Brand *et al. Energy Informatics* 2023, **6**(Suppl 1):19
https://doi.org/10.1186/s42162-023-00276-1

Energy Informatics

RESEARCH Open Access

Assess: anomaly sensitive state estimation with streaming systems

Michael Brand[1*], Dominik Engel[2] and Sebastian Lehnhoff[1]

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

*Correspondence:
michael.brand@offis.de

[1] OFFIS – Institute for Information Technology, Escherweg 2, 26121 Oldenburg, Germany
[2] Salzburg University of Applied Sciences, Urstein Süd 1, 5412 Puch bei Hallein, Austria

Abstract

Information and communication technology (ICT) is an increasing part of modern power systems, which are, therefore, recognised as cyber-physical energy system (CPESs). The increase of ICT affects the situational awareness in CPESs, which is traditionally solely based on information about the power system but not about the ICT system. However, CPESs are facing various challenges regarding the integrity, correctness, and availability of process data due to the interconnection with ICT. Examples are stealthy false data injection attack (FDIAs). This paper pursues a holistic approach to describe the quality of process data, which brings together aspects like integrity, correctness, and availability in multivariate trust values. The arising research question this paper deals with is, how multivariate trust in physical measurements in a CPES can be modelled, estimated, and integrated into situational awareness. A proposed framework implements a context-sensitive and multivariate trust model as well as a trust sensitive state estimation. While these two artefacts are already published, the focus of this paper is on the implementation of the framework and the fulfilment of the requirements for timeliness, interoperability, flexibility, and scalability. It is evaluated in three different scenarios with CIGRE and IEEE benchmark grids.

Keywords: Cyber-physical energy system, State estimation, Trust, Event-driven processing, Data stream management system

Introduction

Modern power systems are characterised by a significantly higher integration of Information and communication technology(ICT) compared to traditional power systems. Therefore, they are referred to cyber-physical energy system (CPESs). ICT enables monitoring and control of CPES with a high amount of decentralised power generation (Panteli 2013). However, it increases the system complexity and interdependencies (Panteli 2013). Additionally, it results in increased threats by software malfunctions and cyber-attacks (Pillitteri Victoria and Brewer 2014). Common processes to deal with software malfunctions from other domains, however, are not applicable in CPESs. This is because the common processes typically shut down, reconfigure, and restart the systems, which

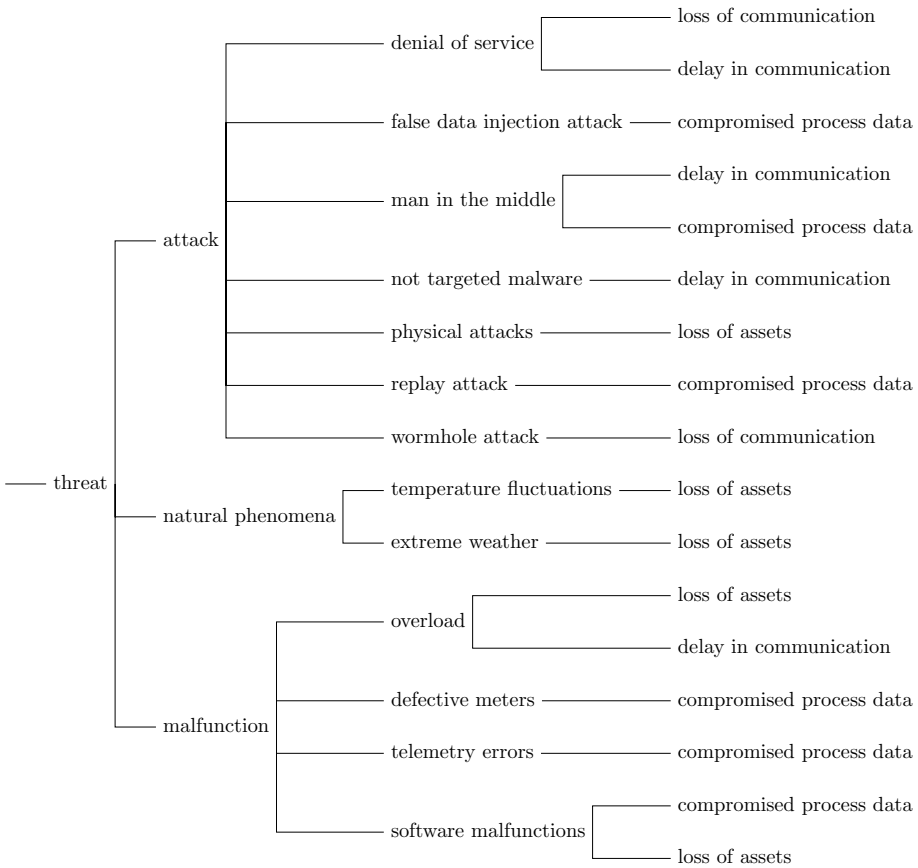


Fig. 1 Exemplary threats for CPESs and especially for state estimation

is not applicable for CPES, which are meant to guarantee power supply at all times (Pillitteri Victoria and Brewer 2014).

A fundamental service for monitoring and controlling CPESs is the state estimation. The task of the state estimation is to estimate the physical values in a CPES required to describe the physical system in total (Abur and Exposito 2004). These values are the complex voltages at all buses and their estimation is based on redundant measurements and the physical system model. Since it is considered that single measurements might be wrong, typically, a bad data detection is implemented to detect, identify, and eliminate such redundant and randomly distributed bad measurements (Abur and Exposito 2004).

Examples for threats for CPESs and, especially, state estimation from literature are shown in Fig. 1[1]. It can be distinguished between threats from attacks, natural phenomena, and malfunctions. The effects, depicted right in Fig. 1, can be categorised into losses of assets or communication, respectively, communication delays, and compromised process data.

In the context of this work, a loss of an asset means a loss of an operational technology (OT) device. This can happen due to a physical attack on that device (Xing 2020), an overload of the device (Xing 2020), or a software malfunction (Kornecki et al.

[1] Fig. 1 does not claim to be complete.

2013). Additional potential causes for an asset loss are natural phenomena like, for example, temperature fluctuations or extreme weather events (Xing 2020; Humayed et al. 2017).

A loss of communication is defined as a situation, in which process data can not communicated from OT to the control room or vise versa. Attacks such as denial of service (Xing 2020; Humayed et al. 2017; Goel and Hong 2015; Wang and Shi 2018; Cai et al. 2019; De Figueiredo et al. 2019; Mahmoud et al. 2019; Alabadi and Albayrak 2020; Ferrag et al. 2020; Gunduz and Das 2020; Karimipour et al. 2020) or wormhole are potential reasons for compromised process data.

Besides losses of communication, the transmission of process data can have a significantly higher delay as normal, which can cause severe problems in time-critical applications. Such a delay of communication can be caused by a denial of service or man in the middle attacks (De Figueiredo et al. 2019; Alabadi and Albayrak 2020; Ferrag et al. 2020; Gunduz and Das 2020). Other potential reasons are not targeted malware (Humayed et al. 2017) and an overload of the OT device (Xing 2020).

The last effect depicted in Fig. 1 are compromised process data, e.g., compromised measurements. Besides software malfunctions, attacks are the main reasons for compromised process data. Such attacks can manipulate topological data (Xing 2020; Cai et al. 2019; Ferrag et al. 2020; Gunduz and Das 2020; Dehghanpour et al. 2019), feed replayed data into the ICT system (Goel and Hong 2015; Wang and Shi 2018; De Figueiredo et al. 2019; Mahmoud et al. 2019; Alabadi and Albayrak 2020; Gunduz and Das 2020; Karimipour et al. 2020), or inject false measurements, known as false data injection attack (FDIA) (Liu et al. 2011).

Coordinated cyberattacks are a special threat to CPESs (Pillitteri Victoria and Brewer 2014). Liu et al. (2011) have shown that attackers performing a coordinated FDIA can influence the estimated system state without being detectable by state-of-the-art bad data detection schemes. Potential goals can be harmful control actions by the system operator or hiding harmful manipulations.

There exist solutions for FIDIAs in the literature [e.g., (Cui et al. 2012; Mo and Sinopoli 2015; Xiong and Ning 2015)]. However, they typically are not applicable to other potential threats. Most of the solutions require a measurement redundancy, which is not given in all power systems, especially in distribution systems. But complexity is also increasing in those systems and, with that, also the need for a state estimation (Huang et al. 2012). In such systems without sufficient measurement redundancy, compromised measurements need to substituted with pseudo measurements (e.g., simulated).

In conclusion, traditional bad data detection is not sufficient to detect coordinated attacks in all possible constellations. Additionally, securing all process data, e.g., with cryptography, would also not be sufficient because it would only increase integrity. However, cyber-security is only one aspect of a reliable and trustworthy situational awareness as shown in Fig. 1. Compared to traditional power systems, the following hypotheses can be stated for CPESs:

- The risk of a decreased integrity of process data is higher.
- The possibility is higher that failures in an up-stream system have influenced the correctness or accuracy of process data.

- The threat is higher that attackers or malfunctions in up-stream systems have decreased the availability of process data.

Facing these challenges, which cannot be categorised into a single threat category like, e.g., cyber-security or functional correctness, a more holistic term (compared to, e.g., integrity) is required to describe the quality of process data. In this work, the term trust is used for this, which is defined as follows for the scope of this work:

Definition 1 (Trust) "Trust is a subjective, context-dependent, and multivariate sense about an entity with respect to its functional correctness, safety, security, reliability, credibility, and usability" (Brand et al. 2020).

Accordingly, a research question arises, how the multivariate trust in physical measurements in a CPES can be modelled, estimated, and integrated into situational awareness. Single artefacts of a solution have been published in the last years:

- a model of multivariate trust and its assessment, called trust in power system network assessment (PSNA-Trust) (Brand et al. 2019, 2020) and
- a model to estimate the multivariate trust in state variables based on the multivariate trust in measurements (Brand et al. 2021).

The solution combining these artefacts has been implemented in a flexible framework, called anomaly sensitive state estimation with streaming systems (ASSESS), with the goal of fulfilling certain requirements to enable a practical use:

- Timeliness: In a complex system with increasing dynamics, situational awareness should be provided as soon as possible.
- Interoperability: ASSESS should be interoperable with existing control room environments and processes.
- Flexibility and scalability: ASSESS should be flexible and scalable to deal with different power grids, environments, and trust goals.

The feasibility of ASSESS has already been demonstrated[2] (Brand et al. 2021). This paper focuses on details of the implementation and an evaluation with respect to the aforementioned requirements.

The concrete contributions of this paper are

- details of an implementation focusing on timeliness, interoperability, flexibility, and scalability, and
- an evaluation considering different power grids and a FDIA each.

The remainder of this paper is structured as follows. Preliminary works regarding a model of multivariate trust and its assessment as well as a model to estimate the multivariate trust in state variables based on the multivariate trust in measurements are

[2] Video of the demonstration: https://youtu.be/3hwi49sfllQ

presented in section Background. In section Implementation, aspects of the implementation of ASSESS are described with the goal to fulfil the requirements. The fulfilment is then evaluated in section Evaluation. Section Conclusion concludes the paper and provides a brief overview of future work.

Background

As background information for this work, this section provides a summary of already published work towards answering the research question, how the multivariate trust in physical measurements in a CPES can be modelled, estimated, and integrated into situational awareness. Subsection Context-Sensitive and Multivariate Trust Model describes a model of multivariate trust and its assessment, called PSNA-Trust, already published in (Brand et al. 2019, 2020). A model to estimate the multivariate trust in state variables based on the multivariate trust in measurements, already published in Brand et al. (2021), is summarised in subsection Trust-Sensitive State Estimation.

Context-sensitive and multivariate trust model

The term trust is interpreted very differently in literature or, in some cases, not defined at all. The related work can be classified in univariate (e.g., (Liu and Li 2018; Ma and Xu 2020; Mustafa et al. 2020; Xie et al. 2019) and multivariate trust models (e.g., (Anders et al. 2011; Rosinger et al. 2013, 2014; Rosinger and Beer 2015)), respectively.

Multivariate trust models rely in most cases on the research about trust in organic computing (OC-Trust) (Steghöfer 2010). In OC-Trust, trust is understood as "a multifaceted concept that incorporates all constituting entities and users of a system and thus enables cooperation in systems of distributed entities. It allows the entities to gauge the confidence they place in their interaction partners in a given context and evolves with the experiences of the entities over time" (Steghöfer 2010). OC-Trust consists of six facets, defined in Definitions 2-7.

Definition 2 (Functional Correctness) "The quality of a system to adhere to its functional specification under the condition that no unexpected disturbances occur in the system's environment" (Steghöfer 2010).

Definition 3 (Safety) "The quality of a system to be free of the possibility to enter a state or to create an output that may impose harm to its users, the system itself or parts of it, or to its environment" (Steghöfer 2010).

Definition 4 (Security) "The absence of possibilities to defect the system in ways that disclose private information, change or delete data without authorization, or to unlawfully assume the authority to act on behalf of others in the system" (Steghöfer 2010).

Definition 5 (Reliability) "The quality of a system to remain available even under disturbances or partial failure for a specified period of time as measured quantitatively by means of guaranteed availability, mean-time between failures, or stochastically defined performance guarantees" (Steghöfer 2010).

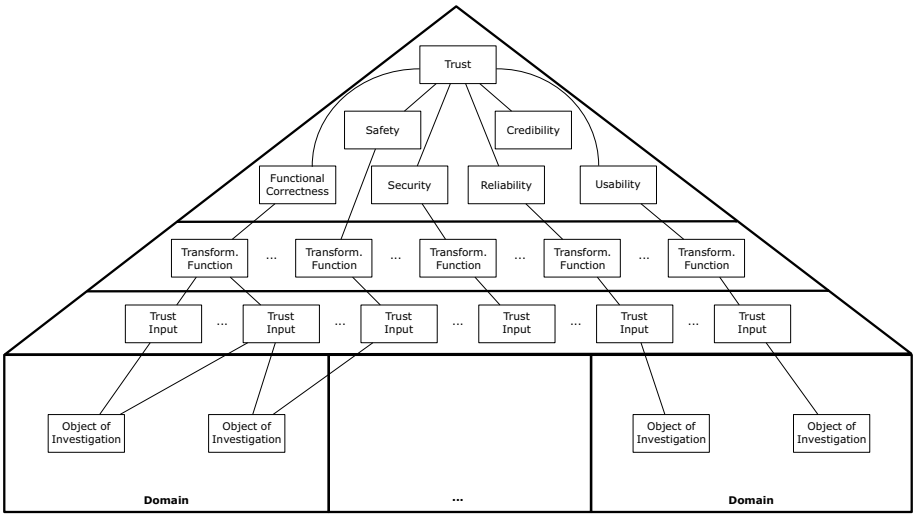


Fig. 2 The trust assessment pyramid (Brand et al. 2020)

Definition 6 (Credibility) "The belief in the ability and willingness of a cooperation partner to participate in an interaction in a desirable manner. Also, the ability of a system to communicate with a user consistently and transparently" (Steghöfer 2010).

Definition 7 (Usability) "The quality of a system to provide an interface to the user that can be used efficiently, effectively and satisfactorily that in particular incorporates consideration of user control, transparency and privacy" (Steghöfer 2010).

However, all found research deal with trust in a multi agent system with other constrains as in a CPES with a central control room. Hence, trust in related work is based on experience of an agent with other agents. This differs for scenarios with a central control room and the task to assess the trustworthiness of components in the field and process data from those components, as focused in this work. In such an environment, most devices are under control of the system operator and, therefore, can be regarded as intended to be trustworthy. Nevertheless, malfunctions, cyberattacks, and other incidents can reduce their trustworthiness. For such events, a trust assessment solely based on experience is not sufficient. Therefore, it is proposed to integrate, among other things, live information from monitoring systems like intrusion detection systems (IDSs) or ICT health monitoring systems.

Figure 2 shows the so-called trust assessment pyramid, with with PSNA-Trust can be described (Brand et al. 2020). On the bottom are objects of investigation, i.e., the entities, which trustworthiness shall be assessed. Examples are remote terminal units (RTUs) or measurements as derived objects of investigation. Derived objects of investigation are entities, which trustworthiness can not directly be assessed by, for example, live monitoring, but can be derived from other objects of investigation (Brand et al. 2020).

$$t_{e,\gamma} = (\gamma, p) \text{with } \gamma \in \Gamma \text{ and } p \in [0,1] \tag{1}$$

$$\boldsymbol{T}_{e,f} = \{t_{e,\gamma} \mid t_{e,\gamma} \xrightarrow{\gamma} f\} \text{with } t_{e,\gamma} \xrightarrow{\gamma} f := \gamma \text{ maps } t_{e,\gamma} \text{ to } f \tag{2}$$

$$\boldsymbol{T}_e = (\boldsymbol{T}_{e,fc}, \boldsymbol{T}_{e,saf}, \boldsymbol{T}_{e,sec}, \boldsymbol{T}_{e,r}, \boldsymbol{T}_{e,c}, \boldsymbol{T}_{e,u}) \tag{3}$$

The trust in objects of investigation is based on trust inputs, which can be very heterogeneous ranging from static information to experience to live information from monitoring systems. A trust estimator γ from a set of all trust estimators Γ uses transformation functions to map the information from trust sources to a trust probability $p \in [0, 1]$ for an entity e (Brand et al. 2021). The combination of a trust estimator γ and its estimated trust probability p is called a simple trust value Eq. (1). Simple trust values are then mapped to one or more trust facets f Eq. (2) and a multifaceted trust value is a tuple consisting of the facets functional correctness *fc*, safety *saf*, security *sec*, reliability *r*, credibility *c*, and usability *u* Eq. (3) (Brand et al. 2021).

Trust-sensitive state estimation

There exist many counter measures against threats, especially against FIDIAs, in literature. However, only a few integrate additional information, like trust, into a state estimation.

One related work ist from Liu et al. Liu et al. (2015). They integrate information from an IDS in a state estimation by mapping all alerts on the respective RTUs and summing them up with respect to their alarm priority. A derived network impact factor matrix is then integrated into the weightest least median square (WLMS) state estimation equation (Liu et al. 2015). However, this approach is limited to not coordinated but single or randomly distributed alerts because the integration into the state estimation influences the convergence of the state estimation. Since one assumption for a WLMS state estimation is that measurement errors are randomly distributed, coherent weighing factors in the network impact factor matrix can cause the state estimation to not converge any more (Brand et al. 2020). Additionally, the multivariated trust values need to be aggregated to a single trust probability and, therefore, the multivariety of the trust cannot be preserved.

Another approach from Basciftci and Ozguner Basciftci and Ozguner (2012) is to use a trust-sensitive particle filter for state estimation, calculating a univariate trust value for each sensor based on the measurements. The authors propose a trust transition matrix consisting of probabilities, with which a sensor is trustworthy or untrustworthy under the condition that a second sensor is trustworthy or untrustworthy. This matrix is then integrated into the particle filter (Basciftci and Ozguner 2012). Therefore, the approach from Basciftci and Ozguner has the same drawbacks as the one from Liu et al.

The approach, published in Brand et al. (2021) as preliminary work, aims at preserving the multiple facets of trust. It utilises the inverse of the derivative of the system model function from the WLMS state estimation. While the derivative can be interpreted as a sensitivity function of the measurements to changes in the state variables, its inverse can be interpreted as a sensitivity function of the state variables to changes in the measurements, accordingly (Brand et al. 2021).

$$w_{i,j,S}(\boldsymbol{x}) = \frac{|s_{i,j}(\boldsymbol{x})|}{\|s_{i,j}(\boldsymbol{x})\|} = \frac{|s_{i,j}(\boldsymbol{x})|}{\sqrt{\sum_{l=1}^{m} s_{i,l}^2}} \tag{4}$$

$$w_{i,j,e}(\boldsymbol{x}) = \frac{1 + \|\boldsymbol{e}\|_\infty - |e_j|}{\|1 + \|\boldsymbol{e}\|_\infty - |e_j|\|} = \frac{1 + \|\boldsymbol{e}\|_\infty - |e_j|}{\sqrt{\sum_{l=1}^{m}(1 + \|\boldsymbol{e}\|_\infty - |e_l|)^2}} \tag{5}$$

$$p_{x_i,\gamma} = \frac{\sum_{j=1}^{m} w_{i,j,S} \cdot w_{i,j,e} \cdot p_{z_j,\gamma}}{\sum_{j=1}^{m} w_{i,j,S} \cdot w_{i,j,e}} \tag{6}$$

The sensitivities $\boldsymbol{S}(\boldsymbol{x}) = (\frac{\partial \boldsymbol{h}(\boldsymbol{x})}{\partial \boldsymbol{x}})^\dagger$ of the state variables $\boldsymbol{x}$ regarding changes of the measurements $\boldsymbol{z}$ are utilised for weighing factors $w_{i,j,S}(\boldsymbol{x})$ for each combination of x_i and z_j Eq. (4). An additional weighing factor $w_{i,j,e}(\boldsymbol{x})$ considers the respective measurement residual e_j relative to the maximum measurement residual $\|\boldsymbol{e}\|_\infty$ Eq. (5). The final trust probability $p_{x_i,\gamma}$ of a simple trust value $t_{x_i,\gamma}$ for x_i is then calculated using both weighing factors for the combination of each measurement and x_i and the given trust probability $p_{z_j,\gamma}$ Eq. (6) (Brand et al. 2021).

Implementation

The implementation of ASSESS has the goal of fulfilling the requirements of timeliness, interoperability, flexibility, and scalability. It is implemented in a framework for customised data stream management system (DSMSs), Odysseus. DSMSs and Odysseus are introduced in subsection Data Stream Management System: Odysseus. Subsection Architecture describes the high-level architecture of ASSESS. Highlights of the implementation to reach the required timeliness, flexibility, and scalability are presented in the subsections Timeliness and Flexibility and Scalability.

Data stream management system: Odysseus

Data stream management systems (DSMSs) are an enhancement of so-called streaming systems. A streaming system is a system that processes data event-driven and in main memory. It retains data only as long as absolutely necessary and processes data only once (Stonebraker et al. 2005).

The measurements from the field are transmitted cyclically or spontaneously by active data sources. Thus, the use of a streaming system with its event-based processing as the technological basis for ASSESS facilitates the interoperability. In addition, both process data and events from trust estimators should be processed as quickly as possible, i.e., event-driven, to ensure timeliness.

However, to enable more flexibility, DSMSs are suitable. A DSMS is a streaming system extended with features of database management systems such as query management, predefined operators, query optimisation and access control (Cugola and Margara 2012; Geisler 2013).

Data sources of DSMSs are thereby assumed to be not under the control of DSMS. The data that an active data source sends is called a data stream. Here, a data stream is a continuous, ordered, and potentially infinite sequence of volatile data stream elements (Golab and Özsu 2003). The ordering is either explicit through timestamps in the

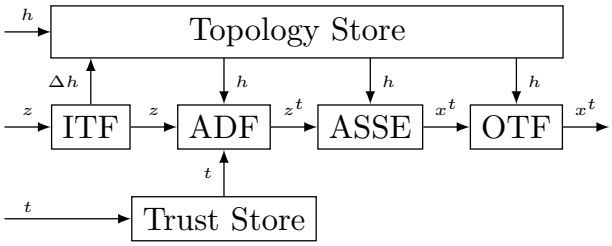


Fig. 3 Components and data flow of ASSESS

incoming data stream elements or implicit by timestamps added to the incoming data stream elements by the DSMS. Outputs from DSMSs are also data streams (Krämer 2007).

The paradigm of data stream processing can be compared to that of databases. In databases, data can be considered static compared to ad hoc queries. In DSMSs, on the contrary, data is volatile and queries are long-running. An example of this is the continuous computation of the average temperature on a data stream from a temperature sensor (Golab and Özsu 2003). Unlike short-lived queries to a database management system, queries to a DSMS are long-living. They are installed once and process volatile data stream elements continuously.

Since not all elements can be stored persistently, their retention time in an DSMS is limited. This can be done by, among other things, window operations (Arasu et al. 2002).

Odysseus (Odysseus 2023) is a a framework for customised DSMSs that allows the creation of different DSMSs tailored to given use cases (Appelrath et al. 2012). Compared to other DSMSs, e.g., Aurora (Hwang et al. 2005), Borealis (Ahmad et al. 2005), OSIRIS-SE (Brettlecker et al. 2005), or Stormy (Merkli 2010), Odysseus is more flexible and easier to extend. Therefore, Odysseus has been chosen to implement ASSESS.

Odysseus is based on the OSGi service platform, a dynamic plug-in based system for Java. Besides plug-ins, another important concept in the OSGi service platform are services. An OSGi service is a Java object that is created in a plug-in but is available system-wide.

The basis for the flexibility of Odysseus are so-called points of variation. These points of variation are OSGi services and, by integration of plug-ins, different implementations of a service can be provided. The amount of so-called fix-points, i.e., structures with a unique implementation, are kept at a minimum (Appelrath et al. 2012).

To easily connect different and also new types of data sources to Odysseus without the need to change existing components, Odysseus uses a so-called access framework. This framework decouples the handling of transport, protocol, and data format into different services. With that, it is possible to simply add new service implementations, e.g., TCP/IP for data transport.

Odysseus provides its own rule-based scripting language called Odysseus Script to let the user decide at run-time which implementation to use for some points of variation (Odysseus 2023). It allows the user to influence various points of variation in addition to actually implementing a query. However, this is only possible if corresponding plug-ins with different implementations of the service are included.

Architecture

The high-level architecture of ASSESS in Odysseus is depicted in Figure Components and data flow of ASSESS (see Fig. 3).

The initial topology h of the CPES is fed into a topology store. Measurements z from the field pass an input transformation framework (ITF), which serves for transforming various OT protocols into a common data scheme. It is based on the access framework of Odysseus and is, therefore, flexible to handle different OT protocols and amounts of data sources.

Topological changes Δh are sent to the topology store to update the topology and measurements are forwarded to an anomaly detection framework (ADF). The ADF is a flexible and extensible framework consisting of anomaly detectors, which use transformation functions to create simple trust values based on trust inputs t from various trust sources like, for example an IDS (cf. subsection Context-Sensitive and Multivariate Trust Model in section Background). The anomaly detectors can retrieve h from the topology store and t from a trust store. They enhance z with simple trust values and the ADF combines these simple trust values for each z to a multifaceted trust value.

The trust-enhanced measurements z^t are forwarded to an anomaly sensitive state estimation (ASSE), which performs a trust-sensitive state estimation as described in subsection Trust-Sensitive State Estimation in section Background. The output are trust-enhanced state variables x^t.

Analogous to the ITF, an an output transformation framework (OTF) is capable of transforming x^t into various protocols and publishing it, e.g., as messages according to the standard IEC 60870-5-104.

Timeliness

The timeliness requirement refers both to an immediate consideration of potentially compromising events and, related, to an event-driven state estimation instead of a cyclically performed one. The use of a DSMS tackles these requirements in general. However, there are also challenges in DSMSs, three of which are particularly relevant to this work, namely blocking operations, efficient creation of measurement sets for the state estimation, and maintaining time semantics while considering contextual information like trust inputs.

Blocking operations

The idea of a data stream processing is to process elements "on-the-fly" without blocking. However, some data stream operations are blocking, mostly to either establish or preserve temporal order in a data stream. Processing based on this principle is called in-order processing, and correspondingly, processing of data streams that are not necessarily temporally ordered is called out-of-order processing. Furthermore, some window operations are blocking. In ASSESS, the problem of blocking can occur as follows.

ASSESS receives measurements directly from the telecontrol system, e.g. from RTUs. Accordingly, there is usually more than one data source, e.g., one per RTU, and the different data streams should be merged as early as possible to limit complexity. For in-order processing, a union operator is suitable for merging but is blocking. The blocking

duration depends on the lowest data rate of the input data streams, becomes problematic in case of unexpected missing measurements, and may even be infinite if no more measurements are received from a data source.

To solve this problem, it is analysed in the following where in-order processing is required. The ADF handles each measured value individually. For the state estimation in the ASSE, a set of measurements must be defined. However, this set of measurements needs not be ordered in time in itself. In conclusion, in-order processing of the measurements can be omitted. This makes it possible to use a so-called merge operator instead of an union, which does not guarantee the temporal order but transfers elements from different input data streams directly into the output data stream. Thus, blocking due to in-order processing can be avoided.

Efficient creation of measurement sets

A measurement set as a set of data stream elements that should be processed together can be defined by window operations in DSMSs (Golab and Özsu 2003; Arasu et al. 2002). Time windows are suitable in principle and, concretely, tumbling time windows processing each data stream element in exactly one window. However, a problem arises when there are large time spans with no elements, since the time progress is measured using the element timestamps. In addition, an adequate window size can only be determined with difficulty if the data stream does not flow smoothly, e.g., the data sources have different data rates or measurements are transmitted spontaneously. The same issue holds for element windows.

$$\Delta t_{win} \geq \Delta t_{max} \vee (\Delta t_{win} \geq \Delta t_{se} \wedge |\boldsymbol{mp}| >= p \cdot m) \tag{7}$$

Therefore, a special window operation is proposed to efficiently create measurement sets for the state estimation. Let Δt_{se} be the average time taken by the state estimation, where Δt_{se} depends essentially on the system model h and the number of measurements. Thus, there is no benefit in a smaller time span between the closing of two successive windows, denoted as Δt_{win}. However, if $\Delta t_{win} = \Delta t_{se}$ is chosen, it is possible that, depending on the data sources, only measurements of a few metering points are in the window. Therefore, it is recommended to choose an additional condition, namely, the amount of distinct metering points p (in percentage), from which measurements should be present in the window. If this combined condition is not fulfilled, a hard condition closes the window. Here it is useful to define a maximum system time Δt_{max} for which the window should be open. This can be based on, e.g., the data rates of the data sources. The full closing condition for the window approach is presented in Eq. (7), with $\boldsymbol{mp}$ as the set of unique metering points in the window and m the total amount of unique metering points.

Context information and time semantics

When enriching measurements with context information (e.g., trust inputs or system models), time semantics must be taken into account, i.e., measurements should only be enriched with context information if both are valid at the same time. A complicating factor is that it cannot be defined for neither measurements nor context information how long they are valid. Theoretically, the validity ends with a new measurement from the same metering point or a new context information of the same type (e.g. a topology

update). For such scenarios, Odysseus provides so-called context stores, which are limited buffer for data stream elements in main memory (Odysseus 2023). A qualifying feature of context stores is that, when a new element is saved, the last saved element is updated in such a way that the end of its validity is set to the timestamp of the new element. This results in an gapless, half-open validity interval in the context store with exactly one piece of context information valid at each point in time (from the timestamp of the first element on).

Flexibility and scalability

Since ASSESS is primarily concerned with the very complex and highly dynamic research fields of CPESs, threats against them, and possible countermeasures, a certain flexibility is required to develop ASSESS in a future-proof manner. Specifically, flexibility in ASSESS refers to the support of various OT protocols, both diverse trust estimators and inputs (cf. section Architecture), different state estimators and other algorithms.

In addition to flexibility, however, scalability is also required, since ASSESS must be able to handle different power system sizes and numbers of trust estimators. Accordingly, the challenge is to be able to adapt, replace and/or scale corresponding system components as easily as possible.

In this context, Odysseus allows to combine queries located in different script files (Odysseus 2023). In particular, the so-called sub-query operator is suitable for this purpose. Sub-query operators hide nested query plans. The hidden sub-queries are normal queries, i.e., installed and started together with the main query. The advantages of sub-queries are on the one hand an improved overview due to multiple abstraction levels and on the other hand a better interchangeability. The latter is achieved by the fact that different queries for the same (sub-) problem can be defined and exchanged simply by calling a different sub-query. Sub-query operators thus represent a suitable tool to achieve the required flexibility.

For scalability, Odysseus provides loop constructs (Odysseus 2023) that enable scaling an operation or sub-query. The required number of, e.g., data sources for measurements or trust estimators can thereby be outsourced using variables in configuration files.

ASSESS uses sub-queries or loop constructs at all points relevant to flexibility or scalability, respectively. Sub-queries are used, e.g., in the ITF for translating the measurements from the used OT protocol into a common data scheme or in the ASSE for the state estimation component to enable interchangeability. Loop constructs are used, e.g., in the ITF for scaling the data sources for measurements.

Evaluation

The evaluation of ASSESS has the goal of, on the one hand, deriving assertions about the correctness of the state estimation results and about the benefit of the multifaceted trust values of the state variables. On the other hand, the evaluation shall demonstrate timeliness, interoperability, flexibility, and scalability of ASSESS.

Table 1 lists all requirements to be evaluated and whether the evaluation is qualitative or quantitative. “Correctness” in this context means that the state variables estimated by ASSESS match those estimated by the same state estimator as used in ASSESS in a stand-alone program. For an expressiveness of the multivariate trust values of the state

Table 1 An overview about the evaluated requirements

Acronym	Requirement	Type
Correctness	The estimated state variables match those estimated by the state estimator without ASSESS	Qualitative
Expressiveness	The multivariate trust correlates with the deviation of the state variables from their normal values without compromise	Qualitative
Timeliness	The latency of ASSESS is of the same order of magnitude as the latency of the integrated state estimator	Quantitative
Interoperability	ASSESS supports the standard IEC 60870-5-104 and is extensible to support other protocols	Qualitative
Flexibility	ASSESS is adaptable for different power systems and trust estimators	Qualitative
	ASSESS can be customised for different OT protocols used	Argumentative
Scalability	ASSESS scales for different numbers of telecontrol connections and trust estimators	Qualitative

variables, two criteria apply. First, deviations of the state variables from the actual state of the power system should be reflected. Second, scenarios should be considered in which a state-of-the-art bad data detection does not detect bad data to show the added value. The evaluation of whether the deviations of the state variables from the actual state of the power system are reflected by the multivariate trust values is done by correlation analysis.

Regarding the timeliness, it should be mentioned again that typically a state estimation is performed as a cyclic process, e.g., every five minutes. An event-driven process, as pursued in this work, is difficult to compare with such a cyclic process in terms of timeliness. Therefore, the goal is that the time required by ASSESS should be of the same order of magnitude as that of a comparable state estimation without trust estimation. Latency in this context is defined as the time span between the arrival of a data stream element and the provision of a result. The latency of ASSESS results from the arrival of the last measurement in the ITF used in a measurement set and the provision of the results in the OTF, while the latency of the integrated state estimator is defined by two metering points, one directly before and one directly after it.

Flexibility and scalability can be shown by using different power systems with different sizes as well as different trust estimators and numbers of them. Flexibility regarding OT protocols is not explicitly evaluated, since in all scenarios the standard IEC 60870-5-104 is used. However, for this work, the access framework of Odysseus was extended to handle messages in that standard, which shows that Odysseus and thus also ASSESS are extensible by protocol implementations.

The remainder of this section is structured as follows. The evaluated scenarios and the overall evaluation setup are described in sections Scenarios and Setup, respectively. Section Results then provides an overview of the results.

Scenarios

This section describes the scenarios implemented for the evaluation and their selection. The motivation for considering different scenarios is to show that ASSESS satisfies the requirements of flexibility and scalability. A morphological box is used as the methodology for identifying potential scenarios and the variation points defining each scenario are explained in the following.

Table 2 An excerpt from the overview of all possible scenarios

Property	Scenario 1	Scenario 2	Scenario 3
Power grid	CIGRE12MV	IEEE39HV	IEEE118HV
Trust sources	• IDS • IT monitoring • history	• IT monitoring	• IDS

To evaluate ASSESS in terms of scalability, power systems of different sizes (and thus different numbers of data sources) are considered for the ITF: a reduced CIGRE medium voltage distribution network with 12 instead of 15 buses (CIGRE12MV),[3] the IEEE 39-bus system (IEEE39HV),[4] and the IEEE 118-bus system (IEEE118HV).[5] In addition, scalability is evaluated with respect to the number of trust sources with three different trust sources available: an IDS, an IT monitoring tool, and a source of historical trust values. These two variation points (power grids and trust sources) are also used to evaluate the flexibility of ASSESS.

In total, 24 scenarios are possible with these variation points. For the evaluation of ASSESS, three scenarios were selected, characterised by different power grids (and their sizes) and numbers of trust estimators (cf. Table 2).

Setup

In the setup described below, each of the scenarios described in subsection Scenarios was run ten times, each with a duration of five minutes. The number and duration are a result of requirements for the latency measurements. While the latency does not have a large variance in a relatively static setup as used in the evaluation, minor fluctuations do occur due to the process management of the operating system. For this reason, ten runs per scenario was considered sufficient. Since the main point within a scenario is to feed ASSESS both without and with compromised measurements, but the system behaviour does not change with more or less state estimation runs with the same measurements, an evaluation duration of five minutes is sufficient (the state estimation for the IEEE118HV takes roughly 20 seconds).

The power system measurements and trust inputs are provided by a co-simulation, which will be described in the following paragraph. ASSESS and the co-simulation were each installed in containers on different virtual machines. Containerisation enables platform independence and the use of different virtual machines enables an exclusive use of the resources of the corresponding machines. Most of the used transformation functions for the trust inputs are the same as in Brand et al. (2020, 2021).

The co-simulation provides, on the one hand, power system measurements for the state estimation and, on the other hand, trust inputs for the trust estimators. It should be noted that in the context of this evaluation, only the outputs of trust estimators are simulated. For example, in a simulator, alarms of an IDS are simulated instead of simulating

[3] https://pandapower.readthedocs.io/en/v2.1.0/networks/cigre.html

[4] https://icseg.iti.illinois.edu/ieee-39-bus-system/

[5] https://icseg.iti.illinois.edu/ieee-118-bus-system/

the IDS itself or even using a real IDS. The reasons for this are the following. First, the setup serves to reduce complexity in the co-simulation and to ensure reproducibility. Second, the configuration of trust sources and trust estimators is not the focus of this work. Third, feasibility was shown in a previous demonstration,[6] in which real trust sources monitored the co-simulation (Brand et al. 2021).

All simulations are oriented to a common clock, which specifies a second-by-second cycle. However, it is up to the simulators at what intervals they generate values. The power system measurements are simulated every five seconds and the trust inputs every second. Furthermore, the co-simulation of a scenario is always divided into two phases: a so-called normal phase, in which neither compromises of the power system measurements nor anomalies in the trust inputs are present, and a so-called abnormal phase, in which, accordingly, the effects of a FDIA are reflected in the power system measurements and anomalies in the trust inputs are present. The power system is simulated steady state, which means that the simulated set of measurements is the same at each instant within a phase. The same applies to the trust inputs, of which concretely the following four can be simulated depending on the scenario: alarms of an IDS, the current CPU and RAM utilisation of the simulated RTUs, and the number of running system processes on the simulated RTUs. A normal phase simulates no IDS alarms, normal CPU and RAM utilisation, and a normal number of system processes. On the other hand, for simulated RTUs whose power system measurements are manipulated by a FDIA, IDS alarms, increased CPU and RAM utilisation, and a number of system processes increased by one are simulated in the abnormal phase. It should be noted again that the goal is to evaluate how ASSESS behaves with such inputs.

The described co-simulation was implemented in Odysseus. The power system measurements are sent out by Odysseus per RTU as messages according to the IEC 60,870-5-104 standard, assuming one RTU per bus. For example, the CIGRE12MV results in a number of twelve data sources of power system measurements for ASSESS. The trust inputs are sent out in CSV format over TCP, with one communication link per trust source, i.e., one for the IDS and one for the IT monitoring tool.

Results

By using ASSESS in the different scenarios described in subsection Scenarios, it was possible to demonstrate the fulfilment of interoperability, flexibility, and scalability. The "correctness", i.e., the correspondence of the state variables estimated by ASSESS with those estimated by the state estimator as a stand-alone program, was verified for all scenarios during the evaluation and is given. In the following, the results on the expressiveness and timeliness are presented.

Expressiveness

The question of whether the trust-sensitive state estimation has a certain expressiveness or benefit includes two requirements. First, deviations of the state variables from the actual state of the power system should be reflected in the trust values. Second, these

[6] Video of the demonstration: https://youtu.be/3hwi49sfllQ

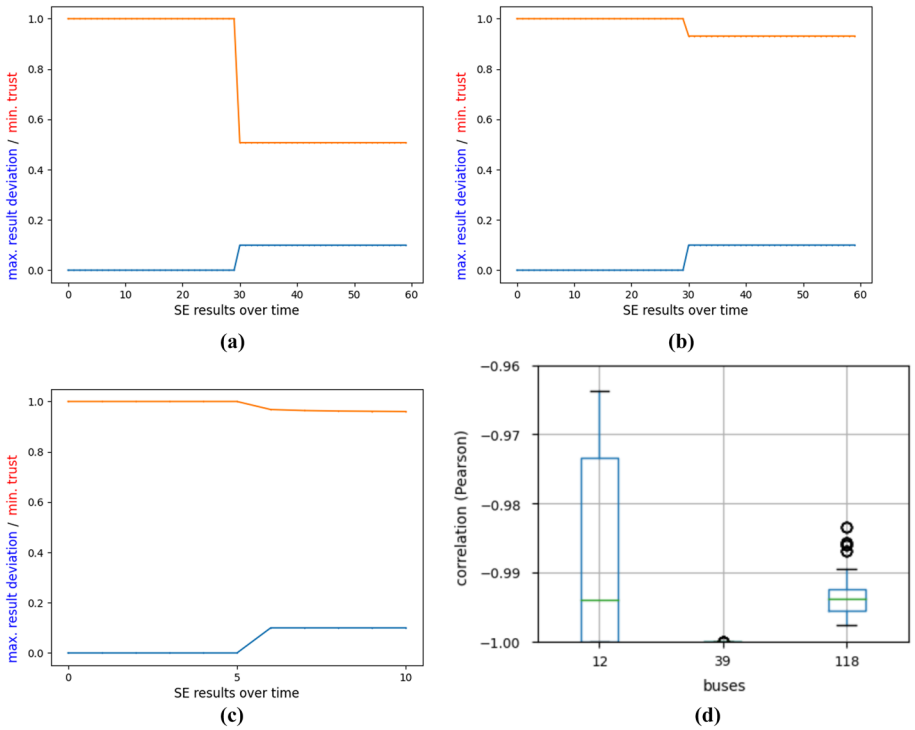


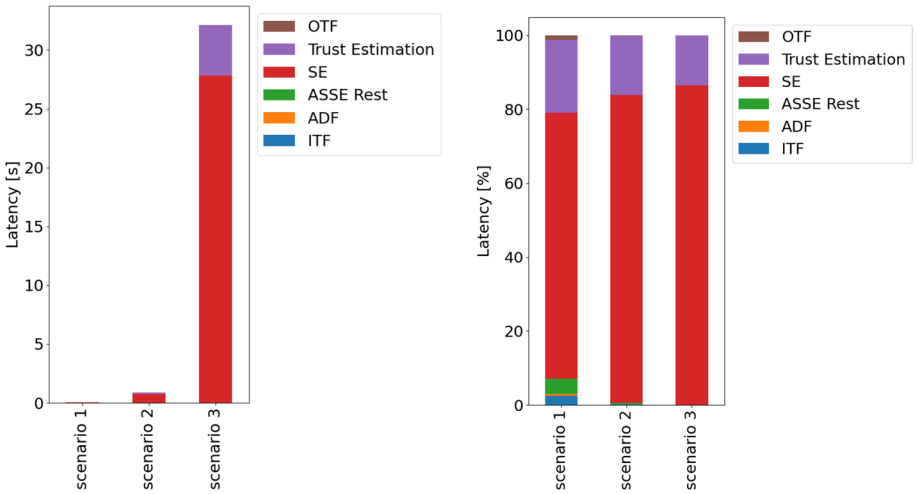
Fig. 4 Evaluation of the expressiveness of a trust-sensitive state estimation. **a** Scenario 1 (CIGRE12MV): The maximum distance of a state variable from its expected normal value, aggregated over all state variables, in blue. The minimum trust in a state variable, aggregated over all trust estimators and state variables, plotted in red. **b** Scenario 2 (IEEE39HV): The maximum distance of a state variable from its expected normal value, aggregated over all state variables, in blue. The minimum trust in a state variable, aggregated over all trust estimators and state variables, plotted in red. **c** Scenario 3 (IEEE118HV): The maximum distance of a state variable from its expected normal value, aggregated over all state variables, in blue. The minimum trust in a state variable, aggregated over all trust estimators and state variables, in red. **d** Pearson's correlation coefficients as box-plots per scenario (12 busbars: CIGRE12MV, 39: IEEE39HV, 118: IEEE118HV). The correlation coefficients of all combinations of state variable and trust estimator are included in the box-plots

should be compromises in which a state-of-the-art bad data detection does not detect bad data. The latter is given by the design of the FIDIAs for the different scenarios.

The description of the algorithm is out of scope of this paper, however, it is assured that without the compromised measurements observability is not given any more.

The evaluation of whether the deviations of the state variables from the actual state of the power system are reflected by the multivariate trust values is performed by Pearson's correlation analysis. The correlation of the following two functions is analysed. The first function represents the deviation of a state variable from its expected value over time, where the expected value is the one obtained from a state estimation with normal, not compromised measurements. The second function is the trust in the state variable estimated by a trust estimator over time.

Qualitatively, this is shown in Fig. 4a to c. The x-axis is defined by the state estimation result sets over time. In blue, the maximum distance of a state variable from its expected value, aggregated over all state variables is shown. The red curve shows the minimum trust in a state variables, aggregated over all trust estimators and state variables. These figures already show that the two functions are correlated, which is equivalent to the fact that the trust in the state variables allows a qualitative statement about whether they



(a) Absolute latency in seconds. (b) Relative latency in percentages.

Fig. 5 The latency (absolute and relative) in histograms, broken down by the most essential components of ASSESS

are compromised. This is supported by the calculated Pearson correlation coefficients, which are shown as box-plots in Fig. 4d. The correlation coefficients of all combinations of state variable and trust estimator are included in the box-plots. Pearson's correlation coefficients are defined for the interval $[-1, 1]$, where 0 corresponds to uncorrelatedness and ± 1 corresponds to strong positive and negative correlation, respectively. Figure 4d shows a strong negative correlation between the distance of a state variable from its expected value and the trust in it for the experiments performed. This means that compromisedness of a state variable is associated with decreased trust in it. Thus, it could be shown that the trust-sensitive state estimation is beneficial with respect to the compromisedness of state variables.

Timeliness

The timeliness requirement is that the latency of ASSESS shall be of the same order of magnitude as that of the integrated state estimator. The latency is thereby measured in ASSESS as follows. When a new data stream element arrives or is created, the current system time is appended to it as the starting point for the latency. In addition, special Odysseus operators are integrated into the queries, which, when a data stream element passes them, append the current system time to it. In addition, the operators can define different metering points, so that the set system times are each assigned to a metering point. An example of such a measuring point in ASSESS is "ITF", under which the system time is stored at which a data stream element has left the ITF. From the difference between system times of different metering points (e.g., ADF and ITF) the latency for the intermediate processing is calculated accordingly.

Figure 5 shows the latency of ASSESS as stacked histograms, broken down by the components of ASSESS. Figure 5a shows the absolute latency in seconds and Fig. 5b the relative latency in percentages. Figure 5a shows a clear increase in latency across the scenarios, which is due to the size of the power grid considered in each case. An increase

Table 3 The latency (absolute and relative), broken down by the most essential components of ASSESS

	Scenario 1		Scenario 2		Scenario 3	
	[s]	[%]	[s]	[%]	[s]	[%]
ITF	0.0	2.384	0.001	0.105	0.001	0.003
ADF	0.0	0.568	0.0	0.018	0.0	0.0
ASSE Rest	0.005	4.116	0.004	0.403	0.008	0.024
State Estimation	0.037	71.99	0.741	83.387	27.808	86.431
Trust Estimation	0.011	19.671	0.142	15.95	4.321	13.528
OTF	0.001	1.256	0.001	0.137	0.004	0.014
total	0.054	100.0	0.888	100.0	32.142	100.0

in the size of the power grid is accompanied by a significantly higher latency of the state estimator (red bars), a higher latency of the trust estimation for the state variables (purple bars), and no visible latency change for the other components. It can be seen in Fig. 5b that the latency of the state estimator accounts for well over 50% of the total latency in all scenarios. The exact absolute and relative latency can be found in Table 3.

Conclusion

Facing various challenges regarding the integrity, correctness, and availability of process data in CPES, this paper proposes trust as a holistic term and its assessment as a holistic model to describe the quality of process data. The paper deals, therefore, with the research question, how multivariate trust in physical measurements in a CPES can be modelled, estimated, and integrated into situational awareness.

Anomaly sensitive state estimation with streaming systems (ASSESS) as a proposed framework implements a context-sensitive and multivariate trust model and a trust sensitive state estimation. While these two artefacts are already published, the focus of this paper is on the implementation of ASSESS and the fulfilment of the requirements for timeliness, interoperability, flexibility, and scalability.

The technological basis for ASSESS is Odysseus, a framework for DSMSs. The use of Odysseus enables an event-driven processing and the required flexibility and scalability. Power system measurements, transmitted in OT protocols are interpreted, enriched with multivariate trust values, and build the input for a ASSE. The ASSE performs a state estimation and estimates the multivariate trust in each state variable based on the multivariate trust in the input measurements.

The evaluation shows, first, that the multivariate trust in the state variables correlate with the deviation of the state variables from their normal value without compromise. Second, the latency of ASSESS, as a measure for timeliness, is of the same order of magnitude as the latency of the state estimator. Third, interoperability, flexibility, and scalability are demonstrated by evaluating different scenarios with different power grid sizes.

However, the expressiveness of multivariate trust values depends to a certain extent on the quality of the trust estimators used. A limitation of this work is the use of very simple trust estimators. The research and development of more elaborated trust estimators or transformation functions is accordingly an aspect for future work. Furthermore, false alarms were not considered or even simulated in the evaluation carried out. However,

the handling of false alarms in the trust inputs can certainly be a quality criterion for trust estimators. Also, the trust estimators implemented in this work only contribute to functional correctness, security and credibility.

Author contributions
MB was in charge of developing ASSESS and writing the paper. SL and DE contributed with expert knowledge to the development of ASSESS and reviews of 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. https://energyinformatics.springeropen.com/articles/supplements/volume-6-supplement-1

Availability of data and materials
There are no sources of data and materials in this article.

Declarations

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

Published: 19 October 2023

References

Abur A, Exposito AG (2004) Power system state estimation: theory and implementation. CRC Press, Boca Raton
Ahmad Y, Berg B, Cetintemel U, Humphrey M, Hwang J-H, Jhingran A, Maskey A, Papaemmanouil O, Rasin A, Tatbul N, et al (2005) Distributed operation in the borealis stream processing engine. In: Proceedings of the 2005 ACM SIGMOD International conference on management of data, p 882–884
Alabadi M, Albayrak Z (2020) Q-learning for securing cyber-physical systems: a survey. In: 2020 International congress on human-computer interaction, optimization and robotic applications (HORA). IEEE, Ankara
Anders G, Steghöfer J-P, Siefert F, Reif W (2011) Patterns to measure and utilize trust in multi-agent systems. In: 2011 Fifth IEEE conference on self-adaptive and self-organizing systems workshops. IEEE, Ann Arbor, p 35–40
Appelrath H-J, Geesen D, Grawunder M, Michelsen T, Nicklas D (2012) Odysseus: a highly customizable framework for creating efficient event stream management systems. In: Proceedings of the 6th ACM international conference on distributed event-based systems. ACM, p 367–368
Arasu A, Babu S, Widom J (2002) An abstract semantics and concrete language for continuous queries over streams and relations. Technical report, Stanford
Basciftci YO, Ozguner F (2012) Trust aware particle filters for autonomous vehicles. In: 2012 IEEE International conference on vehicular electronics and safety, ICVES 2012, p 50–54
Brand M, Babazadeh D, Lehnhoff S, Engel D (2019) Trust in control: a trust model for power system network assessment. EPJ Web Conf 217:01008
Brand M, Babazadeh D, Krüger C, Siemers B, Lehnhoff S (2020) Trust assessment of power system states. Energy Inform 3(1):18
Brand M, Babazadeh D, Lehnhoff S (2021) Trust in power system state variables based on trust in measurements. In: Proceedings of the 2021 IEEE Madrid PowerTech. IEEE, Madrid, p 1–6
Brand M, Castro F, Hage Hassen B, Krüger C, Logemann T, Siemers B, Weller D, Wolff T, Lehnhoff S (2021) Demo abstract: a platform to assess the trust in power system components, data, and services. In: Abstracts of the 10th DACH+ conference on energy informatics. Springer, p 26
Brettlecker G, Schuldt H, Schek H-J (2005) Towards reliable data stream processing with OSIRIS-SE. In: BTW, p 405–414
Cai X, Wang Q, Tang Y, Zhu L (2019) Review of cyber-attacks and defense research on cyber physical power system. In: 2019 IEEE sustainable power and energy conference (iSPEC). IEEE, Beijing, p 487–492
Cugola G, Margara A (2012) Processing flows of information. ACM Comput Surv 44:3
Cui S, Han Z, Kar S, Kim TT, Poor HV, Tajer A (2012) Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions. IEEE Signal Proc Mag 29(5):106–115
De Figueiredo HFM, Ferst MK, Denardin GW (2019) An overview about detection of cyber-attacks on power SCADA systems. In: 2019 IEEE 15th Brazilian power electronics conference and 5th IEEE Southern power electronics conference (COBEP/SPEC). IEEE, Santos
Dehghanpour K, Wang Z, Wang J, Yuan Y, Bu F (2019) A survey on state estimation techniques and challenges in smart distribution systems. IEEE Trans Smart Grid 10(2):2312–2322
Ferrag MA, Babaghayou M, Yazici MA (2020) Cyber security for fog-based smart grid SCADA systems: solutions and challenges. J Inform Sec Appl 52:102500

Geisler S (2013) Data stream management systems. In: Kolaitis PG, Lenzerini M, Schweikardt N (eds) Proceedings of the 2010 data exchange, integration and streams. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Leipzig, pp 275–304
Goel S, Hong Y (2015) Security challenges in smart grid implementation. In: Goel S (ed) Smart Grid Security. Springer, London, pp 1–39
Golab L, Özsu MT (2003) Issues in data stream management. ACM Sigmod Rec 32(2):5–14
Gunduz MZ, Das R (2020) Cyber-security on smart grid: threats and potential solutions. Comput Netw 169:107094
Huang Y-F, Werner S, Huang J, Kashyap N, Gupta V (2012) State estimation in electric power grids: meeting new challenges presented by the requirements of the future grid. IEEE Signal Process Mag 29(5):33–43
Humayed A, Lin J, Li F, Luo B (2017) Cyber-physical systems security—a survey. IEEE Internet Things J 4(6):1802–1831
Hwang J-H, Balazinska M, Rasin A, Cetintemel U, Stonebraker M, Zdonik S (2005) High-availability algorithms for distributed stream processing. In: 21st International conference on data engineering. IEEE, p 779–790
Karimipour H, Srikantha P, Farag H, Wei-Kocsis J (2020) Security of cyber-physical systems. Springer, Cham
Kornecki AJ, Subramanian N, Zalewski J (2013) Studying interrelationships of safety and security for software assurance in cyber-physical systems: approach based on bayesian belief networks. In: Kornecki AJ (ed) 2013 federated conference on computer science and information systems. IEEE, Krakow, pp 1393–1399
Krämer J (2007) Continuous Queries over Data Streams—semantics and implementation. PhD thesis, University of Marburg
Liu Y, Li C (2018) Secure distributed estimation over wireless sensor networks under attacks. IEEE Trans Aerosp Electron Syst 54(4):1815–1831
Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inform Syst Sec 14(1):1–33
Liu T, Sun Y, Liu Y, Gui Y, Zhao Y, Wang D, Shen C (2015) Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection. Future Gener Comput Syst 49:94–103
Ma L, Xu G (2020) Distributed resilient voltage and reactive power control for islanded microgrids under false data injection attacks. Energies 13(15):3828
Mahmoud MS, Hamdan MM, Baroudi UA (2019) Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges. Neurocomputing 338:101–115
Merkli S (2010) Streaming in the cloud. PhD thesis, Master Thesis, Eidgenössische Technische Hochschule, 2009–2010
Mo Y, Sinopoli B (2015) Secure estimation in the presence of integrity attacks. IEEE Transact Autom Control 60(4):1145–1151
Mustafa A, Poudel B, Bidram A, Modares H (2020) Detection and mitigation of data manipulation attacks in AC microgrids. IEEE Trans Smart Grid 11(3):2588–2603
Odysseus. https://odysseus.informatik.uni-oldenburg.de/. Accessed 28 Feb 2023
Panteli M (2013) Impact of ICT reliability and situation awareness on power system blackouts. Doctor thesis, The University of Manchester
Pillitteri Victoria Y, Brewer TL (2014) Guidelines for smart grid cybersecurity. Technical report, NISTIR. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf. Accessed 28 Aug 2023
Rosinger C, Beer S (2015) Glaubwürdigkeit in dynamischen Wirkleistungsverbünden. Informatik-Spektrum 38(2):103–110
Rosinger C, Uslar M, Sauer J (2013) Threat scenarios to evaluate trustworthiness of multi-agents in the energy data management. In: 7th International conference on environmental informatics for environmental protection, sustainable development and risk management, EnviroInfo 2013, Hamburg, Germany, September 2-4, 2013. Proceedings. Shaker, Hamburg, p 258–264
Rosinger C, Uslar M, Sauer J (2014) Using information security as a facet of trustworthiness for self-organizing agents in energy coalition formation processes. In: EnviroInfo. BIS-Verlag, Oldenburg, p 373–380
Steghöfer J-P, Kiefhaber R, Leichtenstern K, Bernard Y, Klejnowski L, Reif W, Ungerer T, André E, Hähner J, Müller-Schloer C (2010) Trustworthy organic computing systems: challenges and perspectives. Springer, Berlin, pp 62–76
Stonebraker M, Çetintemel U, Zdonik S (2005) The 8 requirements of real-time stream processing. SIGMOD Rec 34(4):42–47
Wang J, Shi D (2018) cyber-attacks related to intelligent electronic devices and their countermeasures: a review. In: 2018 53rd International Universities Power Engineering Conference (UPEC). IEEE, Glasgow
Xie B, Peng C, Yang M, Kong X, Zhang T (2019) A novel trust-based false data detection method for power systems under false data injection attacks. J Frank Inst. https://doi.org/10.1016/j.jfranklin.2018.10.030
Xing L (2020) Cascading failures in internet of things: review and perspectives on reliability and resilience. IEEE Internet Things J 4662:1–1
Xiong K, Ning P (2015) Cost-efficient and attack-resilient approaches for state estimation in power grids. In: Proceedings of the 30th annual ACM symposium on applied computing. ACM, Salamanca, p 2192–2197

Publisher's Note