performance degradation.
- Limited state: In this state, the GS has a partial performance degradation. Disturbances impacting the availability, timeliness and/or correctness can cause a GS to transition from the *normal* to the *limited* state. Here, the GS typically resorts to using its fallback mode (e.g., using historical measurements when real-time field measurements are lost). Depending on the disturbances, there is also an increased risk of further performance degradation of the GS. The *limited* state indicates high uncertainties when using the GS, implying that the system operator should use it with caution while aiming to recover it to its *normal* state.
- Failed state: In this state, the GS exhibits full (or unacceptable) performance degradation, i.e., not being available, too slow/late or yielding grossly incorrect results. Depending on the criticality of the GS, the system operator should immediately take suitable actions to improve its performance. Disturbances that impact vital ICT components, such as servers, can cause the GSs that depend on these components to fail.

These operational states are formalised in the preceding work (Haack et al. 2022), where the ICT system is modelled as a graph. The operational states and the conditions for transitions among them are modelled using deterministic finite state automaton, with one automaton for each GS. The conditions for transitions are based on the three aforementioned properties, i.e., availability, timeliness and correctness, which are calculated based on the ICT graph. These three properties capture the impact of different disturbances (e.g., hardware failures, delays, software malfunctions) and repair actions (e.g., repairing hardware, restarting the server) on the ICT system and, consequentially, on the GSs by triggering state transitions. The input to the model is a sequence of events (disturbances and repair actions). The output of the model is the operational state trajectory (sequence of states) of each GS corresponding to the input events. This operational state model is used in the methodology proposed in the current paper.

In the rest of the paper, the *normal*, *limited* and *failed* states are denoted as N (green), L (yellow) and F (red), respectively. Figure 2 shows the three operational states as well as transitions among them for an ICT-enabled GS. For example, NL and LF denote the transitions from N to L and from L to F , respectively. Disturbances can degrade the operational state (i.e., NF , NL , LF), whereas repair actions can improve the state (i.e., LN , FN , FL). Depending on the ICT system and the GS, certain disturbances and repair actions may not necessarily result in a state change. These are represented by the self-transitions NN , LL and FF .

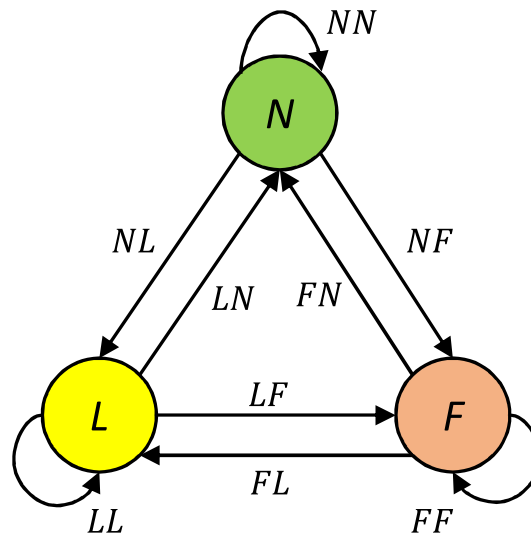


Fig. 2 Operational states and transitions of an ICT-enabled Grid Service

Proposed methodology

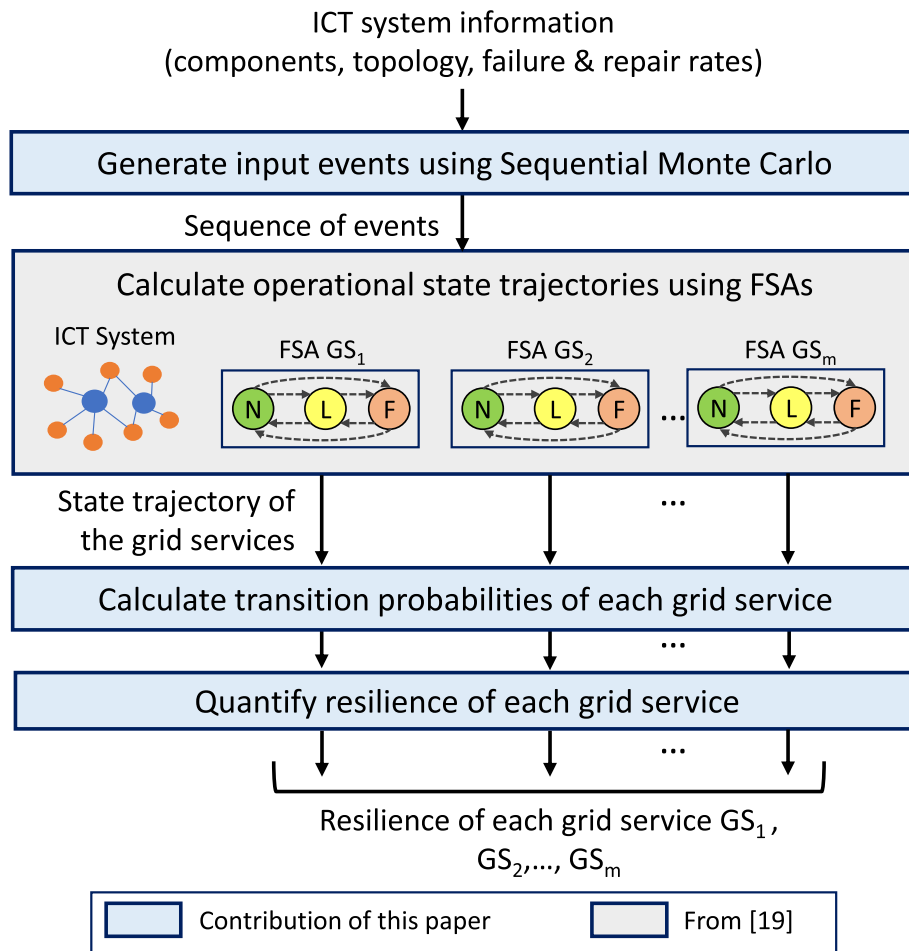
This section presents the proposed methodology and metrics to assess the resilience of ICT-enabled GSs in a CPES. Starting with the core idea of mapping the operational states of the GSs to their resilience, the proposed method is then explained, followed by the metrics to quantify resilience.

Mapping operational states to resilience

This paper focuses on assessing the resilience of the GSs as the role of the ICT system in CPES is to enable the GSs, which has a direct impact on the operation of the interconnected power system. Based on the discussions in “System resilience” and “Operational states of ICT-enabled grid services”, it can be seen that the operational states of the GSs capture their performance, which is an essential aspect of resilience assessment. Therefore, the operational states of the GSs can be used to assess their resilience. Particularly, the transitions among the states can be mapped to the four phases of resilience as follows:

- Robustness can be captured by NN , implying that the input event (disturbance or repair) does not result in performance degradation and the GS stays in the N state.
- Absorption can be captured by NL , implying that the input event has caused a performance degradation in the GS, but has not yet failed.
- Stabilization can be captured by LL , which shows the ability of the GS to maintain itself in a degraded state (i.e., in L state) without failing.
- Recovery can be captured by LN , implying that the GS is restored to normal performance, possibly via repair actions.

Since disturbances are uncontrollable and inevitable, these phases continue to occur throughout a resilient system’s lifetime. The resilience of the system can then be



the input events. The current paper aims to study the performance and, consequently, the resilience of the GSs. Therefore, in contrast to Haack et al. (2022), which considers only a few pre-defined disturbances as input events, the current paper models a wide range of input events consisting of disturbances as well as repair actions. For a given ICT system, the input generation should be done in a generalised manner. These inputs should reflect the typical events that the ICT system and, thus, the GSs will encounter during operation, given that the results are intended to support ICT design decisions. This requires a probabilistic approach since ICT disturbances are stochastic. This paper employs the sequential Monte Carlo (SMC) method. It is a systematic approach that simulates the realistic behaviour of components and systems as a sequence of random events that build upon each other as the system progresses over time (Panteli and Kirschen 2011). The SMC method enables the assessment of the system state, in this case, the state of each GS, at any desirable time using the state of the individual ICT components, which are considered input events.

The SMC method requires a *component behaviour model* to determine the state of each ICT component and the duration for which the component stays in that state. Assuming that the ICT components are operating in their *useful life* phase, the behaviour of each component can be modelled using an exponential distribution (Panteli and Kirschen 2011). This is a common assumption as the failure rate of a component outside its *useful life* phase is drastically high (Kröger 2008; Tuinema et al. 2020). According to this model, an ICT component c can transition between fully functional (UP) and out-of-service or failed (DOWN) states. The time c stays in UP and DOWN states is called time to fail (TTF) and time to repair (TTR), respectively, which can be calculated as follows (Panteli and Kirschen 2011):

$$TTF^c = \frac{-\ln(U_1)}{\lambda^c}, \quad TTR^c = \frac{-\ln(U_2)}{\mu^c} \quad (1)$$

Here λ^c and μ^c are the failure and repair rates of the component c , respectively, and U_1 and U_2 are two uniform random numbers in the interval (0, 1]. These rates remain constant during the component's *useful life* phase (Tuinema et al. 2020). An operating (or UP-DOWN) sequence of c can now be generated by alternatively sampling values of TTF^c and TTR^c using Eq. (1). This can then be extended to all components of the ICT system by considering their respective failure (λ) and repair (μ) rates. Initially, all components are assumed to be fully functional (UP).

The top three curves in Fig. 4 show the exemplary operating sequences of the ICT components. Note that the values of TTF and TTR shown in the figure are unique as they depend on random numbers U_1 and U_2 (cf. Eq. 1). Therefore, different combinations of components failure and repair sequences can be generated using this method, which results in different input events to the finite state automata.

Calculate operational state trajectories and transition probabilities

At each time step k , the set of the states of all ICT components is given as an input to the automata (cf. “Operational states of ICT-enabled grid services”), which is then used to assess the state of the corresponding GSs. When repeated for several time steps, this results in a sequence of operational states, i.e., the state trajectory, of the GSs. Note that,

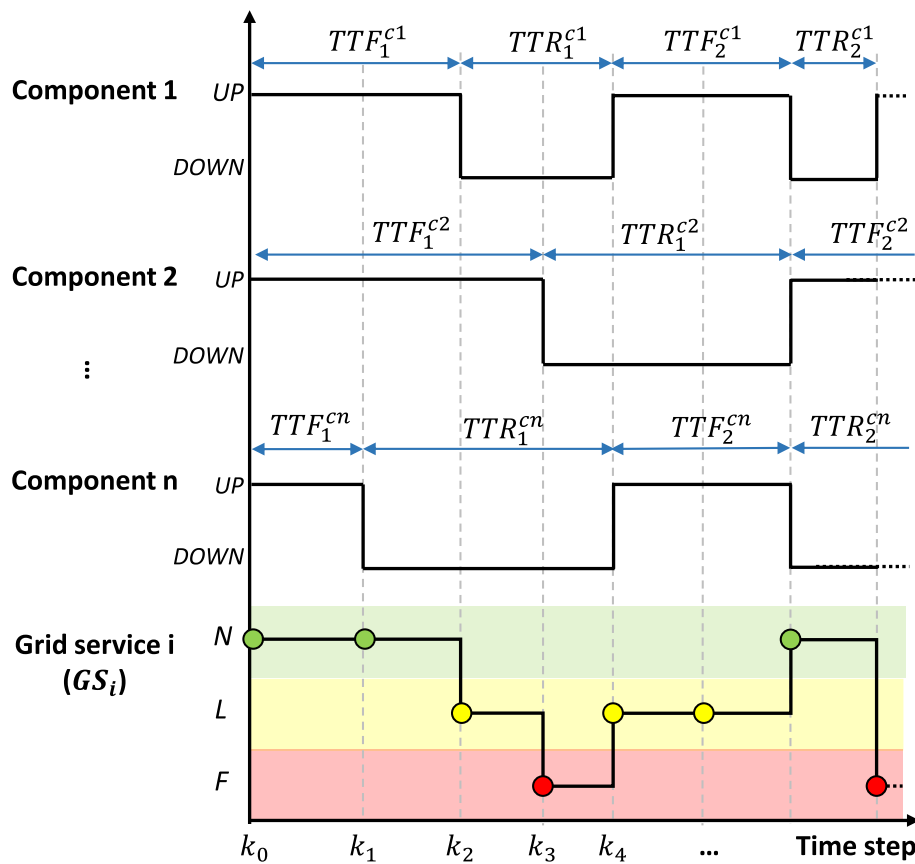


Fig. 4 Example sequence of input events and state of a GS in SMC

as shown in Fig. 3, each GS has its automaton (denoted as FSA), resulting in one trajectory for each GSs. The bottom curve of Fig. 4 shows an exemplary state trajectory of a service GS_i . Since all components are initially UP, the state of GS_i at k_0 is N . At k_1 , the state of GS_i is also N , indicating an NN transition from k_0 to k_1 . This indicates that GS_i is robust to the input events at this time step, i.e., the failure of component- n (shown in the third curve from the top). It can be seen that the state trajectory resulting from the input events can have both degradations (e.g., NL between k_1 and k_2) as well as recoveries (e.g., FL between k_3 and k_4). It can also be seen that the SMC can model the impact of simultaneous component failures and repairs on GSs. For instance, components 1 and n are both in the DOWN state at k_2 and are repaired simultaneously at k_4 . Since the ICT system is modelled as a discrete system, the states and the transitions of a GS are discrete, i.e., transitions occur instantly at time steps without slopes (unlike Fig. 1). Based on the state trajectories of the GSs, the probabilities (p) of the nine transitions shown in Fig. 2 can be computed using the condition $\sum p^{ij} = 1$, where $i, j \in \{N, L, F\}$, i.e., all the nine transition probabilities should sum to one.

The stochasticity of the SMC mandates a convergence condition for determining the number of simulation steps required to achieve the desired level of confidence in the results. Equation (2) shows the condition used in the paper and is based on the absolute error of transition probabilities.

$$Z \frac{S_k^p}{\sqrt{k}} < 0.01 \quad (2)$$

Here k is the number of samples (or time steps), S_k^p is the variance for the k samples of transition probabilities p and Z is the standard normal value for the required confidence interval. For a 95% confidence, the value of Z is 1.96. The term S_k^p/\sqrt{k} denotes the difference between the true mean and the sample mean. The transition probabilities of the GSs are computed using their respective state trajectories, until the time step k at which the absolute error is less than 1%. The SMC terminates when the absolute error of all nine transition probabilities for each GS considered satisfies Eq. (2).

Metrics to quantify resilience of a grid service

The quantification of the resilience of a GS requires suitable metrics. The metrics proposed in this paper are derived based on the aforementioned transition probabilities because the phases of resilience can be mapped onto them (cf. “[Mapping operational states to resilience](#)”). The following metrics are defined for the four phases of resilience.

$$R^H = p^{NN}, \quad R^A = p^{NL}, \quad R^S = p^{LL}, \quad R^R = p^{LN} \quad (3)$$

Here R^H , R^A , R^S and R^R denote the robustness (or hardening), absorption, stabilization and recovery metrics, respectively. The different values of p represent the corresponding transition probabilities, e.g., p^{NN} denotes the probability of NN transition, which indicates robustness, and p^{LN} represents the probability of LN transition, which indicates recovery. Using these, a metric R denoting the *probability of resilient behaviour* of an ICT-enabled GS can be defined as:

$$R = e(R^H + R^A + R^S + R^R), \quad (4)$$

$$\text{where, } e = \begin{cases} 0 & (R^A > 0 \vee R^R > 0) \wedge R^A \times R^R = 0, \\ 1 & \text{otherwise.} \end{cases} \quad (5)$$

Here the value of the coefficient e goes to zero when the trajectory has an absorption without recovery and vice versa, as they are mandatory for resilient behaviour (cf. “[System resilience](#)”). Since R is calculated based on probabilities, its domain is $[0, 1]$, and its value is dimensionless. $R = 1$ indicates the highest probability of resilient behaviour of a GS with its state trajectory consisting of only the transition between and within N and L states, including absorption and recovery. On the other hand, $R = 0$ indicates that the probability of resilient behaviour is zero, implying that the GS is not resilient. $0 < R < 1$ indicates that the GS has some probability of resilient behaviour. This means that its trajectory enters the F state at least once but also has at least one absorption and one recovery phase, which do not necessarily have to be consecutive.

Equation (4) shows that the resilience of a GS depends only on p^{NN} , p^{NL} , p^{LL} and p^{LN} , i.e., probabilities of the transitions within and between N and L states. This is because, as in Fig. 1, a transition to failure or the F state is typically not considered to be a resilient behaviour. These transitions, namely, NF , LF and FF , however, can yield valuable insights into the performance of a GS. For instance, a disturbance causing an NF transition can

be regarded as a high-impact event causing the GS to fail instantly (without entering the L state). The FF transition captures the inability of the GS to escape the F state. Accordingly, the following two metrics can be defined:

$$R^F = p^{NF} + p^{LF} + p^{FF} \quad (6)$$

$$\begin{aligned} \hat{R}^R &= \hat{R}^{R,N} + \hat{R}^{R,L} + R^R \\ \text{where, } \hat{R}^{R,N} &= p^{FN} \text{ and } \hat{R}^{R,L} = p^{FL} \end{aligned} \quad (7)$$

The failure metric (or failure probability) R^F captures the (dis)ability of the GS to enter and stay in F state. \hat{R}^R is the extended recovery metric, which, in addition to R^R (i.e., p^{LN}), also includes recoveries from F . Considering this, a metric R^{MOP} , which measures the performance of a GS from a resilience viewpoint, is defined as:

$$R^{MOP} = w^N (R^H + R^R + \hat{R}^{R,N}) + w^L (R^A + R^S + \hat{R}^{R,L}) - w^F (R^F) \quad (8)$$

Here $w^N, w^L, w^F \in [0, 1]$ are the weights of the transitions to the N, L and F states, respectively. They can be used to weigh the contribution of the three states to the overall performance of the GS and could be adjusted as required. Typically, $w^N > w^L$ since it is better for a GS to be in N state than in L . Since a failure is an undesired behaviour from the resilience perspective, the performance metric R^{MOP} is penalised (i.e., subtracted) by the failure metric R^F . Due to this penalisation, the domain of R^{MOP} is $[-1, 1]$, and its value is dimensionless.

Although the metric R (Eq. 4) captures resilience as discussed in “System resilience”, several state trajectories can have an R value of one. Examples include (i) a GS that remains in the N state with only NN transitions, (ii) a GS that oscillates between N and L states, and (iii) a GS that enters L , stays there for a long time (LL transitions) and recovers to N state. This is because they are all resilient based on the definition in acatech/Leopoldina/Akademiunion (2021), which also makes it challenging to compare the GSs solely based on R . In such cases, the metric R^{MOP} from Eq. (8) can be used along with R to assess the performance of a GS. Therefore, the resilience and the performance of individual GSs can be quantified using Eqs. (4) and (8).

In the rest of the paper, exemplary weights of $w^N = 1, w^L = 0.5$ and $w^F = 1$ are considered. Consequentially, $R^{MOP} = 1$ indicates that the GS remains in the N state (best possible performance). If $0 < R^{MOP} < 1$, it indicates that the GS is in the N and L states more than the F state. Contrarily, $R^{MOP} < 0$ indicates that the GS is expected to enter in F state frequently (R^F is greater than the sum of the other terms in Eq. (8)), despite the repair actions considered in the input events. Figure 5 shows the exemplary operational state trajectories of six GSs to illustrate the proposed metrics R and R^{MOP} . The SMC is assumed to have converged within six time steps in all these cases. The R values of GS_1 and GS_2 indicate a 100% probability of resilient behaviour with GS_1 never degrading and GS_2 having both absorption and recovery phases without failing. However, GS_2 has a worse performance, i.e., lower R^{MOP} , since it enters the L state more than GS_1 . Contrarily, GS_4 and GS_5 both have zero probability of resilient behaviour. The former has absorption but never recovers from the L state, while the latter often fails without absorption and recovery. In this case, the R^{MOP} metric can be used to identify the better

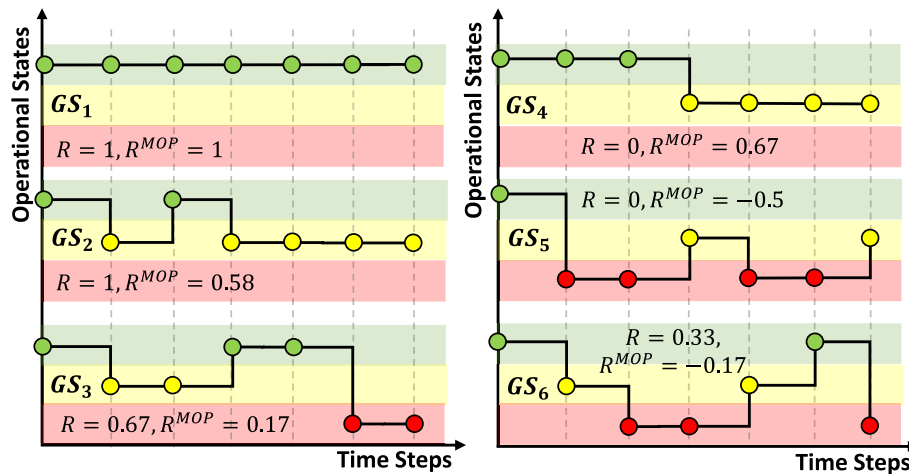


Fig. 5 Exemplary state trajectories of six GSs to illustrate the proposed metrics

GS, which in this case would be GS_4 , which has fewer transitions to F state. This also indicates that it would be easier to make GS_4 resilient when compared to GS_5 . Both GS_3 and GS_6 have positive resilience probability R despite entering F state. However, the R^{MOP} of GS_6 is negative and GS_3 is positive because the former has more transitions to the F state. Overall, while GS_1 depicts the ideal GS from a resilient viewpoint, GS_2 is the second best considering both resilience probability R and performance R^{MOP} . Although GS_4 has a higher R^{MOP} than GS_2 and GS_3 , the former is considered worse from a resilience viewpoint because it has zero resilient behaviour probability. Note that the values of R^{MOP} depend on the chosen weights.

The developed metrics are modular, i.e., the phases can be analysed both individually as well as in combination with others to quantify the overall resilience of the GS. As discussed in “System resilience”, some research considers robustness to be part of resilience, while others do not. In the latter case, Eqs. (4) and (8) can be easily adapted by removing R^H (robustness metric). Then, the other metrics have to be scaled accordingly in order for R and R^{MOP} to have the same domain, i.e., $[0, 1]$ and $[-1, 1]$, respectively. Since these metrics have a bounded domain, they are easy to comprehend and hence, can be used as a basis to compare the resilience of different GS architectures and design choices, e.g., central vs distributed SE. This can then be used for designing ICT systems with the goal of improving the resilience of the GSs it enables.

Scenario design

This section presents the simulation scenario to demonstrate the proposed resilience assessment methodology and metrics. The scenario consists of an ICT network with SE as an exemplary GS, both of which are explained in the following subsections. Note that the GS simulation in this paper is done from an ICT point of view while abstracting the power system aspects.

State estimation service

SE is one of the most important GS as it estimates the state variables, i.e., bus voltage magnitudes and angles, in real-time based on field measurements from sensors

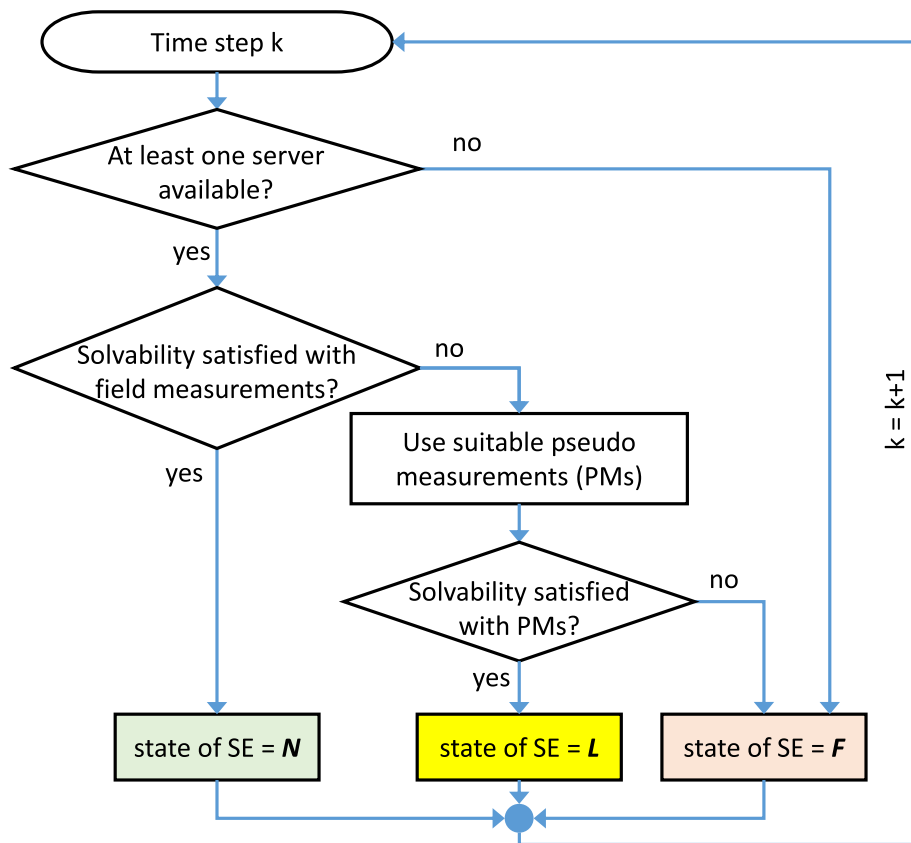


Fig. 6 Operational state assessment of state estimation (SE) service

located across the ICT system (Abur and Gomez-Exposito 2004). This paper considers a central weighted-least squares SE, where measurements from sensors are transmitted via the communication network to a server, typically located in the control room. The server hosts the SE algorithm, where the received measurements are processed, and the state variables are estimated. The necessary condition for the solvability of the weighted-least squares SE is $\rho(H) = n_{sv}$ (Klaes et al. 2020), 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 available field measurements. Failure of sensors or communication network problems may result in a loss of field measurements at the server, possibly violating the solvability condition. In this case, suitable pseudo-measurements (PMs) can substitute the missing field measurements to satisfy the solvability condition. PMs are typically based on historical measurements and, therefore, increase the uncertainties of SE results when used (Abur and Gomez-Exposito 2004).

Figure 6 presents the process behind the automaton for the operational state assessment of the SE service at each time step k of the SMC simulation. The unavailability (or failure) of the server causes the SE to transition to the F state unless there is a backup or a redundant server. If a server is available, the solvability condition is checked with the field measurements available at the server at that time step. If the

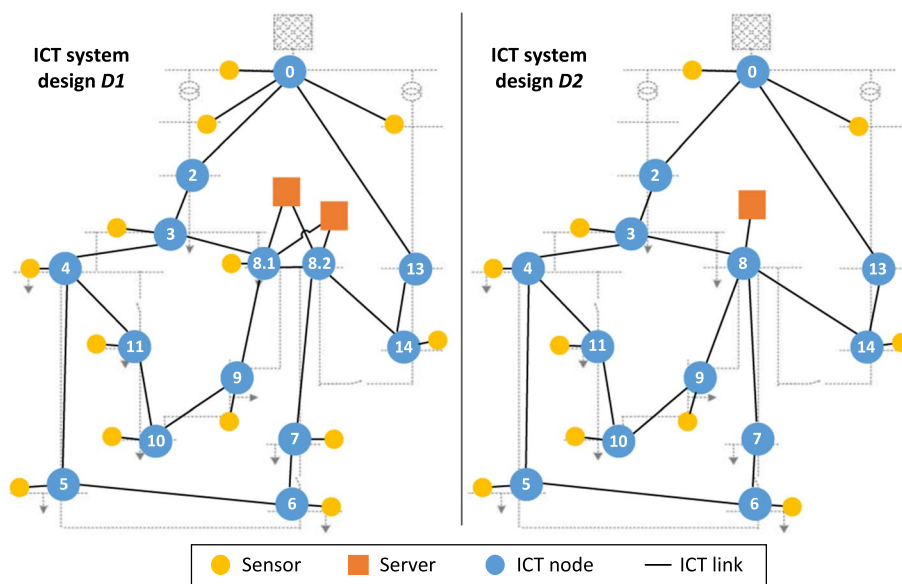


Fig. 7 Two ICT system designs (*D1* and *D2*) for the CIGRE MV benchmark grid are shown in grey in the background

solvability condition is satisfied, the state of SE is *N*, else suitable PMs are used, and the condition is checked again. If the solvability condition is satisfied using PMs, the state of SE is *L*; else, the state of SE is *F*. The solvability condition can also be violated if suitable PMs are not available or if too many field measurements are lost, thereby requiring too many PMs. Typically, a threshold is defined for the maximum number of PMs that could be used in each run of SE, i.e., at each time step *k*. In the *N* state, the operator can confidently trust and use the results of SE service to take operational decisions, whereas, in the *L* state, the results should be used with caution (cf. “Operational states of ICT-enabled grid services”). The time step is then advanced, and the process in Fig. 6 is repeated. When repeated for several time steps, this results in the operating state trajectory of the SE service, based on which its transition probabilities can be calculated.

Designs of ICT systems

To demonstrate the proposed method and metrics for the resilience assessment of GSs, two ICT system designs (*D1* and *D2*) for the CIGRE MV benchmark power grid are considered, both with the SE service. Since there is a lack of standard ICT system designs for CPES, the designs considered in this paper represent two possibilities considering the increasing penetration of ICT in distribution grids. They are based on the ICT scenarios presented in Narayan et al. (2021), Kuzlu et al. (2014).

Figure 7 shows the two ICT designs considered in this paper. Here, the ICT system consists of sensors, servers, ICT nodes and wired ICT links. Each bus, representing a substation, is associated with an ICT node, shown with blue circles in Fig. 7, and the ICT links follow the grid topology. The top three buses have a transformer between them. This indicates that they are located in the same substation and hence are associated with the same ICT node 0. Sensors, indicated by yellow circles, are located at the

Table 1 Factors differentiating the two ICT system designs

Factors	System D1	System D2
Observability	87%	66%
PM availability	Buses 8, 14	Buses 3, 5, 9, 10, 14
Server redundancy	Yes	No

buses and measure power system parameters such as voltage and current. Since the CIGRE medium voltage grid represents a distribution grid, which typically has limited observability, sensors are placed only at specific buses, as shown in Fig. 7. The server is located at bus-8, the most central node [measured using the betweenness centrality as in Narayan et al. (2021)]. It hosts the SE software described in “[State estimation service](#)”. In design *D1*, 8.1 and 8.2 represent redundant nodes for the servers, which are located at the same bus. The ICT nodes and links facilitate communication between the sensors and the server.

The design of the ICT system, which also includes the design of the GSs, influences the performance and, consequentially, the resilience of the GSs. Table 1 presents the factors differentiating ICT system designs *D1* and *D2*. They are chosen to include hardware-based factors, such as observability and redundancy, and software-based (or algorithmic) factors. Although several other factors exist for designing ICT systems with GSs (see (Wolgast and Nieße 2019; Antoniadou-Plytaria et al. 2017) for examples), this paper is restricted to the ones in Table 1, since the goal is to demonstrate the ability of the method and metrics to assess the resilience of GSs considering different ICT system designs. The considered design factors are:

- **Observability:** This is the percentage ratio of the number of sensors to buses. While the power grid has 15 buses, the ICT system *D1* has 13 sensors (87% observability), and *D2* has 10 sensors (66% observability). Higher observability should result in higher robustness in the case of measurement losses.
- **PM availability:** When the solvability condition is not satisfied using field measurements, the SE service uses PMs. *D1* has PMs for buses 8 and 14, whereas *D2* has PMs for buses 3, 5, 9, 10 and 14. The higher the availability of PMs, the more the SE service can transition to and stay in the *L* state instead of failing (*F* state). This should improve absorption as well as stabilization (cf. “[Mapping operational states to resilience](#)”).
- **Server redundancy:** As shown in Fig. 6, a failure of the server will cause the SE service to fail and, so server redundancy could improve its robustness, i.e., staying in *N* state. This makes the server one of the most critical ICT components. While design *D1* has redundant servers as well as ICT nodes and links to which it is connected, design *D2* has a single point of failure.

While PM availability is a GS-specific design factor for the SE service, observability and redundancy are general design factors for all the GSs in the ICT system. The SMC method also requires the rates λ^c and μ^c for the ICT system components (cf. Eq. 1). For simplicity, uniform values of $\lambda^c = 0.009 h^{-1}$ and $\mu^c = 0.2 h^{-1}$ are assumed for all ICT

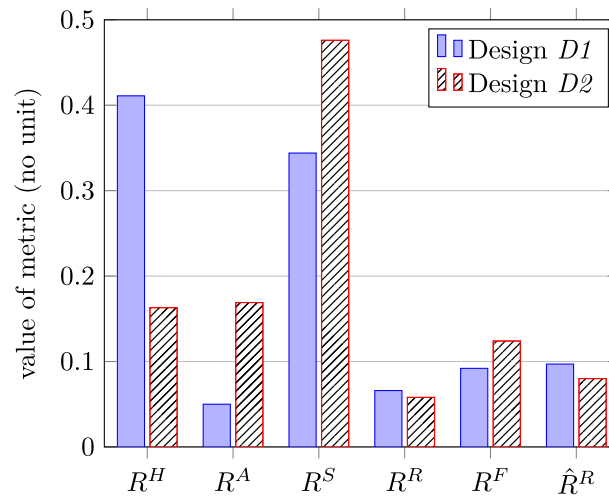


Fig. 8 Metrics showing phases of the resilience of SE service for both ICT system designs

components based on Panteli and Kirschen (2011). This assumption could, however, easily be removed by using the corresponding rates of the ICT components. Based on these design considerations, the following hypothesis is outlined for the simulations results presented in this paper:

Hypothesis The SE service in the ICT system design $D1$ will have more robustness than design $D2$, while that in $D2$ will have more absorption and stabilization than $D1$.

Results and discussion

This section presents the simulation results showing the resilience and the performance of the SE service considering the two ICT system designs $D1$ and $D2$. The simulations are done in Python using the NetworkX¹ package for modelling the ICT graph. The convergence of the SMC method required 14,900 and 11,108 time steps for $D1$ and $D2$. This is because design $D1$ has more ICT components than $D2$, implying more variability due to the increased number of operating sequences. The resulting operational state trajectory of the SE service is then used to compute the probability of its state transitions. Its resilience is then computed using the equations from “Metrics to quantify resilience of a grid service”.

Figure 8 shows the results of Eqs. (3), (6) and (7), i.e., the phases of the resilience of the SE service, also considering the degradation to and recovery from F state. The results show that, for the SE service, design $D1$ is more robust (R^H) compared to $D2$, meaning that the SE service in $D1$ has more resistance to degradation from N . This can be attributed to the increased hardware redundancy (i.e., more observability and redundant servers) in $D1$. On the other hand, owing to the increased PM availability, $D2$ has higher values of absorption (R^A) and stabilization (R^S) metrics than $D1$. Specifically, more PMs enable the design $D2$ to compensate for the loss of more field measurements, caused either due to the failure of the sensor itself or the communication path between

¹ NetworkX: <https://networkx.org/> (last accessed: 17th June 2023).

Table 2 Resilience and performance of SE service for ICT system designs $D1$ and $D2$

Grid service	ICT system design	R (no unit) Eq. (4)	R^{MOP} (no unit) Eq. (8)
SE	$D1$	0.871	0.605
	$D2$	0.866	0.436

the sensor and the server, than $D1$. These results also validate the aforementioned hypothesis.

The design $D2$ has a marginally higher failure metric (R^F), indicating that $D2$ enters the F state more often compared to $D1$. Furthermore, it can be seen that the extended recovery metric (\hat{R}^R) of both designs is greater than the respective recovery metric (R^R) since the former includes the value of the latter (cf. Eq. 7). This shows that the proposed method and metrics can quantify the individual phases of the resilience of an ICT-enabled GS, including the transitions related to the F state. The impact of the design factors shown in Table 1 on the phases of resilience can also be captured. Using the results, relevant design factors that improve the favourable phases of resilience, while lowering unfavourable ones (i.e., R^F), could be analysed and implemented.

Table 2 presents the calculated probability of resilient behaviour R from Eq. (4) and the corresponding performance R^{MOP} from Eq. (8) of SE service for the two ICT system designs. These metrics aggregate the phases from Fig. 8. Since both designs have a similar value of resilience probability R , it can be said that the decrease of R^H in design $D2$ is nearly compensated by the increase in R^A and R^S . However, because of higher R^F and lower \hat{R}^R values, design $D2$ has a lower performance R^{MOP} than $D1$. It can be concluded that the ICT system design $D1$ is better for the considered implementation of the SE service (i.e., centralised WLS), because of the higher R^{MOP} than $D2$. However, both R and R^{MOP} are less than the maximum possible value of 1 (cf. “Metrics to quantify resilience of a grid service”), indicating a possibility for improvement in the design $D1$.

This approach can be extended to consider more ICT system design factors and GSs. The corresponding results might indicate that different designs are better for different GSs. The criticality of the GSs, if known, can be used to decide between ICT system designs. Furthermore, cost is an important factor, against which resilience has to be weighed while designing systems (Stanković et al. 2022). In the considered scenario, increasing grid observability and redundancy will require more sensors and servers, respectively. Consequently, although design $D1$ offer better resilience performance than $D2$ for the SE service, $D1$ will be more expensive due to increased hardware components. Therefore, the proposed method and metric can serve as one of the aspects of system design as improving the resilience (and performance) of the GSs can improve the resilience (and performance) of the interconnected power system.

Conclusion and future work

This paper presents a method and metrics for the resilience assessment of ICT-enabled GSs in CPES. The operational state model of GSs, which classifies their operational state into *normal*, *limited* or *failed* states, is used for quantifying their performance. Sequential Monte Carlo simulations are performed using the exponential distribution model

of the ICT components. This yields a state trajectory of the GSs based on which their transition probabilities are computed. Using this, metrics are derived to quantify the different phases of resilience, which are then aggregated to compute the probability of resilient behaviour. Another metric for measuring the performance of a GS from a resilient viewpoint, including the *failed* state, is also proposed. While the aggregated metrics quantify the overall resilience of the GS, the individual metrics quantify its different phases. The method and metrics are demonstrated using two ICT system designs for the CIGRE medium voltage grid with the SE service. A preliminary simulated-based validation is performed based on hypothesis testing. Since enhancing the resilience of the ICT system with the GSs can enhance the resilience of the whole CPES, the proposed method can be used to analyse and compare various design factors for the ICT system.

Future research should include additional simulations employing larger ICT networks, especially with more GSs. This is essential since SMC simulations could be computationally intensive for larger networks. Along these lines, an elaborated validation of the proposed method should also be conducted. Further properties of the ICT system, such as timeliness (latency) and correctness (data corruption), should also be integrated into the SMC simulation. This will enable the analysis of further ICT design factors (e.g., network topology, different GS algorithms, bandwidth, computational resource) on the resilience of GSs. In this regard, the sensitivity of the resilience phases to the various design factors could also be of interest.

Author contributions

AN was responsible for developing the resilient assessment methodology, conducting simulations and writing the paper. MB contributed towards conceptualising the metrics and manuscript review. SL contributed with expert knowledge in the field and review. All authors read and approved the final manuscript.

About this supplement

This article has been published as part of Energy Informatics Volume 6 Supplement 1, 2023: Proceedings of the 12th DACH+ Conference on Energy Informatics 2023. The full contents of the supplement are available online at <https://energyinformatics.springeropen.com/articles/supplements/volume-6-supplement-1>.

Funding

This research has been funded by German Federal Ministry for Economic Affairs and Energy (BMWi) under agreement no. 03EI1020E (Resilienz-Monitoring für die Digitalisierung der Energiewende) and by Deutsche Forschungsgemeinschaft (DFG)—project number 359778999.

Availability of data and materials

No additional data or material is used for this article.

Declarations

Competing interests

The authors declare that they have no competing interests.

Published: 19 October 2023

References

- Abur A, Gomez-Exposito A (2004) Power system state estimation: theory and implementation, vol 24. CRC Press, Boca Raton
- acatech/Leopoldina/Akademienunion (2021) The resilience of digitalised energy systems. Options for reducing blackout risks (Series on science-based policy advice). acatech/Leopoldina/Akademienunion
- Afzal S, Mokhlis H, Illias HA, Mansor NN, Shareef H (2020) State-of-the-art review on power system resilience and assessment techniques. *IET Gener Transm Distrib* 14(25):6107–6121

- Antoniadou-Plytaria KE, Kouveliotis-Lysikatos IN, Georgilakis PS, Hatzigiorgiou ND (2017) Distributed and decentralized voltage control of smart distribution networks: models, methods, and future research. *IEEE Trans Smart Grid* 8(6):2999–3008
- Bhusal N, Abdelmalak M, Kamruzzaman M, Benidris M (2020) Power system resilience: current practices, challenges, and future directions. *IEEE Access* 8:18064–18086
- Haack J, Narayan A, Patil A, Klaes M, Braun M et al (2022) A hybrid model for analysing disturbance propagation in cyber-physical energy systems. *Electr Power Syst Res* 212:108356
- Jimada-Ojuolape B, Teh J (2020) Impact of the integration of information and communication technology on power system reliability: a review. *IEEE Access* 8:24600–24615
- Klaes M, Narayan A, Patil AD, Haack J, Lindner M, Rehtanz C et al (2020) State description of cyber-physical energy systems. *Energy Inform* 3(1):1–19
- Kröger W (2008) Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. *Reliab Eng Syst Saf* 93(12):1781–1787
- Kuzlu M, Pipattanasomporn M, Rahman S (2014) Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput Netw* 67:74–88
- Liu X, Chen B, Chen C, Jin D (2020) Electric power grid resilience with interdependencies between power and communication networks—a review. *IET Smart Grid* 3(2):182–193
- Nan C, Sansavini G (2017) A quantitative method for assessing resilience of interdependent infrastructures. *Reliab Eng Syst Saf* 157:35–53
- Narayan A, Klaes M, Babazadeh D, Lehnhoff S, Rehtanz C (2019) First approach for a multi-dimensional state classification for ICT-reliant energy systems. In: International ETG-congress 2019; ETG symposium. VDE, pp 1–6
- Narayan A, Klaes M, Lehnhoff S, Rehtanz C (2021) Analyzing the propagation of disturbances in CPES considering the states of ICT-enabled grid services. In: 2021 IEEE electrical power and energy conference (EPEC). IEEE, pp 522–529
- NERC (2004) Technical analysis of the August 14, 2003 blackout: what happened, why, and what did we learn? Report to the NERC board of trustees by the NERC steering group. System, pp 1–119
- Nichelle-Le KC, Dobson I, Wang Z (2021) Extracting resilience metrics from distribution utility data using outage and restore process statistics. *IEEE Trans Power Syst* 36(6):5814–5823
- Panteli M, Kirschen DS (2011) Assessing the effect of failures in the information and communication infrastructure on power system reliability. In: 2011 IEEE/PES power systems conference and exposition. IEEE, pp 1–7
- Panteli M, Mancarella P (2015) The grid: stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. *IEEE Power Energy Mag* 13(3):58–66
- Patil AD, Haack J, Braun M, Meer HD (2020) Modeling interconnected ICT and power systems for resilience analysis. *Energy Inform* 3(1):1–20
- Samarajiva R, Zuhyle S (2013) The resilience of ICT infrastructure and its role during disasters. United Nations—Economic and Social Commission
- Schossig T, Schossig W (2014) Disturbances and blackouts—lessons learned to master the energy turnaround. In: 12th IET international conference on developments in power system protection (DPSP 2014)
- Stanković A, Tomsović K, De Caro F, Braun M, Chow J, Āukalevski N et al (2022) Methods for analysis and quantification of power system resilience. *IEEE Trans Power Syst* 38:4774–4787
- Sterbenz JP, Hutchison D, Çetinkaya EK, Jabbar A, Rohrer JP, Schöller M, Smith P (2010) Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. *Comput Netw* 54(8):1245–1265
- Tuinema BW, Rueda Torres J, Stefanov A, Gonzalez-Longatt F, van der Meijden M (2020) Probabilistic reliability analysis of power systems. Springer, Cham
- Tøndel IA, Foros J, Kilskar SS, Hokstad P, Jaatun MG (2018) Interdependencies and reliability in the combined ICT and power system: an overview of current research. *Appl Comput Inform* 14(1):17–27
- Whitehead DE, Owens K, Gammel D, Smith J (2017) Ukraine cyber-induced power outage: analysis and practical mitigation strategies. In: 2017 70th annual conference for protective relay engineers (CPRE), pp 1–8
- Wolgast T, Nieße A (2019) Towards modular composition of agent-based voltage control concepts. *Energy Inform* 2:1–18

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen® journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► [springeropen.com](https://www.springeropen.com)
