Energy Informatics

RESEARCH Open Access

Modelling the propagation of properties across services in cyber-physical energy systems

Anand Narayan[1,2*], Michael Brand[1], Nils Huxoll[1], Batoul Hage Hassan[1] and Sebastian Lehnhoff[1,2]

*Correspondence:
anand.narayan@uol.de

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

Abstract

Modern power systems, referred to as cyber-physical energy systems (CPESs), are complex systems with strong interdependencies between power and information and communication technology (ICT) systems. CPESs also have dependencies between the essential grid services. For instance, coordinated voltage control depends on state estimation, which depends on measurement acquisition. Since the operation of CPESs is largely influenced by these grid services, assessing their performance is crucial for assessing the performance of a CPES. Most of these grid services are enabled by the ICT system, i.e., they rely to a high degree on ICT. Hence, properties such as availability, correctness and timeliness, which depend on the involved software, hardware and data of the ICT system, must be considered for assessing the performance of an ICT-enabled grid service. Disturbances and repairs in CPESs impact these properties, which can then propagate and affect the performance of a grid service as well as other dependent grid services. There is, therefore, a need to model the influence of the properties of software, hardware and data on ICT-enabled grid services for single services as well as across several services, resulting in a propagation of these parameters. Current literature lacks such a model, which can used not only to investigate but also to visualise the impact of these properties on the overall perfromance of a grid service as well as other dependent grid services. This paper proposes a meta model for assessing the performance of ICT-enabled grid services, which can be instantiated for different grid services considering their dependencies. A multi-dimensional operational state space, which serves as a visualisation of the performance of grid services in terms of their state trajectory, is also proposed in this paper. The contributions are then demonstrated by a case study with a state estimation service and the widely-used CIGRE medium voltage benchmark power grid augmented with an ICT system. Three scenarios with disturbances are presented to show the benefits of the contributions. Specifically, the performance of the state estimation service considering the disturbances is investigated using the meta model, and the change in performance is visualised as trajectories using the operational state space. These contributions enable new possibilities for planning and vulnerability analyses: property changes in parts of the ICT system can be simulated to investigate their consequences throughout the ICT-enabled grid services. A trajectory representing their performance can then be visualized in the state space based on which measures could be implemented to potentially improve the resilience of the service against the considered disturbances.

Keywords: Cyber-physical energy system, System modelling, Properties propagation, Operational state space

Introduction

Motivation

Compared to traditional, modern power systems are distinguished by a significantly higher integration of information and communication technology (ICT), resulting in cyber-physical energy systems (CPESs). ICT facilitates the monitoring, data transfer, decision-making and control of CPESs with a substantial amount of decentralised power generation (Brown and Zhou 2012). However, this also increases system complexity and the interdependencies between the power and ICT systems (Panteli 2013). Additionally, it leads to increased threats from the ICT domain, such as software malfunctions and cyber-attacks, which can propagate and impact the interconnected power system (Pillitteri and Brewer 2014).

In a CPES, monitoring and control are based on ICT-enabled grid services (Klaes et al. 2020), which rely heavily on the ICT system and its components. Examples of such grid services are state estimation (Abur and Exposito 2004) for calculating the power system state variables (i.e., complex voltages of the power grid) based on measurements (Abur and Exposito 2004) and coordinated voltage control for mitigating under- or over-voltage situations using flexibilities in the power grid (Viawan and Karlsson 2008). Accordingly, ICT components and data transferred via these components significantly influence the performance of these grid services. Each ICT-enabled grid service is implemented using software, using (or running on) hardware, and most services process input data to provide output data. The state estimation service, for example, is implemented as a software component that runs on a server, processes input measurements from the field as inputs and calculates the state variables as output (Klaes et al. 2020).

As shown in Narayan et al. (2021), the performance of an ICT-enabled grid service can be defined using three ICT properties, namely, availability, correctness and timeliness. For the example of a state estimation service, its performance can be defined as whether the grid service can provide (availability) correct (correctness) state variables in time (timeliness). Hardware components can influence the performance of an ICT-enabled grid service by their availability, integrity and, if they have sensing or actuation capabilities, accuracy. The availability of a server on which the state estimation is running directly influences the availability of the state estimation service. In contrast, the integrity of the server may influence the correctness of the state estimation output. For a coordinated voltage control, the accuracy of the controllers in the field influences whether the voltage setpoints can be realised correctly. Furthermore, the properties of the input data also influence the performance of an ICT-enabled grid service. For example, if the measurements required for the state estimation are not available on time or are incorrect, the availability, timeliness and correctness, respectively, of the state estimation are impacted. Performance degradation in these grid services is already shown to impact the performance of the interconnected power system (Klaes et al. 2020). To assess the performance of an ICT-enabled grid service, it is crucial to assess the relevant properties of the involved hardware and input data.

Furthermore, ICT-enabled grid services often depend on the output data of other ICT-based hardware and services. For instance, the state estimation uses field measurements as inputs, which are provided by the measurement acquisition service (Abur and Exposito 2004). In contrast to state estimation, which typically runs centrally on a server or is distributed across a few servers, the measurement acquisition service is distributed across sensing hardware (i.e., sensors) in the power grid. The communication network, hosting the data transmission service, transports these measurements via components such as routers from the field to the servers in the control room, where the received measurements are interpreted and processed (Narayan et al. 2021). This leads to a propagation of properties, where the properties of interconnected ICT components influence each other. The accuracy of sensing hardware in the field influences the correctness of the data from measurement acquisition, which further influences the correctness of the state estimation output. Similarly, increased timeliness in the data transmission service can delay the arrival of measurements at the server, which can delay the state estimation output. Therefore, to assess the performance of an ICT-enabled grid service, it is crucial to assess the relevant properties of involved hardware, services and input data.

This paper proposes a meta model as a foundation for modelling ICT-enabled grid services considering their dependent hardware, services and data. This model can be instantiated for any ICT-enabled grid service and can be used to assess the influence of properties of hardware, data and services on the performance of the grid service. This model can further be used to analyse the impact of different ICT disturbances on the properties of ICT hardware, services, data and, consequently, the grid service. For example, a coordinated false data injection attack (Shi et al. 2021) can be modelled by reducing the integrity of hardware in the field. With an instantiation of the proposed meta model, the influence of such reduced integrity on the ICT-enabled grid service can then be automatically assessed.

Related work

This section presents literature, first from other domains and then specific to CPESs. The concept of *error propagation* between the components in a system is discussed in Avizienis et al. (2004). Here, error is defined as the deviation of the attributes of components from their respective normal (or preferred) values and can be caused by disturbances. Errors can, for instance, negatively impact the output data from the component. Errors from component A can propagate to component B if component A provides data to component B. Note that these components can be hardware or software, and a chain of interaction components can propagate errors. Cortellessa and Grassi (2007) uses the concept from Avizienis et al. (2004) to derive an analytical model for error propagation between the components in a system. The goal is to analyse the impact of errors in a component on the reliability of the whole system. Although errors in a component can propagate and impact the overall reliability, this propagation often depends on the connections between the components in the system. The authors discuss cases where subsequent components do not propagate the error. However, Avizienis et al. (2004), Cortellessa and Grassi (2007) do not consider the properties of individual components of a system. Error propagation between the components of software systems using probabilistic models is discussed in Popic et al. (2005). This work concludes that each component of a complex system can have its own attributes, which must be considered for the accurate modelling of error propagation.

From a CPES perspective, an abstract model for the ICT system is proposed in Konig and Nordstrom (2009) considering different components and their attributes, hereafter referred to as properties. Here, the ICT components are differentiated into information (data objects), behaviour (function and services) and structure (communication network and software components). The model also defines the relationship between the components, e.g. functions that read or write data objects. Different properties such as accuracy, availability, security and response time are considered, and the model is demonstrated using an automatic voltage control service. The authors of Wäfler and Heegaard (2013) model the ICT components and services using state machines, with one machine for each ICT object such as hardware, intelligent device and service. Disturbances can impact each of the three objects, causing a state change. Simple rules are then defined to determine the impact on the overall monitoring of the power grid. However, the model is only conceptual without any concrete use cases.

The authors in Klaes et al. (2020); Narayan et al. (2021) discuss the propagation of disturbances across grid services in a CPES. Three properties of grid services, namely, availability, accuracy and latency, were identified, based on which the performance of grid services is classified into one of three operational states: normal, limited and failed. Due to the dependencies of grid services in CPESs, an operational state change in one can propagate and cause a state change in another. A use case is also presented, showing how an operational state change in the state estimation service can result in a state change in the voltage control service that depends on state estimation results. The latency and accuracy properties, however, pertain only to communication network delays and measurement errors, respectively. They cannot capture disturbances such as software bugs leading to increasing processing times and data manipulations.

In Mangalwedekar et al. (2015), the authors investigate the impact and propagation of a false data injection attack on different implementations of the state estimation service. For a linear implementation, the attack impacts the correctness property of the resulting state variables in an additive manner, whereas, for a nonlinear implementation, the same attack has an exponential impact. However, the presented case studies focus purely on the power grid and do not model the interconnected ICT system. Furthermore, the approach is specific only to false data injection attacks and cannot model other disturbances such as component failures, software bugs and congestion.

The propagation of disturbances with a focus on the availability of components in CPESs is discussed in Lu et al. (2017) and Sturaro et al. (2016). These works model both power and ICT systems, focusing on how component failures in one domain propagate to the other, thereby impacting the combined CPES. However, the impact of the failures is investigated using the number of loads shed while ignoring the perspective of the grid services' performance. These works are also limited to component failures and cannot model disturbances such as attacks, bugs and congestion.

The literature review revealed that to model the performance of an ICT-enabled grid service comprehensively, its ICT components and properties should be considered. Additionally, the propagation of properties between the components should also be modelled. Current literature focuses only on a subset of properties, limiting the range of disturbances they can analyse. There is also a lack of an approach to visualise the results of the propagation of disturbances and its impact on the overall performance of a grid service.

Contribution and outline

The first contribution of the paper is a meta model for ICT-enabled grid services considering the ICT components used by the grid services, as well as the properties of these components. This model is based on a UML class diagram, where a distinction is made between the hardware, service and data of the ICT system, along with properties specific to each of them. Disturbances and repair actions can be mapped to the model as changes in these properties, which can propagate based on the connections between the components in the model. The meta model can be instantiated for any ICT-enabled grid service and can be used to analyse how variations of the properties propagate across the ICT components and impact the performance of the grid service.

The second contribution is a multi-dimensional operational state space for visualising the performance of a grid service derived from the meta model in terms of its operational state trajectory. The state space is constructed based on the relevant properties of the grid service and, therefore, can be used to depict the impact of disturbances and repair actions on the properties. The state space can also be adapted depending on the situations in the power and ICT systems.

The two contributions, namely, the meta model and the operational state space, are demonstrated using a modified CIGRE medium voltage benchmark grid augmented with an ICT system. Specifically, the meta model is instantiated for the components in the benchmark grid, based on which the propagation of their properties is described mathematically. The aim is to analyse how the degradation (due to disturbances) of different components of a grid service impacts their properties and, consequentially, the overall grid service. To do so, three scenarios, each focusing on different properties, are simulated using the meta model and their corresponding trajectories are plotted using the state space. The results enable new possibilities for planning and vulnerability analysis since property changes in different parts of the ICT system can be simulated to analyse their propagation through the ICT-enabled grid services. The results also show how the impact of disturbances and repair actions build upon one another, potentially resulting in state transitions.

This paper is structured as follows: Section Background presents the necessary fundamentals, i.e., the properties and operational states of grid services for capturing their performance. Sections Meta model for ICT-enabled grid services and Operational state space present the meta model and the operational state space, which are the two contributions of this paper. The case studies consisting of state estimation service and the CPES are shown in Section Case study: central state estimation service, along with the corresponding instantiation of the meta model. Section Results and discussion then presents the considered disturbances, the simulation results, and their implications and limitations. Section Conclusion finally concludes the paper.

Background

This section presents the operational states of the grid services from Narayan et al. (2021), which are used to capture the performance of the ICT-enabled grid services. The ICT system in a CPES includes components (hardware and software) for data acquisition, control (or actuation), computation and data transfer. This paper focuses on field devices such as sensors and controllers, communication network devices such as routers, antennas and fibre optic cables, and servers for computation. While components such as smart meters can only act as sensors, components such as remote terminal units (RTUs) or intelligent electronic devices (IEDs) can perform both sensing and actuation. The servers can either be located in the control room (centralised architecture) or spread across substations (decentral or distributed architecture) (Antoniadou-Plytaria et al. 2017). The ICT system provides the automation required for the grid services, aiding in operating the interconnected power grid.

The performance or operational state of a grid service depends on three ICT properties, namely availability, timeliness and correctness (Narayan et al. 2021). These properties not only represent the requirements of grid services on the ICT system but also map the impact of various disturbances on the ICT system and, consequentially, on the grid services it enables. Availability pertains to components and data. On the one hand, it indicates if the components required by the grid service are operational at a given time instant and can be attributed to sensors, controllers and servers. On the other hand, it indicates if the data required by the grid service is present at a given time instant and is attributed to measurements, control signals and data from other grid services as well as external sources. The availabilities of data and components are connected such that if a component is unavailable, so is the data from that component. For example, a sensor failure will cause the measurements from that sensor to be unavailable. Additionally, disturbances in the communication network can also result in the unavailability of these measurements. Timeliness is a data property and is the total time lapse between the transmission and the reception of data. Timeliness can not only be impacted by the communication network latency but also by delays in ICT components (e.g., actuation delay in controllers, processing delay in servers) (Wu et al. 2015). Correctness is also a data property and captures the closeness of data, such as measurements and control signals, to its ground truth. Data correctness can be impacted by the accuracy of sensors and disturbances such as cyber-attacks, which can impact the integrity of data (Brand et al. 2019). Based on these properties, the operational states of each grid service in the ICT system can now be defined as follows (Narayan et al. 2021):

- Normal: In this state, the grid service is fully functional and can be used as intended. Coordinated decision-making and control are possible in this state. A grid service is said to be in its normal state if no disturbance has occurred or if the disturbances have been absorbed by the robustness of the ICT system (e.g., redundant components). In this state, the required data is available and is transmitted correctly on time.
- Limited: This state indicates partial performance degradation of the grid service, and the service should be used with caution. This state is typically characterised by disturbed communication, which limits the coordination among various actors. A grid

service is in its limited state if certain disturbances have negatively impacted the availability, timeliness and correctness, causing it to resort to fallback mechanisms (e.g., using local instead of wide-area measurements).

- Failed: In this state, the service is no longer functional, i.e. not available, too slow/late or yields grossly incorrect results. Suitable actions should immediately be taken to restore the functionality of the service. A grid service is said to be in its failed state if disturbances have impacted the properties beyond the scope of the fallback mechanisms.

A grid service can transition among these operational states, which are discrete in nature. Disturbances typically cause a state degradation (e.g., normal to limited), whereas recovery actions such as repairing a component or restarting a server can improve the state (e.g., failed to limited). The formalisation of these operational states is presented in Haack et al. (2022).

Meta model for ICT-enabled grid services

The properties describing the performance of a grid service, namely, availability, correctness and timeliness, typically influence the same properties of the output of the respective service. For example, a service with a decreased correctness usually results in incorrect outputs. Furthermore, since grid services are typically dependent on each other, the output of a grid service is often the input for another grid service, resulting in a propagation of the properties assigned to the output data.

Consequently, the properties of the output of a grid service are influenced by the properties of its input data, its algorithm, the hardware it runs on and the properties of other grid services it depends on. Disturbances in the ICT system (e.g., sensor failures, cyber-attacks or congestions in communication networks) can impact these properties, which can propagate and impact different grid services using these ICT components. The model described in this section is a meta model for the performance parameters and how they impact the overall ICT-enabled grid service. This model can be instantiated for dependent grid services to represent the propagation of performance parameters across these services.

Figure 1 shows the meta model as an UML class diagram. This is adapted from the system modelling presented in Konig and Nordstrom (2009); Wäfler and Heegaard (2013) consisting of hardware, service and input/output data objects. Hardware objects (on the top in blue) represent the physical components of the ICT system, such as sensors (e.g., RTUs, IEDs), communication nodes (e.g., routers) and servers (e.g., control room servers). Hardware objects can have two properties, namely, availability and integrity, which are linked to the performance of a service using this hardware. In this context, availability is a binary property indicating whether the corresponding hardware is available for the service. A reduced integrity of a hardware component, e.g. vulnerabilities or alerts from cyber-attacks, directly influences the trust (or correctness) in the services using this hardware. A third property applicable only to sensors (e.g., RTUs, IEDs) is metering accuracy, which is also linked to correctness. For example, manufacturing errors or ageing of components in sensors can cause inaccurate metering and uncertainty in the

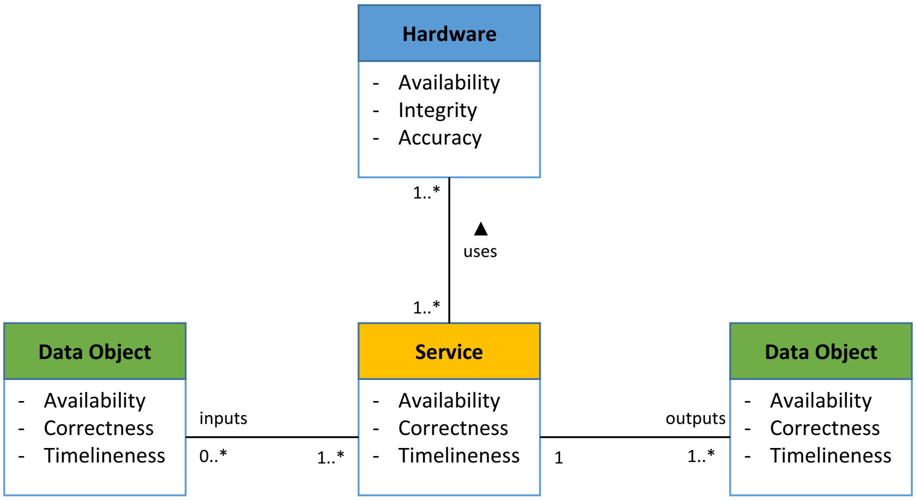

Fig. 1 Meta model for propagating data quality properties throughout ICT-enabled grid services

metered values, which may, in turn, impact the correctness of the service (Konig and Nordstrom 2009).

Service objects (in the middle in yellow) represent the transformation of input data to output data. In the scope of this paper, this represents the transformation of the properties of input data to the properties of output data, considering the involved hardware and service-specific properties. The transformation is also service-specific. Some services, for example, only send data (e.g., metering service in the field), while others perform complex operations to derive outputs (e.g., decision-making services in the control room). The hardware can each host multiple services; however, a service can also use multiple hardware if implemented using a distributed architecture (Antoniadou-Plytaria et al. 2017). Service objects have availability, correctness and timeliness as properties (cf. Background). While the involved hardware might be available, the service as software itself could be unavailable. Correctness might be affected by software that functions incorrectly (due to disturbances). Additionally, a reduced integrity or accuracy of the hardware also affects the correctness of services using the hardware. Regarding timeliness, processing latency influences how fast a service can produce outputs for given inputs. Furthermore, the performance parameters of the input data can have a significant influence on the performance of the service. Accordingly, unavailability of input data can result in the service not producing output, while incorrectness or delay of input data can result in incorrect or delayed outputs from the service, respectively.

Data objects (left and right in green) represent data exchanged between services. Data objects can, therefore, be the output of a grid service and the input of another. They also have the three properties mentioned above: availability, correctness and timeliness. These properties are directly affected by the service that produces the data and indirectly by the hardware used by the service. The availability of output data is a service-specific function comprising the availability of the service and the availability of the input data, where a service might be able to produce a subset of its output in case of unavailability of some of the inputs. For example, certain state estimation algorithms are capable of estimating state variables only for the observable parts of a power grid (Krause et al. 2015) (i.e., parts of the power grid with measurements), whereas other algorithms can only estimate the whole power grid (Hage Hassan et al. 2023). Therefore, partly missing input data, depending on the grid service algorithm, may result in a reduced availability of the output data. The correctness of output data is also a service-specific function of the correctness of the service and the correctness of the input data. Here, the dependency on the correctness of the output data object can be a complex function of the correctness of the input data, based on how the input and output data relate to each other. For example, in the case of state estimation, input measurements and output state variables are linked via a system model, which means that measurements have different degrees of influence on the state variables. For timeliness, the dependency is more straightforward since the cumulative delay (the timeliness of all related input data) is already an input for the timeliness of the service. Therefore, the latter also corresponds to the timeliness of the output data from the service.

Table 1 provides an overview of the described dependencies between the properties and their propagation. A cross indicates direct impact, while a right arrow indicates propagation. The availability, correctness and timeliness of input data directly influence the availability, correctness and timeliness of the service, respectively. They also indirectly (i.e., through the service) influence the corresponding properties of the output data. Analogously, the availability, integrity and accuracy of hardware directly influence the availability and correctness of the service. With that, they also indirectly influence the availability and correctness of the output data. Finally, the properties of a service directly influence the respective properties of the output data. As mentioned in , this meta model is the first contribution of this paper.

Operational state space

A drawback of the operational states presented in is that the limited state encompasses a wide range of behaviours – everything between but excluding fully functional to complete failure. This is due to the discrete nature of these states. If a grid service, however, is in its limited state but close to its failed state, it is more severe than if the same grid service is in its limited state but close to its normal state. Assessing this mandates the

Table 1 Overview of the influence of properties of specific component types on other component types with the following abbreviations: A: availability; C: correctness; I: integrity; P: accuracy, T: timeliness

property of ↓ affects →		**Service**			**Data (output)**		
		A	C	T	A	C	T
Data (input)	A	×	⟶		×		
	C		×	⟶		×	
	T			×	⟶		×
Hardware	A	×	⟶		×		
	I		×	⟶		×	
	P		×	⟶		×	
Service	A				×		
	C					×	
	T						×

need for a finer granular state classification. However, increasing the number of states will increase the overall complexity due to the large number of grid services in CPESs. Since the operational states are intended for system operation, a balance has to be established between ease of use and complexity in terms of capturing the actual system/phenomena under interest.

Furthermore, the definition of the operational states based on the three properties can vary depending on the situation in the ICT system as well as the interconnected power grid. In this regard, the authors in Narayan et al. (2020) discuss how, during communication network congestion, the sampling rate (timeliness) of non-critical grid services can be purposefully changed to ease the load on the network for critical grid services. Here, the sampling rate of the unit commitment service is increased from 1.5 s to 5 s, thereby freeing up the communication network bandwidth for the state estimation and voltage control services, which are more critical than unit commitment. Since this change is intentional, the unit commitment service is still considered to be in the normal state. However, its state definition based on the timeliness property has changed. Another example is shown in Das et al. (2021), where the sampling rates of phasor measurement units are increased based on under voltages in the power grid to capture the phenomenon better. In this case, the grid service has a higher sampling rate requirement for its normal state. Evidently, the thresholds based on the availability, timeliness and correctness properties are flexible and dependent on situations in the power and ICT systems.

To address these challenges with the discrete operational states, a multi-dimensional operational state space is proposed in this paper, an example of which is illustrated in Fig. 2. The state space is specific to each grid service and consists of the three ICT properties, i.e., availability, timeliness and correctness, as its three dimensions. These properties can be calculated using an instantiation of the for a specific grid service. Different regions in the state space can represent different operational states based on the service-specific thresholds of the three properties. Disconnected regions in the state space can also correspond to the same state. Table 2 shows exemplary thresholds of the three properties for the operational states, which are only used to illustrate the proposed state space. These thresholds can be used to derive the regions shown in Fig. 2. For example, the limited state is defined with an availability interval of [0.6, 0.8), a timeliness interval of $(2, 3.5]s$ and a correctness interval of [0.7, 0.9). As mentioned earlier, since the definition of the operational states based on these properties can change, multiple disconnected regions in the state space can correspond to the same operational state.

The benefits of this state space can be understood using the exemplary state trajectory shown (black lines) in Fig. 2, which can be caused by disturbances and repair actions. Based on the three properties, the black dots represent the operational states of a grid service at different time instances. T_a represents the initial state of the grid service,

Table 2 Property thresholds for the operational states of an exemplary grid service in Fig. 2

	Availability	Timliness	Correctness
Normal	[0.8, 1.0]	$\leq 2s$	[0.9, 1.0]
Limited	[0.6, 0.8)	$(2, 3.5]s$	[0.7, 0.9)
Failed	< 0.6	$> 3.5s$	< 0.7

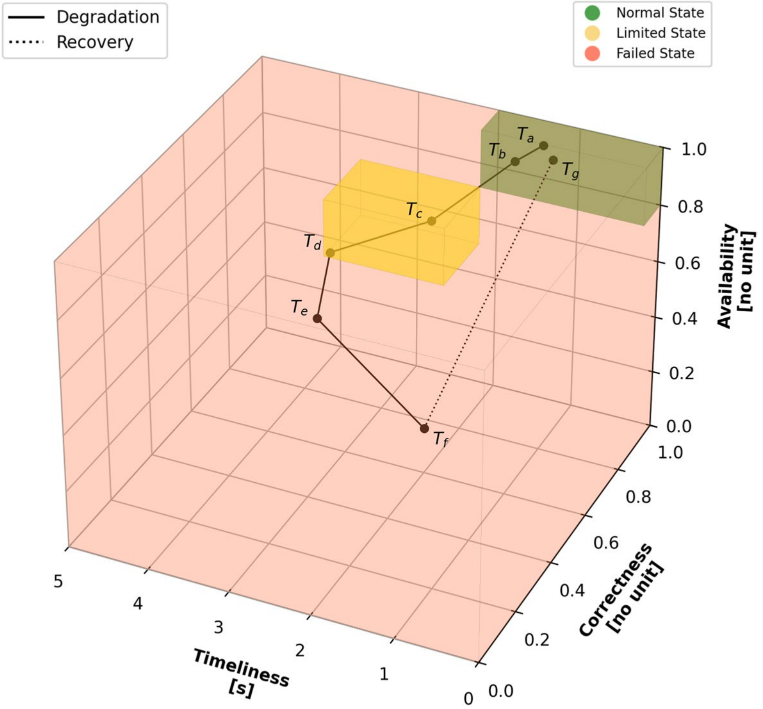

Fig. 2 Examplery operational state space visualization for the state trajectory of a grid service

which is normal. This represents an undisturbed state. $T_a - T_b$ represents a state degradation potentially caused by a disturbance. The grid service, however, remains in the normal state at T_b but is closer to limited compared to T_a. $T_b - T_c$ represents a state degradation to the limited state. Although T_c and T_d are both in the limited state, T_d is more severe as it is close to the failed state. The same is true for T_e and T_f, with the latter being the worst state of this trajectory. The transition $T_f - T_g$ represents the recovery to the normal state, which can be due to repair actions carried out in the ICT system. The main benefit of the proposed operational state space is that it can capture the current state and where the grid service is in that state (exact values of availability, timeliness and correctness) without increasing the number of states. This can be used to analyse the criticality of the state transition and estimate the effort required to recover the grid service. For instance, recovering the service from T_e could be easier than from T_f because the latter has a worse availability and correctness. The operational state space can also be used to visualise the state trajectory with degradation and recovery, which can then be used to assess the resilience of the grid service. The operational state trajectory of all grid services in a CPES could be tracked using this state space but using the corresponding grid service-specific thresholds for the regions. As presented in Contribution and outline, this operational state space is the second contribution of this paper.

Case study: central state estimation service

This section presents a case study using the state estimation service to demonstrate the developed meta model and operational state space. First, the architecture of the CPES consisting of power and ICT systems is presented, followed by the operational states of a state estimation grid service. The meta model is then initialised for this grid service, based on which the propagation of properties is elaborated.

Power and ICT systems

The power system model considered is the modified CIGRE medium voltage benchmark grid from des grands (2014) and is shown on the left side of Fig. 3. The grid consists of 12 buses, with bus 0 considered the slack bus and connected to the external grid. Each bus has an IED for measuring active (P) and reactive (Q) power flows in power lines, i.e., two measurements per IED. Note that the power flows in the lines are measured at the sending end, e.g., the power flow between buses 4 and 5 is measured by IED *S*4. Measurements from these IEDs are transmitted to the control room via a communication network. The ICT system, which encompasses the IEDs, server and communication network, is designed based on Brand et al. (2019) and shown on the right side of Fig. 3. Each bus also has an edge router connected to the respective IED. The edge routers are then connected to a core network, which is abstracted as a single core router in this paper. The edge routers and the core network connect the IEDs to the server located in the central control room. A communication path must exist between an IED and the server for the corresponding measurements to reach the server. The number of routers can vary depending on the communication network architecture.

State estimation service

The state estimation service is one of the most important grid services for performing real-time monitoring of the power system (Abur and Exposito 2004) and is, therefore, considered for this case study. It estimates the power system state variables, namely, the complex bus voltages, based on field measurements from various IEDs. The state estimation used in this paper is a weighted least mean square (WLMS) from Krause et al.

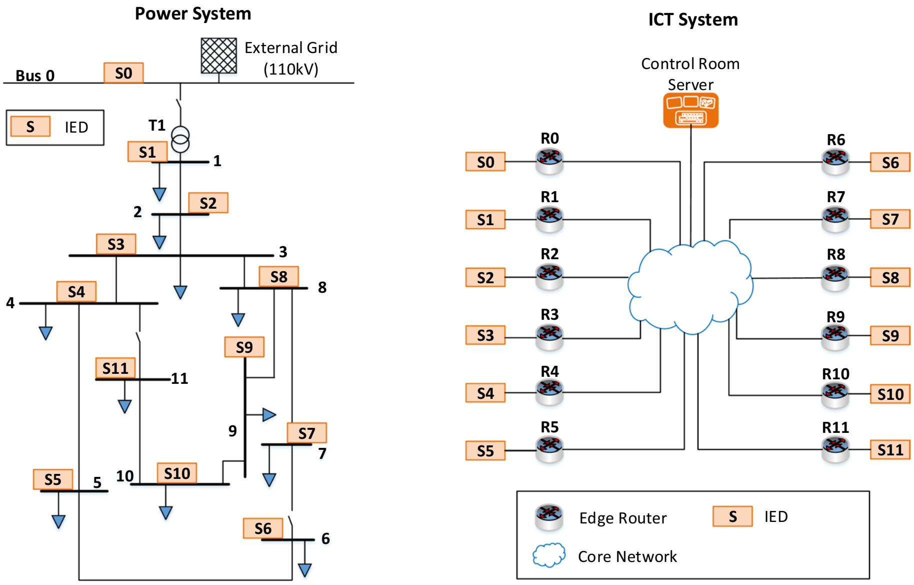

Fig. 3 Cyber-physical energy system considered

(2015). This state estimator is assumed to run centrally in the control room server, where the measurements from the IEDs are received and processed. The WLMS algorithm requires certain field measurements to calculate the state variables, which influences the solvability condition of the service (Krause et al. 2015). ICT disturbances such as failures of IEDs or congestions in the communication network may cause or hinder the timely arrival of specific measurements to the server, possibly violating the solvability condition. Solvability can be satisfied in such cases by substituting the missing measurements with suitable pseudo-measurements, typically calculated based on historical measurements (Abur and Exposito 2004). Consequently, the state estimation results may not capture the recent events in the power grid when pseudo-measurements are used.

Table 3 summarises the operational states of the state estimation service and is based on Narayan et al. (2021). These states inform the system operator about the performance of the grid service, based on which better decisions could be taken. For instance, in the normal state, the operator can confidently use the results of the service to make operational decisions. In contrast, when in the limited state, the results should be used cautiously as recent events may not be captured. Note that, due to the centralised architecture, the failure of the server will cause the state estimation to fail unless a redundant server is present. This will, however, be different for decentral and distributed implementations (Hage Hassan et al. 2023).

Meta model instantiation

This section presents the instantiation of the proposed for the state estimation service mentioned above, considering the power and ICT systems shown in Fig. 3. The instantiation model is shown in Fig. 4, which incorporates the hardware, services and data objects of the ICT system. The 12 IEDs, 12 edge routers, the core router and the server are modelled as hardware objects (shown in blue). The field acquisition services use the IEDs (one service per IED). They wrap the measured parameters from the IEDs in telemetry protocols such as IEC 60870-5-104. This is denoted as wrapped measurements-1 (data object). Although each IED measures two parameters (cf.), they are wrapped and transmitted in the same message, yielding 12 instances of wrapped measurements-1. The ICT transmission services communicate these measurements to the control room using edges and core routers. This service typically consists of routing tables to determine the data flow in the communication network. It can consist of routing protocols such as open shortest path first (OSPF) and border gateway (BGP) (Narayan et al. 2020).

Table 3 Operational states of state estimation service adapted from Narayan et al. (2021)

Normal	• Required field measurements are available on time and are correct • Solvability condition can be met using only field measurements • State estimation results enables correct decision making
Limited	• Certain field measurements are not available on time or are incorrect • Solvability condition can be only be satisfied by using field as well as pseudo measurements (fall-back) • More uncertainty in state estimation results—decision making with caution
Failed	• Certain field measurements are not available on time or are incorrect • Suitable pseudo-measurements are either not available or required in excess • Solvability condition can be met by neither using field nor pseudo measurements • No situational awareness—Cannot take decisions based on state estimation

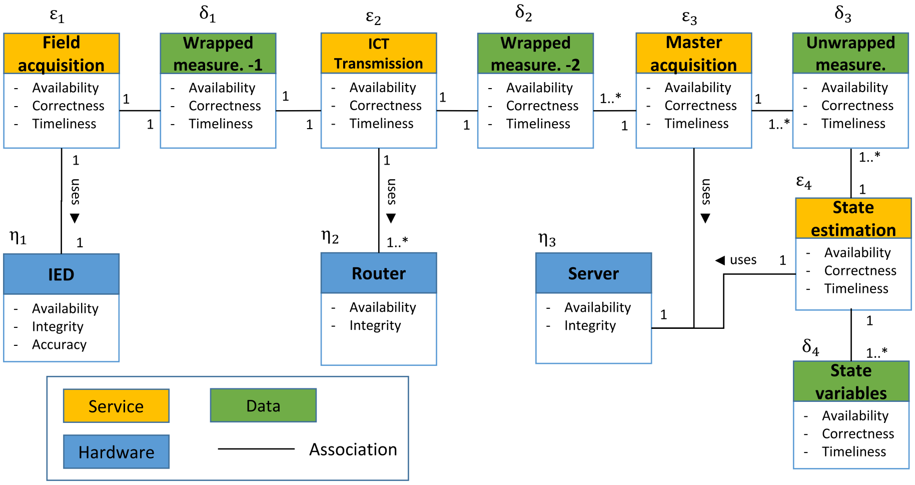

Fig. 4 Instantiated version of Meta model for state estimation service

The wrapped measurements-2 data objects are the output of the ICT transmission services and are received by the master acquisition service running on the server. Here, the measurements are unwrapped from the protocols into 24 individual measurements (12 IEDs measure two parameters each) such that they can be processed by the state estimation service, which, in this case, is the WLMS algorithm running on the same server. The result is a set of power system state variables (data objects) representing the output of the state estimation service. Note that 24 state variables exist, i.e., a voltage magnitude and an angle for each of the 12 buses.

From Fig. 4, it can be observed that the data objects interface different services running on hardware. Therefore, a change in the properties of hardware and service objects, potentially by disturbances or repair actions, propagates through the data objects. This propagation integrates the properties of the service creating the data and that of the hardware the service runs on. This propogation follows the description in Table 1. For example, the availability of wrapped-measurements-1 (data object) depends on the availability of the corresponding field acquisition (service) and the involved IED (hardware). Similarly, the correctness of wrapped measurements-1 depends on the correctness of the corresponding field acquisition as well as the accuracy and integrity of the corresponding IED. Its timeliness, however, depends only on the corresponding field acquisition, as IEDs (hardware) do not have a timeliness property (cf. Fig. 1). A valid communication path should exist for measurements from an IED to reach the server. For example, measurements from *S*5 can reach the server only via *R*5 and the core network (cf. Fig. 3). Therefore, the properties of measurements from *S*5 (an instance of wrapped measurements-1) are impacted by the corresponding properties of *R*5, core router and their respective ICT transmission service. Consequently, the timeliness of the resulting data (wrapped measurements-2) depends on the cumulative timeliness of wrapped measurements-1 and the respective ICT transmission service. Contrary to IEDs, routers do not have the accuracy property as they do not measure power system parameters. The properties of the state variables (output data object of state estimation service) depend on the corresponding properties of unwrapped measurements (data object), state estimation (service) and server (hardware). The timeliness of the state variables would consist of the cumulative timeliness of all the data objects and the services in Fig. 4. From the figure, it is also evident that the properties of the state variables depend on the propagated properties from IEDs till the state estimation service. In a nutshell, while the properties of hardware and services can be initialised and changed based on disturbances and repair actions, the properties of data objects are calculated (or inherited) based on the associated service object and input data object. This propagation is primarily influenced by the type of service and the architecture of the ICT system. Since IEDs are also capable of actuating (or controlling) power system components, the instantiated meta model in Fig. 4 can be adapted to include grid services that depend on the results of state estimation, e.g., coordinated voltage control (Viawan and Karlsson 2008).

As described in Table 3, the availability, timeliness and correctness of the state variables can be used to determine the operational state of the state estimation grid service. Table 4 shows the property thresholds for the operational states of the state estimation service considered in this paper. The availability of state variables is 1.0 if all 24 state variables can be estimated using only field measurements (normal state) or a combination of field and pseudo-measurements (limited state). As per (Kansal and Bose 2012), the state estimation is assumed to run every 5 s, which yields the timeliness threshold. The thresholds for correctness are arbitrarily defined as shown in Table 4. While a minor decrease in correctness (until 0.90) is acceptable in the normal state, a further decrease will cause the state estimation service to transition to the limited state. However, a large decrease in correctness (less than 0.75) will result in the failed state. These thresholds can be used to construct the proposed and can be easily adapted depending on the requirements of the system operator. It is to be noted that the thresholds in Table 4 just represent one possibility from literature to define the operational states. Further examples of such thresholds for different grid services can be found in Narayan et al. (2020); Das et al. (2021); Kansal and Bose (2012); Kuzlu et al. (2014). Using different thresholds, however, will result in different regions in the state space as well as different state transitions corresponding to disturbances and repair actions.

Properties propagation

The section formalises the propagation of properties for the state estimation service in Fig. 4. To do so, the hardware, service and data objects, along with their properties, are modelled. Let η, ϵ and δ denote hardware, service and data objects, respectively. Based on Fig. 4, Table 5 presents the nomenclature used in the formalisation and the initial values of the properties. These values are adapted from Brand et al. (2019, 2021) and are chosen to illustrate different aspects of the meta model and the operational state space. While properties of hardware and service objects can be initialised,

Table 4 Property thresholds for the operational states of state estimation service

	Availability	Timliness	Correctness
Normal	1.0	≤ 5 s	[0.9, 1.0]
Limited	1.0	≤ 5 s	(0.9, 0.75]
Failed	< 1.0	> 5 s	< 0.75

Table 5 Nomenclature and initial values of properties in Fig. 4

Objects		Properties	Initial value
$\eta_1 = \{\eta_{1,1}, \eta_{1,2}, \ldots\}$	Set of IEDs	η_1^A	1
		η_1^I	1
		η_1^P	0.99
$\eta_2 = \{\eta_{2,1}, \eta_{2,2}, \ldots\}$	Set of edge and core routers	η_2^A	1
		η_2^I	1
η_3	Server in control room	η_3^A	1
		η_2^I	1
$\epsilon_1 = \{\epsilon_{1,1}, \epsilon_{1,2}, \ldots\}$	Set of field acquisition services	ϵ_1^A	1
		ϵ_1^T	0.2s
		ϵ_1^C	1
$\epsilon_2 = \{\epsilon_{2,1}, \epsilon_{2,2}, \ldots\}$	Set of ICT transmission services	ϵ_2^A	1
		ϵ_2^T	0.4s
		ϵ_2^C	1
ϵ_3	Master acquisition service	ϵ_3^A	1
		ϵ_3^T	0.1s
		ϵ_3^C	1
ϵ_4	State estimation service	ϵ_4^A	1
		ϵ_4^T	5s
		ϵ_4^C	1
$\delta_1 = \{\delta_{1,1}, \delta_{1,2}, \ldots\}$	Set of wrapped measurements-1 (output of field acquisition)	δ_1^A	Calc
		δ_1^T	Calc
		δ_1^C	Calc
$\delta_2 = \{\delta_{2,1}, \delta_{2,2}, \ldots\}$	Set of wrapped measurements-2 (output of ICT transmission)	δ_2^A	Calc
		δ_2^T	Calc
		δ_2^C	Calc
$\delta_3 = \{\delta_{3,1}, \delta_{3,2}, \ldots\}$	Set of unwrapped measurements (output of master acquisition)	δ_3^A	Calc
		δ_3^T	Calc
		δ_3^C	Calc
$\delta_4 = \{\delta_{4,1}, \delta_{4,2}, \ldots\}$	Set state variables (output of state estimation)	δ_4^A	Calc
		δ_4^T	Calc
		δ_4^C	Calc

Calc indicates the properties that are calculated based on other initial values

the properties of the data objects are calculated (denoted as 'calc' in the table) based on the corresponding hardware and services.

The sets in Table 5 indicate the presence of multiple instances of the same object, e.g., the ICT system in Fig. 3 has several IEDs but only one server. Specifically, the ICT network consists of 12 IEDs ($|\eta_1| = 12$) with 12 corresponding edge routers and a core router ($|\eta_2| = 13$). The measurements from the IEDs are wrapped by the corresponding field acquisition service in each IED ($|\epsilon_1| = 12$) and communicated by an ICT transmission service per IED ($|\epsilon_2| = 12$). Since the measurements from the IEDs are wrapped and transmitted as a single message, $|\delta_1| = |\delta_2| = 12$. However, these measurements are unwrapped at the master acquisition and, therefore, $|\delta_3| = 24$ (2 measurements per IED). Finally, the unwrapped measurements are processed by the state estimation service, resulting in 24 state variables ($|\delta_4| = 24$). As discussed in the previous section, the properties of hardware and services can be instantiated, while the properties of data objects are calculated based on the properties of associated hardware and services.

Let the properties of the objects be denoted as availability A, timeliness T, accuracy P, integrity I and correctness C. For example, η_3^A and η_3^I represent the availability and integrity of the server (hardware). Since the state variables (δ_4) are the output of state estimation, their properties are of interest to the operational state classification. The availability of state variables $\delta_4^A \in [0, 1]$, shown in Eq. (1), is calculated as the product of availabilities of server η_3^A, state estimation service ϵ_4^A as well as the availability of unwrapped measurement data δ_3^A. Let f^o be a function representing the observability calculations, which takes δ_3^A as input. This calculation is an essential part of a state estimation service and is shown in Abur and Exposito (2004). This function yields 1 if the power grid is observable with the available δ_3^A and 0 otherwise. In this regard, the calculation of all the 24 state variables is possible only if the grid is observable, i.e., $f^o(\delta_3^A) = 1$. Since a central state estimation with a single server is considered, the terms η_3^A and ϵ_4^A are multiplied. This represents a single point of failure for the hardware (η_3) and service (ϵ_4), and can be adapted accordingly in the case of redundant servers. $\delta_4^A = 1$ indicates that all 24 state variables can be estimated, whereas $\delta_4^A = 0$ indicates that none of the state variables can be calculated (no observability).

$$\delta_4^A = \eta_3^A \cdot \epsilon_4^A \cdot f^o(\delta_3^A) \tag{1}$$

$$\delta_3^A = \eta_1^A \cdot \epsilon_1^A \cdot \eta_2^A \cdot \epsilon_2^A \cdot \eta_3^A \tag{2}$$

Equation (2) denotes the availability of the unwrapped measurements (δ_3^A) in Eq. (1). For a measurement from a particular IED to be available at the master acquisition, the corresponding IED, field acquisition, ICT transmission, router and the master acquisition service itself should be available (cf. Fig. 3). As a result, the terms in Eq. (2) are multiplied. The term $\eta_2^A \cdot \epsilon_2^A$ denotes a communication path between the corresponding IED and the master acquisition (through the field acquisition service). All terms in Eqs. (1) and (2) are binary, representing the availability of the corresponding objects. Note that the number of IEDs, routers, field acquisition and ICT transmission can vary depending on the implementation of the grid service. Although master acquisition and state estimation services run on the same server η_3, its availability η_3^A appears only once in the above equations. This is due to the binary and multiplicative nature of the availability property, implying that it is sufficient to consider the term only once.

The timeliness of state variables in Fig. 4 can be computed as the sum of the timeliness of the objects the data flows through. This is shown stepwise in Eqs. (3)–(6). The timeliness of state variables δ_4^T consists of the processing time of the state estimation service ϵ_4^T and the timeliness of the received measurements δ_3^T. While the former is an intrinsic property of the state estimation service, the latter, as shown in Eq. (4), is the sum of the processing latency at master acquisition, and the worse-case (maximum) delay among the wrapped measurements-2 (δ_2) received. This is because, in order to have the most updated monitoring of the power grid, measurements are processed at the master acquisition only when the required ones are received. Since measurements have different communication paths, they can have different timeliness values depending on the corresponding ICT transmission service. This is shown in Eq. (5). When public communication networks are used, like in the case of distribution grids, the value of ϵ_2^T can only be estimated as the average delay through the network (Kuzlu et al. 2014). Finally, Eq. (6) represents the timeliness of the wrapped measurements-1, which is solely determined by the processing time of the field acquisition service. Note that timeliness is a positive float (i.e., ≥ 0) and is measured in seconds.

$$\delta_4^T = \epsilon_4^T + \delta_3^T \tag{3}$$

$$\delta_3^T = \epsilon_3^T + max(\delta_{2,j}^T, \forall j \in \delta_2) \tag{4}$$

$$\delta_2^T = \epsilon_2^T + \delta_1^T \tag{5}$$

$$\delta_1^T = \epsilon_1^T \tag{6}$$

By substituting Eqs. (4)–(6) in Eq. (3), the timeliness of the state variables can be written as shown in Eq. (7). δ_4^T can then be used to assess the state of the state estimation service and plot the corresponding operational state space.

$$\delta_4^T = \epsilon_4^T + \epsilon_3^T + max(\epsilon_2^T + \epsilon_1^T). \tag{7}$$

As shown in Eq. (8), the correctness of the state variables δ_4^C in Fig. 4 can be computed as the minimum of correctness of state estimation service (ϵ_4^C), integrity of the server (η_3^I) and the correctness of unwrapped measurements (δ_3^C). Let f^k be a function for mapping the dependency of the state variables on the unwrapped measurements. f^k basically represents the sensitivities of the state variables on the measurements, and its calculation is specific to the state estimation algorithm used. One example for calculating f^k can be found in Brand et al. (2021). In Eq. (8), the function f^k links the correctness of the 24 unwrapped measurements(δ_3^C) to that of the 24 state variables (δ_4^C). The equations for correctness presented in this paper assume the worst-case and, therefore, the individual correctness of the objects is aggregated as the minimum correctness. This could, however, be easily replaced by suitable alternatives. Equation (9) shows the correctness of the unwrapped measurements, which is determined by the minimum of correctnesses of master acquisition (ϵ_3^C), integrity of the server (η_3^I) and correctness of wrapped measurements-2 (δ_2^C). In contrast to the availability, correctness is neither binary nor multiplicative. Therefore, the integrity of server η_3^I appears both in Eqs. (8) and (9), especially because the master acquisition and state estimation services use the same server η_3. While ϵ_3^C and η_3^I are intrinsic properties of master acquisition and server, respectively, the property δ_2^C is shown in Eq. (10) as the minimum of the correctness of ICT transmission service (ϵ_2^C), the integrity of routers (η_2^I) and the correctness of wrapped measurement-1 (δ_1^C). Eq. (11) shows the correctness of the wrapped measurement-1 and follows the same structure as Eq. (10). Since IEDs measure the physical parameters of the power grid, both its integrity and accuracy are considered in the calculation of the correctness of wrapped measurement-1. Note that the value of correctness lies in the interval [0, 1], with 1 being the best possible value. Since sensors, in this case, IEDs are typically associated with standard deviations, the accuracy of IEDs is initialised at 0.99 (indicating 1% deviation) and is shown in Table 5.

$$\delta_4^C = min(\epsilon_4^C, \eta_3^I, f^k(\delta_3^C)) \tag{8}$$

$$\delta_3^C = min(\epsilon_3^C, \eta_3^I, \delta_2^C) \tag{9}$$

$$\delta_2^C = min(\epsilon_2^C, \eta_2^I, \delta_1^C) \tag{10}$$

$$\delta_1^C = min(\epsilon_1^C, \eta_1^I, \eta_1^P) \tag{11}$$

Similar to timeliness, Eqs. (9)–(11) can be substituted in Eq. (8) to summarise the correctness property of state variables as Eq. (12). To plot the operational state space, a single correctness value is required for δ_4^C. This is calculated as the minimum correctness of the 24 state variables.

$$\delta_4^C = min(\epsilon_4^C, \eta_3^I, f^k(\epsilon_3^C, \eta_3^I, \epsilon_2^C, \eta_2^I, \epsilon_1^C, \eta_1^I, \eta_1^P)) \tag{12}$$

Results and discussion

This section presents a simulation-based proof of concept to demonstrate the propagation of properties through the proposed model and the operational state space. An overview of the scenarios considered is first provided, followed by the simulation results and the operational state trajectories of the state estimation service. The initial values of the properties of Fig. 4 are shown in Table 5. Note that the meta model and the WLMS state estimator from Krause et al. (2015) are both implemented and simulated in Java. The details of the benchmark grids used can be found in https://pandapower.readthedocs.io/en/v2.13.1/networks/cigre.htmlmedium-voltage-distribution-network.

Disturbance scenarios

Disturbances in the ICT system can be associated with ICT components (hardware) and software (services), and their impact on the properties of the data can be calculated as shown in . Exemplary ICT disturbances, shown in Table 6, are chosen to illustrate the resulting impact on the operational state of state estimation. IED failures can occur due to hardware or software problems, while congestion can result from excess data traffic in the communication network. A cyber-attack occurs if hackers exploit vulnerabilities in the ICT components. Failures in the state estimation service can be due to software bugs causing the grid service to fail. Note that the disturbances with the same number are assumed to occur successively, building upon one another.

Four simulation scenarios are presented in this paper as a proof of concept for the proposed meta model and the operational state space. These scenarios include different disturbances, such as hardware and service failures, congestions and cyber-attacks. While the disturbances in Scenario 1 focus on the power system field devices

Table 6 Disturbance scenarios considered and their impact on the properties

Scenario	Description	Impact on availability, timliness and correctness properties
0	Initial baseline. No disturbance.	No impact on properties
1a	Redundant IED failed	Availability of S9 is set to false ($\eta^A_{1,9} = 0$)
1b	Cyber-attack—hacker gains access to more and more IEDs	Integrity of S0 is set to 0.12 ($\eta^I_{1,0} = 0.12$)
1c		Integrity of S0, S1 is set to 0.12 ($\eta^I_{1,0} = \eta^I_{1,1} = 0.12$)
1d		Integrity of S0, S1, S2 is set to 0.12 ($\eta^I_{1,0} = \eta^I_{1,1} = \eta^I_{1,2} = 0.12$)
1e		Integrity of S0, S1, S2, S3 is set to 0.12 ($\eta^I_{1,0} = \eta^I_{1,1} = \eta^I_{1,2} = \eta^I_{1,3} = 0.12$)
2a	Congestion in communication Network	Timeliness of ICT transmissions is set to 2.7s ($\epsilon^T_1 = 2.7$)
3a	State estimation software crashed due to bug	Availability of state estimation service is set to false ($\epsilon^A_4 = 0$)
3b	Software bug was fixed but with incorrect data	Correctness of field acquisition on $S2$ and $S3$ is set to 0.5 ($\epsilon^C_{1,2} = \epsilon^C_{1,3} = 0.5$)

and are based on the case study in Brand et al. (2019), Scenario 3 is designed as per the disturbances causing the 2003 North American blackout shown in NERC (2004). Scenario 2 focuses on the communication network, which transfers data from the field to the control room.

Scenario 0 represents the baseline scenario, where no disturbance is considered and is designed such that the properties of the grid service are within their normal state thresholds as per Table 4. In this scenario, the state estimation service receives all the measurements and delivers the output as expected. The three other scenarios are assumed to build on Scenario 0. In Scenario 1, the disturbance sequence d_{1a}, d_{1b}, d_{1c}, d_{1d}, d_{1e} is considered. Disturbance d_{1a} is a hardware failure resulting in the loss of IED $S9$, thus impacting its availability. This is followed by a cyber-attack, where a hacker sequentially gains access to the IEDs $S0$, $S1$, $S2$ and $S3$ (i.e., d_{1b}, d_{1c}, d_{1d}, d_{1e}). The hacker can manipulate the measurements from these IEDs, thereby affecting their integrity property, reducing it from 1 (ideal value) to 0.12. The integrity of data from hardware can be measured using intrusion detection systems, as shown in Brand et al. (2019).

Scenario 2 has the disturbance d_{2a} representing the congestion in the communication network. Here, the timeliness of the ICT transmission services is increased from 0.4s to 2.7s to simulate congestion in the core network. This impacts the transmission of measurements, causing the delayed arrival of field measurements at the server located in the control room. Consequently, these measurements are not processed by the master acquisition and the state estimation services. The disturbance sequence in Scenario 3 is d_{3a} and d_{3b}. Disturbance d_{3a} represents a software bug causing the state estimation service to crash. This can be modelled by changing the availability of the service from one to zero, i.e., $\epsilon^A_4 = 0$. This software bug is assumed to be remedied (ϵ^A_4 is set to 1), thereby restoring the functionality of the service. This is, however, done using outdated measurements from IEDs $S2$ and $S3$, which is modelled by reducing the correctness of the corresponding field acquisitions from 1 to 0.5, i.e., $\epsilon^C_{1,2} = \epsilon^C_{1,3} = 0.5$. d_{3b} corresponds to this action using outdated measurements.

Operational state trajectories for state estimation

The disturbance scenarios presented in Table 6 are simulated using the instantiated meta model from Fig. 4. The results, in terms of the availability, timeliness and correctness of the state variables data object (output of state estimation δ_4), are visualised using trajectories in the proposed Operational state space. The axes in Fig. 5, Fig. 6 and Fig. 7 correspond to the properties δ_4^A, δ_4^T and δ_4^C. Since all state variables must be estimated for the state estimation service to be in its normal or limited state (cf. Table 4), the corresponding regions are flat surfaces at $\delta_4^A = 1$. Scenario 0 is assumed to be the starting point for the other three scenarios and is indicated by T_0 in the figures. As mentioned earlier, this baseline scenario is designed such that the properties of state variables are within the normal state thresholds. This state indicates that all state variables can be estimated, satisfying the timeliness and correctness thresholds.

Figure 5 shows the trajectory of the state estimation service for the disturbances in Scenario 1. The points in the state space indicate the impact of the corresponding disturbances. It can be seen that the disturbance d_{1a} (loss of $S9$) does not impact the properties of the state variables, and the grid service remains in the normal state (indicated by T_{1a}). This implies the corresponding IED $S9$ is redundant, i.e., all the state variables can be estimated despite the loss of measurements from this IED. Redundant measurements are relevant in implementing grid services as they increase robustness against loss of measurements (Abur and Exposito 2004). However, the cyber-attack on IED $S0$ degrades the correctness of the state variables from 0.93 to

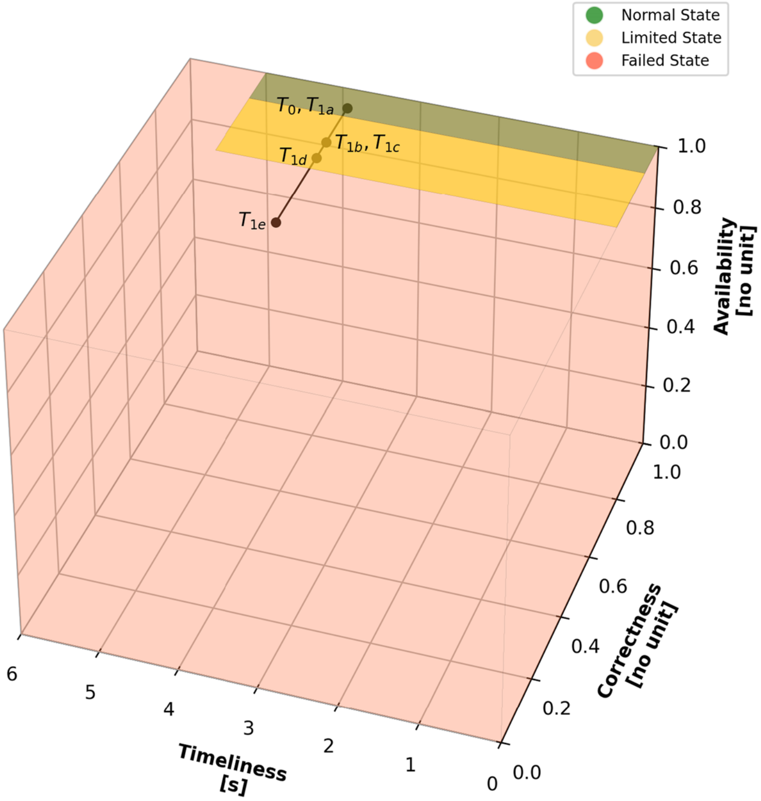

Fig. 5 Operational state trajectory of state estimation service: Scenario 1

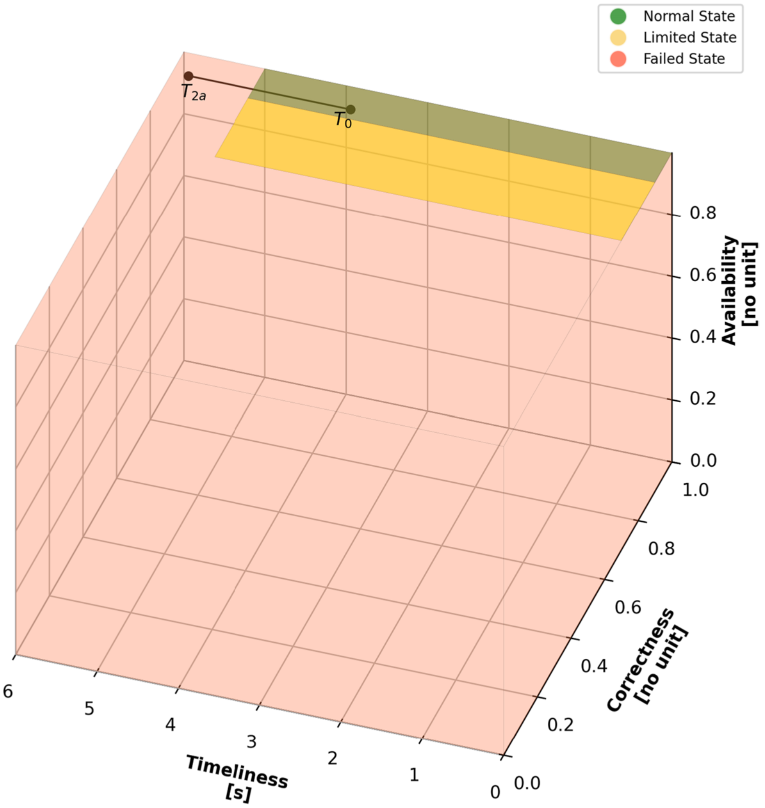

Fig. 6 Operational state trajectory of state estimation service: Scenario 2

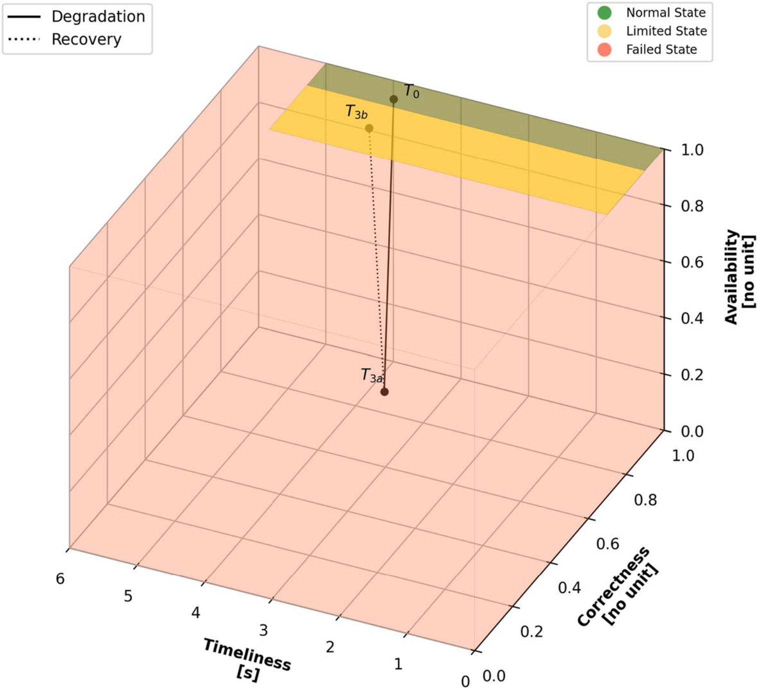

Fig. 7 Operational state trajectory of state estimation - Scenario 3

0.80, causing a degradation to the limited state (indicated by T_{1b}). Based on this, the system operator is informed that the state estimation service must be used cautiously. d_{1b} decreases the integrity of the measurements, which propagate through the other objects in Fig. 4 to impact the correctness of the state variables. The next disturbance d_{1c} impacts the integrity of IED $S1$ but, contrary to d_{1b}, does not degrade the correctness of state variables. Consequently, the grid service remains in a limited state (indicated by T_{1c}), which implies that $S1$ is also redundant. Although the disturbance d_{1d} results in a decrease in the correctness of state variables from 0.80 to 0.76, the grid service is still in the limited state (indicated by T_{1d}) but is more critical than T_{1d} as it is closer to the failed state. The last disturbance d_{1e}, also a part of the cyber-attack impacting the integrity of IEDs, degrades the correctness of state variables to 0.5, causing the grid service to enter the failed state (indicated by T_{1e}). In this case, the system operator cannot use the output for situational awareness and has to take suitable actions to recover the state of the grid service. The trajectory of Scenario 1 shows the state degradation of the grid service due to the correctness property, particularly the ability of the proposed model to analyse the propagation of integrity from field IEDs to the state variables. It also shows the proposed operational state space can depict not only the discrete operational states but also their severity without increasing the total number of states.

Figure 6 shows the trajectory of the state estimation service for the disturbance in Scenario 2. As mentioned earlier, the state estimation service is initialised in its normal state (T_0). The disturbance d_{2s} represents congestion in the communication network, increasing the timeliness of the core network. This delays the transfer of data from the field to the server located in the control room, which in turn delays the calculation of state variables by the state estimation service. Consequently, the timeliness of state variables is increased from 3.8s to 5.8s. The new timeliness corresponds to the failed state as per Table 4, since the state variables are required within 5 s. Scenario 2 shows the state degradation of the grid service due to the timeliness property and the ability of the proposed model to analyse the impact of the timeliness of communication network components on the state variables. Based on this, the system operator could take countermeasures like the ones discussed in Oest and Lehnhoff (2022) and Narayan et al. (2020) to relieve the congestion in the core network.

Figure 7 shows the trajectory of the state estimation service for the disturbances in Scenario 3. From the initial state T_0, the disturbance d_{3a} represents a crash of the state estimation service, decreasing its availability to zero ($\delta_4^A = 0$). This degrades the grid service to its failed state (indicated by T_{3a}). In this state, the service can no longer calculate the state variables, resulting in a loss of situational awareness to the operator. While aiming to remedy the software bug, the operator used outdated (incorrect) measurements corresponding to IEDs $S2$ and $S3$. Although this action improved the availability of state variables to one ($\delta_4^A = 1$), it degraded their correctness, i.e., δ_4^A, from 0.93 to 0.88. This correctness corresponds to the limited state as per Table 4. In this state, the system operator should use the grid service with caution, while aiming to recover it to the normal state. The trajectory of Scenario 3 shows the state degradation of the grid service due to the available property, particularly the ability of the proposed model to analyse not only the impact of disturbances but also of suitable repair actions.

Summary and implications

The simulation scenarios show that the meta model (first contribution) can analyse the impact of different disturbances (e.g., IEDs failures, cyber attacks, congestion and software bugs) on the ICT-enabled grid services, which in this case is state estimation. Specifically, the disturbances are mapped as changes in availability, timeliness and/or correctness (cf. Table 6) of different ICT components such as hardware, services and data. These are then propagated across the model to determine the impact on the properties of state variables, which is the output of the grid service. This approach could be easily extended to consider additional grid services by the corresponding instantiation of the meta model. Using this, the propagation of properties across dependent grid services can also be modelled and investigated, for example, a voltage control service that uses the output of state estimation. The operational state space (second contribution) can then be used to plot the change in the properties from the meta model to capture the performance of the grid service. These state trajectories depict how disturbances build upon one another in terms of availability, timeliness and correctness. Since regions in the state space correspond to the operational states, the trajectory can also indicate state transitions. As shown by T_0 and T_{1a} in Fig. 5, the trajectories can also capture the impact of measures such as redundancy, which can increase the robustness of the grid services against disturbances. This can be used to investigate the benefits of different robustness and resilience measures that can potentially improve the performance of grid services under consideration of different disturbances.

The unique aspects of this paper that set it apart from existing liteature (cf.) are the incorporation of multiple ICT component properties, especially correctness and the ability to visualise the impact of property propagation as trajectories in the operational state space of an ICT-enabled grid service. The approach presented in Avizienis et al. (2004) and des grands (2014) considers only component failures and, therefore, can only analyse disturbances $1a$ and $3a$ (cf. Table 6). They are not capable of considering the other disturbances, i.e., cyber-attacks ($1b - 1e$), congestion ($2a$) and incorrect repair actions ($3b$). Although the approach in Konig and Nordstrom (2009) considers properties of ICT components, data errors are only represented by accuracy. While accuracy is a static property capturing only errors in metering and software algorithms, correctness is dynamic and can also capture data manipulations (Narayan et al. 2021). Therefore, this approach cannot analyse the cyber-attacks $1b - 1e$. The proposed meta model incorporates both of these properties. Furthermore, the visualisation of the propagation of disturbances and their impact on the performance of a grid service is a novel contribution of this paper and, to the best of our knowledge, has not been found in the existing literature. The proposed state space enables a better understanding of the results of meta model and can potentially be used by system operators to monitor the performance of different grid services in the control room.

Limitations and future work

As discussed in , the operational states of grid services are a fundamental prerequisite for this paper. While the states of grid services with central architectures have been well-established in literature (Klaes et al. 2020; Narayan et al. 2021; Haack et al. 2022), the states of decentral and distributed architectures are an ongoing research (Hage Hassan et al. 2023). This limits the applicability of the proposed operational state space to grid services with such architectures, which is essential considering the rising prominence of multi-agent systems in CPESs (Nieße and Tröschel 2016). However, the proposed meta model is designed to be sufficiently generic to also model such architectures, and future work entails applying the meta model to decentral and distributed grid services. Along these lines, the model should be applied to grid services with control capabilities (e.g., on-load tap changer-based voltage control).

CPESs are geographically large-scale systems with numerous components. Correspondingly, instantiating the meta model for grid services with a large number of components and properties could be cumbersome. This is aggravated by the fact that a CPES can have different operators, each being responsible for a part of the system. For example, the transmission or distribution system operator could own field devices such as IEDs and servers, while the public internet could be used as the communication network, which is owned by a telecommunication operator. Renewable energy sources, if present, could be owned by consumers and other small companies. In such cases, having knowledge of the properties of all components in the CPES is often infeasible. A balance should then be established between the required level of detail and the modelling effort. Different parts of the CPES could be abstracted depending on the interests of stakeholders. For instance, if cyber threats on field IEDs are of interest, the communication network could be abstracted, considering historical average values for its properties. In this regard, testing the scalability of the meta model for larger CPESs with different operators is also an important next step.

The three simulation scenarios show that disturbances and repair actions can be mapped onto the meta model by suitably modifying the corresponding properties. However, disturbances such as coordinated cyber attacks or software bugs could be hidden and could impact a large number of components (Wäfler and Heegaard 2013), implying that the corresponding change in properties is often not known. This makes it challenging to map such disturbances onto the meta model. In such cases, monitoring systems such as the ones proposed in Brand et al. (2019); Chromik et al. (2018) are required to detect such disturbances and identify the change in properties, which can then be mapped onto the proposed meta model. Integrating such monitoring systems and testing the model for a wide range of disturbances and repair actions is also part of future work.

Conclusion

This paper presents a meta model for ICT-enabled grid services in CPESs, incorporating different ICT components such as hardware, services and data. Services run on hardware and process input data to provide required output data. The meta model also incorporates properties specific to the ICT components. The model can be used to analyse the propagation of properties caused by disturbances or repair actions across the ICT components and determine the impact on the performance of the grid service. A multi-dimensional operational state space is also proposed to visualise the performance of ICT-enabled grid service. The state space is constructed using three properties, namely availability, timeliness and correctness, of the output from the grid service. The two contributions of this paper, i.e., the meta model and the operational state space, are demonstrated using the CIGRE medium voltage benchmark power grid and a suitable ICT system with the state estimation as an exemplary grid service. Simulation scenarios considering sequences of ICT disturbances such as cyber-attacks, congestion and hardware failures are presented and discussed. The resulting impact on the properties of state variables, i.e., the output from state estimation, is calculated by instantiating the meta model for the state estimation service. This is visualised as trajectories in the operational state space. The results show that the proposed model can map the variations in properties of ICT components caused by disturbances in the output of the grid service, thereby aiding vulnerability analysis in CPESs. The state space can indicate not only the current state but also the criticality of the grid service in the state.

The contributions are, however, only applied to centralised grid services, making their application to decentralised and distributed services part of future work. Applying the meta model for large-scale systems could be challenging due to many components and properties. Furthermore, the model should also be evaluated by considering further disturbances and repair actions. This can potentially yield trajectories where the state of the grid service returns to the initial state which can further be used to assess the resilience of the grid service. By considering more disturbances and repair actions, the trajectories could also be used to predict future states and facilitate preventive actions.

Abbreviations

BGP	Border gateway protocol
CIGRE	International Council on Large Electric Systems
CPES	Cyber-physical energy systems
ICT	Information and communication technology
IED	Intelligent electronic device
OSPF	Open shortest path first
RTU	Remote terminal unit
UML	Universal markup language
WLMS	Weighted least mean squares

Acknowledgements
Not applicable.

Author contributions
The authors A.N. and B.H. developed the operational state space, while M.B. developed the meta model. M.B and N.H. implemented the meta model. A.N and B.H. developed the case studies to demonstrate the contributions. The paper was jointly written by A.N. and M.B. N.H. and B.H. prepared the figures and the simulation results. S.L. contributed to the paper with expert guidance in the field and review. All authors read and approved the final manuscript.

Funding
Open Access funding enabled and organized by Projekt DEAL. 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

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 20 December 2023 Accepted: 6 March 2024
Published online: 26 March 2024

References

Abur A, Exposito AG (2004) Power system state estimation: theory and implementation. CRC press, Boca Raton

Antoniadou-Plytaria KE, Kouveliotis-Lysikatos IN, Georgilakis PS, Hatziargyriou ND (2017) Distributed and decentralized voltage control of smart distribution networks: models, methods, and future research. IEEE Trans Smart Grid 8(6):2999–3008

Avizienis A, Laprie J-C, Randell B, Landwehr C (2004) Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secure Comput 1(1):11–33

Brand M, Ansari S, Castro F, Chakra, R, Hassan BH, Krüger C, Babazadeh D, Lehnhof S (2019) A framework for the integration of ict-relevant data in power system applications. In: 2019 IEEE Milan PowerTech, pp. 1–6 . IEEE

Brand M, Babazadeh D, Lehnhoff S (2021) Trust in power system state variables based on trust in measurements. In: 2021 IEEE Madrid PowerTech, pp. 1–6 . IEEE

Brown MA, Zhou S (2012) Sustainable smart grids, emergence of a policy framework. In: Electrical transmission systems and smart grids: selected entries from the encyclopedia of sustainability science and technology, pp. 271–318. Springer, New York

Chromik JJ, Remke A, Haverkort BR (2018) An integrated testbed for locally monitoring scada systems in smart grids. Energy Inform 1(1):1–29

CIGRE Medium voltage distribution network. https://pandapower.readthedocs.io/en/v2.13.1/networks/cigre.htmlmedium-voltage-distribution-network

Cortellessa V, Grassi V (2007) A modeling approach to analyze the impact of error propagation on reliability of component-based systems. In: Component-Based Software Engineering: 10th International Symposium, CBSE 2007, Medford, MA, USA, July 9-11. Proceedings 10, pp. 140–156 (2007). Springer

Das P, Narayan A, Babazadeh D, Baboli PT, Lehnhoff S (2021) Real-time context-aware operation of digitalized power systems by reporting rate control of pmus. In: 2021 IEEE Madrid PowerTech, pp. 1–6 . IEEE

des grands réseaux électriques. Comité&nbsp;d'études C6, C.I.: Benchmark Systems for Network Integration of Renewable and Distributed Energy Resources. Cigré, Paris (2014)

Haack J, Narayan A, Patil AD, Klaes M, Braun M, Lehnhoff S, de Meer H, Rehtanz C (2022) A hybrid model for analysing disturbance propagation in cyber-physical energy systems. Electric Power Syst Res 212:108356

Hage HB, Narayan A, Brand M, Lehnhoff S (2023) Modeling of Resilient State Estimation in Cyber-physical Energy Systems. In: Abstracts of the 12th DACH+ Conference on Energy Informatics. DACH+ Conference on Energy Informatics, vol. 6 (Suppl 2). Springer, New York. https://doi.org/10.1186/s42162-023-00272-5

Kansal P, Bose A (2012) Bandwidth and latency requirements for smart transmission grid applications. IEEE Trans Smart Grid 3(3):1344–1352

Klaes M, Narayan A, Patil AD, Haack J, Lindner M, Rehtanz C, Braun M, Lehnhoff S, Meer H (2020) State description of cyber-physical energy systems. Energy Inform 3(1):1–19

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

Konig J, Nordstrom L (2009) Assessing impact of ict system quality on operation of active distribution grids. In: 2009 IEEE Bucharest PowerTech, pp. 1–8 . IEEE

Krause O, Martin D, Lehnhoff S (2015) Under-determined wlms state estimation. In: 2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–6 . IEEE

Krüger C, Narayan A, Castro F, Hassan BH, Attarha S, Babazadeh D, Lehnhoff S (2020) Real-time test platform for enabling grid service virtualisation in cyber physical energy system. In: 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 109–116 . IEEE

Lu Z, Wei M, Lu X (2017) How they interact? understanding cyber and physical interactions against fault propagation in smart grid. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pp. 1–9 . https://doi.org/10.1109/INFOCOM.2017.8057061. IEEE

Mangalwedekar S, Surve SK, Mangalvedekar H (2015) Error propagation in linear and non-linear systems for false data injection attack. In: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 662–667 . https://doi.org/10.1109/ICACCI.2015.7275686. IEEE

Narayan A, Hassan BH, Attarha S, Krüger C, Babazadeh D, Lehnhoff S (2020) Grid function virtualization for reliable provision of services in cyber-physical energy systems. In: 2020 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5 . IEEE

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), pp. 522–529 . IEEE

NERC: Technical Analysis of the August 14, 2003 Blackout: What Happened, Why, and What Did We Learn? Report to the NERC Board of Trustees by the NERC Steering Group. System, 1–119 (2004)

Nieße A, Tröschel M (2016) Controlled self-organization in smart grids. In: 2016 IEEE International Symposium on Systems Engineering (ISSE), pp. 1–6 . IEEE

Oest F, Lehnhoff S (2022) Constraint-based Modeling of Smart Grid Services in ICT-Reliant Power Systems. In: ENERGY 2022, The Twelfth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, pp. 15–21. IARIA XPS Press, Lisbon

Panteli M (2013) Impact of ICT reliability and situation awareness on power system blackouts. Doctor thesis, The University of Manchester

Pillitteri VY, Brewer TL, (2014) Guidelines for smart grid cybersecurity. Technical report. https://doi.org/10.6028/NIST.IR.7628r1

Popic P, Desovski D, Abdelmoez W, Cukic B (2005) Error propagation in the reliability analysis of component based systems. In: 16th IEEE International Symposium on Software Reliability Engineering (ISSRE'05), p. 10 . IEEE

Shi H, Xie L, Peng L (2021) Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method. Comput Electr Eng 91:107058

Sturaro A, Silvestri S, Conti M, Das SK (2016) Towards a realistic model for failure propagation in interdependent networks. In: 2016 International Conference on Computing, Networking and Communications (ICNC), pp. 1–7 . IEEE

Viawan, FA, Karlsson D (2008) Coordinated voltage and reactive power control in the presence of distributed generation. In: 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–6 . IEEE

Wäfler J, Heegaard PE (2013) Interdependency modeling in smart grid and the influence of ict on dependability. In: Meeting of the European Network of Universities and Companies in Information and Communication Engineering, pp. 185–196. Springer

Wu Y, Nordström L, Bakken DE (2015) 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), pp. 478–484 . IEEE

Publisher's Note