

RESEARCH

Open Access

Trust assessment of power system states



Michael Brand*, Davood Babazadeh, Carsten Krüger, Björn Siemers and Sebastian Lehnhoff

From The 9th DACH+ Conference on Energy Informatics
Sierre, Switzerland. 29–30 October 2020

*Correspondence:
michael.brand@offis.de
OFFIS – Institute for Information
Technology, Escherweg 2, 26121
Oldenburg, Germany

Abstract

Modern power systems are cyber-physical systems with increasing relevance and influence of information and communication technology. This influence comprises all processes, functional, and non-functional aspects like functional correctness, safety, security, and reliability. An example of a process is the data acquisition process. Questions focused in this paper are, first, how one can trust in process data in a data acquisition process of a highly-complex cyber-physical power system. Second, how can the trust in process data be integrated into a state estimation to achieve estimated results in a way that it can reflect trustworthiness of that input?

We present the concept of an anomaly-sensitive state estimation that tackles these questions. The concept is based on a multi-faceted trust model for power system network assessment. Furthermore, we provide a proof of concept by enriching measurements in the context of the IEEE 39-bus system with reasonable trust values. The proof of concept shows the benefits but also the limitations of the approach.

Keywords: Power system, State estimation, Trust

Motivation

Modern power systems are cyber-physical systems (CPSs). The need for information and communication technology (ICT) and the dependency of power systems on ICT is growing. A major driver for this development is the energy transition implicating an increasing distributed generation based on renewable energy sources. This leads to the need to include more (end-) devices and their data into the data acquisition process to still be able to supervise and control the highly-complex CPS (Nijhuis et al. 2015; Pillitteri and Brewer 2014).

Better penetration of ICT in power systems gives us some advantages. We can gain more flexibility, efficiency, and sustainability (Nijhuis et al. 2015; Pillitteri and Brewer 2014). But it also comes along with some drawbacks. First, the ICT that helps to handle the increasing complexity leads itself to increased complexity. Second, interdependencies between the classical power system and the ICT can occur and are, potentially, hard to identify. Third, issues from ICT like cybersecurity become more important in a CPS (Pillitteri and Brewer 2014).

Against this background, the trustworthiness of process data, e.g. measurements from the field, is not given any more by definition. Process data could be manipulated by a cyberattack, provided by a non-credible data source, or not reliable because of the complexity of the CPS or interdependencies.

Cyber security issues are one example. In traditional power systems, cyber security is still often achieved through obscurity (Pillitteri and Brewer 2014). But modern power systems use standardized protocols, interfaces, and software to achieve better interoperability (Greer et al. 2014). Furthermore, security mechanisms like encryption often interfere with real-time constraints, limited resources, and costs (Pillitteri and Brewer 2014). Coordinated false data injection attacks (FDIAs) (Liu et al. 2011), for example, have been proven to be potentially undetectable by state-of-the-art state estimation and bad data detection. The idea behind coordinated FDIAs is to hide the manipulation of process data with knowledge about the system, i.e. to change the process data in a coordinated way so that it gives the impression of reasonable values (Liu et al. 2011).

And security is just one aspect. One can question, whether the devices function correctly or whether they are still reliable. Therefore, we propose to use the terminologies “trust” and “trustworthiness” as an umbrella for the different aspects like security, reliability, and credibility.

The question, whether measurements are trustworthy, is closely linked to the question, whether a state estimation result, i.e. the estimated complex voltages at the buses, is trustworthy. The reason is that they are estimated based on the input measurements. Therefore, we present in this paper an approach to estimate the trustworthiness of state variables based on the trust assessment of the input measurements.

The contributions in this paper are the following:

- a model to assess trust in the power system network assessment (PSNA) process,
- an anomaly-sensitive state estimation (ASSE) that considers the trustworthiness of input measurements for a trust estimation of the state variables, and
- a proof of concept by enriching measurements in the context of the IEEE 39-bus system with reasonable trust values.

Related work

Trust is a well-known concept in the field of organic computing (OC) but there exist also adaptations for the field of power systems. This section gives an overview of research on trust in both fields.

Trust in organic computing

Steghöfer et al. (2010) propose a trust model, named OC-Trust, where agents interact with each other and with humans. The authors state that trust is context-dependent and multi-faceted. Concretely, they define six different trust facets:

- functional correctness as “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 et al. 2010),
- safety as “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 et al. 2010),

- security as “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 et al. 2010),
- reliability as “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 et al. 2010),
- credibility as “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 et al. 2010), and
- usability as “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 et al. 2010).

The authors of this paper adapt in Brand et al. (2019) OC-Trust to PSNA. The main difference in the context of PSNA to OC is that it is in terms of PSNA about trust in a process variable several devices (or agents) had an influence on.

Trust in power systems

In the context of the research project SmartNord, a trust model based on OC-Trust (Steghöfer et al. 2010) has been developed (Rosinger et al. 2013; Rosinger et al. 2014). Rosinger et al. (2014) define a trust tuple that contains the trust of an agent in another agent in a certain context and timeframe. The timeframe can be regarded as a special aspect of a context. The drawback of that approach for PSNA is the same as of OC-Trust.

Other research focuses on an increased trust by a distributed state estimation. Matei et al. (2012) assume agents in the field performing a distributed state estimation and assigning trust values to neighboring agents. The use of high trustworthy nodes, e.g. highly secured, is proposed by Zheng et al. (2010). Both work assume trust to be unidimensional in difference to OC-Trust, Smart Nord, and us. Furthermore, we focus on a centralized state estimation without the possibility to integrate secured nodes.

Many other measures against attacks like FDIAs focus on security and have drawbacks when the origin of a compromise is not a cyberattack (cf. Cui et al. (2012) and Liang et al. (2016) for an overview of detection schemes).

Trust in power system network assessment

Based on OC-Trust (Steghöfer et al. 2010) (cf. [Trust in power system network assessment](#)), we define PSNA-Trust as follows:

Definition 1 *Trust is a subjective, context-dependent, and multivariate sense about an entity with respect to its functional correctness, safety, security, reliability, credibility, and usability.*

The PSNA-Trust model, which is developed in the research project “Smart Grid Cyber-Resilience Laboratory” (OFFIS 2017) at OFFIS (cf. also Brand et al. (2019)), is visualized in Fig. 1 in the shape of a trust assessment pyramid. On the bottom level are objects of investigation that can be categorized into domains. Objects of investigation are processes, functions, or components, for which the trust shall be assessed. An example object of

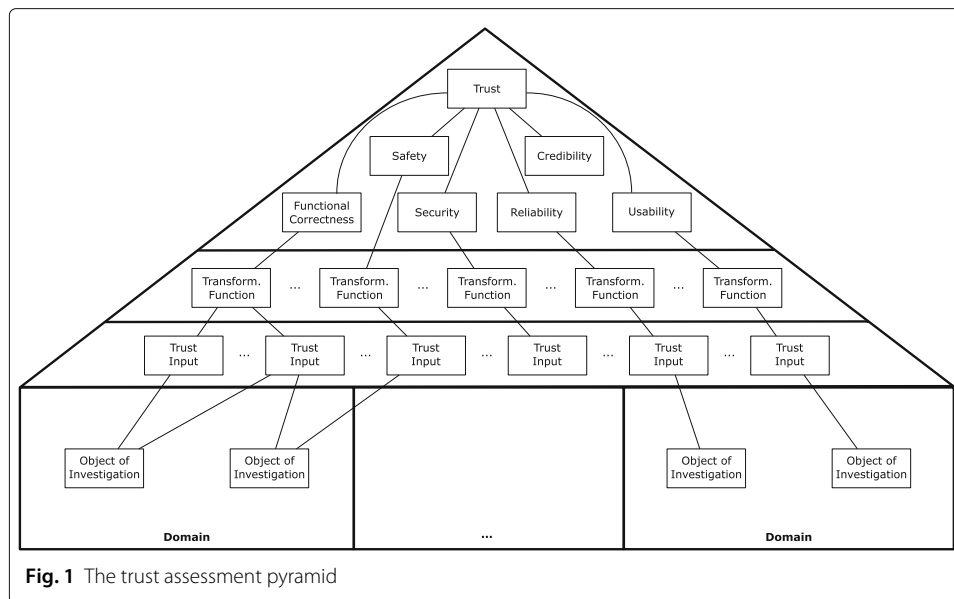


Fig. 1 The trust assessment pyramid

investigation can be the data acquisition process with metering devices, remote terminal units (RTUs), and routers as contained sub-objects of investigation. The metering devices can be classified into the power domain and the RTUs and routers into the ICT domain. Other examples for domains are the market and the cognitive domain. The latter becomes relevant when it is about humans and their behavior.

Trust inputs are located above objects of investigation in Fig. 1. They define the information that is used to assess the trust in the objects of investigation. Examples for trust inputs are quality-of-service information about components or network traffic. Trust inputs are provided by trust sources that can be represented by any tool, technique, or person that provide information about the object of investigation. Examples for trust sources are information technology (IT) monitoring tools that provide quality-of-service information and intrusion detection systems (IDSs) that collect information about the network traffic. The trust assessment pyramid abstracts from the concrete tools and technologies by only describing the trust inputs. Each trust inputs must be transformed into a single trust value t which domain is $[0, 1]$ ($t \in \mathbb{R}, 0 \leq t \leq 1$). In other words, single trust values reflect the probability that the object of investigation is trustworthy or not from the perspective of the source of the single trust value. The transformation is done by transformation functions and their output can contribute to several trust facets that are collections of single trust values mapped to their source. Transformations can include but are not limited to normalization, aggregation, and weighting.

Target application: state estimation

The PSNA-Trust model can be used for any purpose, where the trustworthiness of processes, components, or process data in a power system is of interest. An example purpose is the state estimation. The state estimation (Abur and Exposito 2004) estimates state variables, i.e. the complex voltages at the buses, based on, in most cases redundant, measurements. Typically, bad data detection (Abur and Exposito 2004) is added to the state estimation to detect, identify, and eliminate gross, independent measurement failures. If

bad data is detected and could be identified and eliminated, state estimation is run again. This iterative procedure ends when there is no bad data any more detected or if it can't be eliminated. It is important to make clear that bad data detection can only handle gross and independent measurement failures. Coordinated attacks like coordinated FDIAs can bypass the bad data detection as research on FDIAs (Liu et al. 2011) has proven.

Against this background, the use of the trustworthiness of input measurements in a state estimation can be of significance. It can give hints about a potential FDIA and other events in the system that compromise measurement data. This is a benefit compared to solutions that tackle only FDIAs or other cyberattacks. We propose in this context a so-called anomaly-sensitive state estimation (ASSE). The idea is to use anomaly detectors to estimate the trustworthiness of the input measurements for a state estimation and to include the trust data in the state estimation. An anomaly is in this context an event that reduces the trust in a process variable. Anomaly detectors are based on trust inputs such as alerts from an IDS or information from an IT-monitoring system. The complex trust value of an input measurement is aggregated to a single trust value $t \in [0, 1]$ and converted to a standard deviation. The state estimation result contains an uncertainty for each state variable, calculated based on the standard deviation of the input measurements. These uncertainties represent the trustworthiness of the state variables.

Proof of concept

The purpose of the proof of concept is to validate certain hypotheses about the effects of the reduced trustworthiness of measurements on the estimated state variables and their uncertainties. The hypotheses are the following:

Hypothesis 1 The trustworthiness of measurements from a single bus influences the trustworthiness of state variables in most cases not noticeable.

Hypothesis 2 The trustworthiness of measurements from multiple buses influences the trustworthiness of state variables in most cases noticeable.

Hypothesis 3 The trustworthiness of measurements from a single bus influences the estimation of state variables in most cases not noticeable.

Hypothesis 4 The trustworthiness of measurements from multiple buses influences the estimation of state variables in most cases noticeable.

The definition of the term “noticeable” depends on the state variable of investigation. Typically, the uncertainty of voltage magnitudes $u(V_m)$ is negligible, i.e. $u(V_m) \leq 0.001$ p.u. The uncertainty of voltage angles $u(V_a)$ is typically higher if no measurements from phasor measurement units but only from RTUs are available. Therefore, we consider an uncertainty for a voltage angle as noticeable if $u(V_a) > 0.03^\circ$ holds. For voltage magnitude values, the standard deviation of the metering devices is used as a threshold for the term “noticeable”, i.e. the estimated voltage magnitudes should not vary more than the maximum standard deviation of the metering devices compared to a scenario with full trustworthiness. This approach is not feasible for voltage angles because we neither have metering devices nor standard deviations for them. We consider triple the maximum standard deviation of the metering devices compared to a scenario with full trustworthiness as the threshold for the term “noticeable”.

The reason for the hypotheses is that the state estimation should be able to use other measurements from buses in the neighborhood if only measurements from one bus are

affected. If a complete neighborhood is affected, the deviations (errors) of the measurements are no longer independent as expected in the state estimation process (Abur and Exposito 2004). In the remainder of this section, information about the setup is provided. Afterward, the results of the proof of concept are presented and discussed.

Setup

The setup for the proof of concept is divided into the setup of the CPS and the setup of the trust assessment.

Cyber-Physical system

The physical part of the CPS of investigation is the IEEE 39-bus system (Pai et al. 1989). It consists of 29 PQ buses, i.e. buses for which active (P) and reactive (Q) power measurements are available, 9 PV buses, i.e. buses for which P and voltage magnitude (V_m) measurements are available, and a slack bus, i.e. a bus for which a V_m measurement is available and the voltage angle (V_a) is defined as 0° . We assume one RTU per bus transmitting the measurements of the respective bus. The ICT system is assumed to be structured as the power system, i.e. 39 routers, one per RTU, connected according to the branches of the power system. The router at bus 16 is assumed to be connected to the router of the control room. The configuration of the state estimator is the following. It stops the iterative process if the improvement compared to the last iteration is less or equal than $\epsilon = 0.001$ or if it needs 50 iterations.

Trust assessment

Figure 2 shows an instantiation of the trust pyramid (cf. Fig. 1) for the proof of concept. The object of investigation is the data acquisition process with three relevant types of

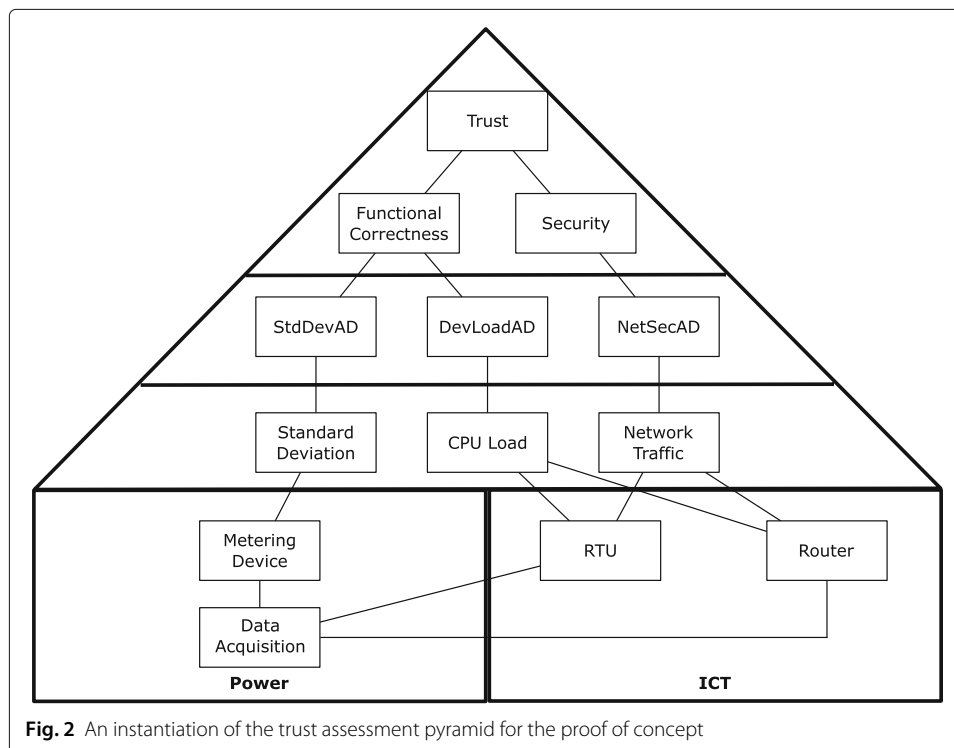


Fig. 2 An instantiation of the trust assessment pyramid for the proof of concept

components: metering devices, RTUs, and routers. Trust inputs are the standard deviations of the metering devices, CPU load information of the RTUs and routers, and network traffic information. Accordingly, three anomaly detectors (transformation functions) are used. The first is a static one that transforms the standard deviation of the metering devices into a trust value for the functional correctness facet: $t_{stdDev}(y) = 1 - stdDev_{m_y}$. y is a measurement, m_y the device metering y , and $stdDev_{m_y}$ the standard deviation of that metering device. The second anomaly detector is named “network security anomaly detector” and provides a trust value for the security facet. It is based on alerts from an IDS. The calculation of a trust value based on alerts for potentially several devices that are involved in the data acquisition of measurement is based on Liu et al. (2015).

$$\Omega_i = \sqrt{1 + \sum_{k \in a(i)} m^{p(k)}} \quad (1)$$

The so-called network impact factor (Liu et al. 2015) Ω of alerts for a specific device i is calculated as shown in Equation 1. $a(i)$ is the set of alerts for i , $p(k)$ the priority of an alert k , and m a weight coefficient for the threat priority (Liu et al. 2015). Ω increases with the amount and severity of alerts. Its boundaries are 1 for $|a(i)| = 0$ and $\lim_{|a(i)| \rightarrow \infty} \Omega_i = \infty$.

$$t_{netSec}(y) = \frac{|I|}{\sum_{i \in I} \Omega_i} \quad (2)$$

Based on the network impact factor, we define the trustworthiness $t_{netSec}(y)$ of a measurement y as in Equation 2. I is the set of devices involved in the data acquisition of y . The boundaries of $t_{netSec}(y)$ are 1 for $\Omega = |I|$ and $\lim_{\Omega \rightarrow \infty} t_{netSec}(y) = 0$.

The third anomaly detector is named “device load anomaly detector” and provides a trust value for the functional correctness facet. It is based on CPU load information (Lewis 2019) for devices from an IT monitoring system.

$$t_{devLoad}(i) = \begin{cases} 0 & l_{CPU,5} > 5 \cdot c \\ 0.25 & c < l_{CPU,5} \leq 5 \cdot c \\ 0.5 & 0.7 \cdot c < l_{CPU,5} \leq c \\ 1 & else \end{cases} \quad (3)$$

The trustworthiness of a single device y based on the average CPU load of the last five minutes ($l_{CPU,5}$) is calculated as shown in Equation 3. c is the number of available cores. The calculation of a trust value based on average load information is based on Lewis (2019). We chose the average of the last five minutes because the average of the last minute is too volatile and the average of the last fifteen minutes is too long-running in our scenario, where we get measurements every fifty milliseconds. The thresholds of $5 \cdot c$, c , and $0.7 \cdot c$ are based on the rules described in Lewis (2019). They are configurable and, in general, all anomaly detectors and the choice of the anomaly detectors are configurable.

$$t_{devLoad}(y) = \frac{1}{|I|} \sum_{i \in I} t_{devLoad}(i) \quad (4)$$

Based on the device load metric for single devices, we define the trustworthiness $t_{devLoad}(y)$ of a measurement y as in Equation 4. I is the set of devices involved in the data acquisition of y . The boundaries of $t_{devLoad}(y)$ are 1 for $t_{devLoad}(i) = 1 \forall i \in I$ and 0 for $t_{devLoad}(i) = 0 \forall i \in I$.

Scenarios

In our proof of concept, we want to investigate seven scenarios. In the scenarios, we investigate the influence of a high priority IDS alert, of a high average device load, or both. Furthermore, we investigate the behavior if the reduced trustworthiness is for an RTU, concrete at bus 26, or for a router that is involved in the data acquisition of measurements from several RTUs, concrete the router at bus 26. The scenarios are the following:

Scenario 1 no anomaly detectors except the static standard deviation of the metering devices (baseline),

Scenario 2 an IDS alert for RTU 26,

Scenario 3 a high device load average for RTU 26,

Scenario 4 a combination of Scenario 2 and 3,

Scenario 5 an IDS alert for router 26,

Scenario 6 a high device load average for router 26, and

Scenario 7 a combination of Scenario 5 and 6.

$t_{netSec}(y)$ is calculated based on Equation 1 and 2 with $m = 2$, $p(k) = 3$ for a single alert, and five routers involved. The trust value is $t_{netSec}(y) = \frac{6}{5+\sqrt{9}} = 0.75$ for all y provided by RTU 26 in Scenario 2. In Scenario 5, $|I|$ is 6, 7, 8, and 9 for measurements provided by RTU 26, 28, 29, and 38, respectively. $t_{devLoad}(y)$ is calculated based on Equation 3 and 4 with $c = 1$ and an average load of the last five minutes of $c < I_{CPU,5} \leq 5 \cdot c$. The trust value is $t_{devLoad}(y) = \frac{5+0.25}{6} = 0.875$ for all y provided by RTU 26 in Scenario 3. In Scenario 6, $|I|$ is on the lines of Scenario 5. For Scenario 4 and Scenario 7, the multiplication of all single trust values ($t_{stdDev}(y) \cdot t_{netSec}(y) \cdot t_{devLoad}(y)$) is used to aggregate the complex trust values to a single one.

Results

Table 1 gives an overview of the key findings on a grid-wide scale. The number of used iterations in the state estimation process and even whether it converges or not differs for the particular scenarios. In Scenario 1, six iterations are needed. For a decreased trustworthiness of measurements of a single bus (Scenario 2–Scenario 4), the state estimator converges and the used iterations increase with a decrease of the trustworthiness of the measurements. The state estimator does not converge when the trustworthiness of measurements from several buses is decreased (Scenario 5–Scenario 7). This shows the influence of changing the trustworthiness in terms of standard deviations of the input measurements on the state estimation behavior.

The V_m and V_a values are always compared to the baseline while the $u(V_m)$ and $u(V_a)$ values are absolute. The amounts of buses with noticeable deviations or uncertainties are calculated based on our assumptions of noticeable values (cf. Proof of concept). The results do not comply with Hypothesis 1 (no noticeable uncertainties in Scenario 2–Scenario 4). There are noticeable values for up to four V_m and thirty-eight V_a values. The uncertainties for V_m values are low (max. 0.004 p.u.) but can be high for V_a values (max. 0.82°). For Hypothesis 2 (noticeable uncertainties in Scenario 5–Scenario 7), the results are as expected. There are noticeable uncertainties for up to thirty-one V_m and thirty-eight V_a values. The uncertainties for V_m and V_a values can be high (max. 0.146 p.u. and 4.011°, respectively). The results do also comply with Hypothesis 3 and Hypothesis 4 (no noticeable value changes).

Table 1 Overview of the results for the respective scenarios compared to the baseline [Scenario 1](#)

Scenario	1	2	3	4	5	6	7
# iterations of state estimator	6	8	6	24	50	50	50
minimum V_m dev. [p.u.]	-	0	0	0	0	0	0
maximum V_m dev. [p.u.]	-	0.001	0	0.001	0.001	0.001	0.001
average V_m dev. [p.u.]	-	≈ 0	0	≈ 0	≈ 0	≈ 0	≈ 0
# buses with noticeable V_m dev.	-	0	0	0	0	0	0
minimum $u(V_m)$ [p.u.]	0	0.001	0.001	0.001	0.001	0.001	0.001
maximum $u(V_m)$ [p.u.]	0.001	0.003	0.002	0.004	0.11	0.051	0.146
average $u(V_m)$ [p.u.]	≈ 0	0.001	0.001	0.001	0.013	0.006	0.0171
# buses with noticeable $u(V_m)$	0	3	1	4	31	28	30
minimum V_a dev. [°]	-	0	0	0	0	0	0
maximum V_a dev. [°]	-	0.002	0.002	0.002	0.003	0.001	0.003
average V_a dev. [°]	-	0.001	0.001	0.001	0.002	≈ 0	0.002
# buses with noticeable V_a dev.	-	0	0	0	0	0	0
minimum $u(V_a)$ [°]	0.001	0.001	0.001	0.001	0.001	0.001	0.001
maximum $u(V_a)$ [°]	0.036	0.592	0.313	0.82	3.13	1.694	4.011
average $u(V_a)$ [°]	0.024	0.391	0.206	0.541	0.754	0.537	0.977
# buses with noticeable $u(V_a)$	3	38	38	38	38	38	38

The content of [Table 2](#) is focused on the buses with measurements for which the trustworthiness has been reduced in the different scenarios. It can be seen that the value differences and uncertainties match the maximum values in [Table 1](#). In other words, the state variables, related to buses to which also the measurements with reduced trustworthiness are related to, and their uncertainties are affected most.

Discussion

The results comply with three of four hypotheses. The fact that the data does not comply with [Hypothesis 1](#) is not a bad result either. It shows that, at least in this setup, also the reduced trustworthiness of measurements from a single bus influences the uncertainty of the related state variables.

Table 2 Results for specific buses and the respective scenarios compared to the baseline [Scenario 1](#)

Scenario	1	2	3	4	5	6	7
bus 26: V_m dev. [p.u.]	-	0	0	0	0	0	0
bus 26: $u(V_m)$ [p.u.]	0.001	0.003	0.002	0.004	0.042	0.019	0.055
bus 26: V_a dev. [p.u.]	-	0.002	0.002	0.002	0.003	0.001	0.003
bus 26: $u(V_a)$ [p.u.]	0.026	0.592	0.312	0.82	1.045	0.763	1.346
bus 28: V_m dev. [p.u.]	-	0	0	0	0	0	0
bus 28: $u(V_m)$ [p.u.]	0.001	0.002	0.001	0.002	0.082	0.038	0.108
bus 28: V_a dev. [p.u.]	-	0.001	0.001	0.002	0.002	0	0.003
bus 28: $u(V_a)$ [p.u.]	0.027	0.591	0.313	0.818	1.543	1.034	1.963
bus 29: V_m dev. [p.u.]	-	0	0	0	0	0	0
bus 29: $u(V_m)$ [p.u.]	0.001	0.001	0.001	0.002	0.093	0.043	0.122
bus 29: V_a dev. [p.u.]	-	0.002	0.001	0.002	0.003	0	0.003
bus 29: $u(V_a)$ [p.u.]	0.029	0.59	0.313	0.817	1.892	1.177	2.4
bus 38: V_m dev. [p.u.]	-	0.001	0	0.001	0.001	0.001	0.001
bus 38: $u(V_m)$ [p.u.]	0.001	0.001	0.001	0.001	0.11	0.051	0.146
bus 38: V_a dev. [p.u.]	-	0.002	0.001	0.002	0.002	0	0.003
bus 38: $u(V_a)$ [p.u.]	0.036	0.59	0.313	0.817	3.13	1.694	4.011

Another key finding is that the state estimator does not converge when the trustworthiness of several data sources is reduced. This is an unintended issue. The reason is most probably that, in a typical state estimation, the measurement errors are assumed to be independent. Our results show that for dependent measurement errors, expressed by reduced trustworthiness, the convergence of the state estimation is not given any more in all scenarios. Therefore, we are convinced that it is not an optimal solution to convert complex trust values to standard deviations of measurements. We should rather investigate on a solution that reflects the trustworthiness of the measurements but does not affect the convergence of the state estimation.

Future work

The convergence behavior of the state estimator is one of the key findings of the proof of concept. We plan to investigate on how to enhance the state estimation by a calculation of complex, multi-faceted trust values based on complex, multi-faceted trust values of the measurements. Another aspect of future work is a comprehensive evaluation. The proof of concept is meant to test the concept and to identify conceptual errors (cf. the already mentioned aspect of future work). With an improved concept and realization, a more comprehensive evaluation with more anomaly detectors and events that compromise the measurements is planned. A third aspect is a further development of the information model of the trust assessment. With a more comprehensive information model, it shall be possible to model the trust assessment for different components, processes, and power systems in general.

Conclusion

With the ASSE, we proposed in this paper a special kind of state estimation. It calculates uncertainties of estimated state variables based on the trustworthiness of measurements. The trust in measurements and process data, in general, is founded on PSNA-Trust, a multi-faceted trust model. A proof of concept showed the benefits but also the limitations of the approach. On the one hand, we saw how the reduced trustworthiness of measurements from a single bus and multiple buses influences the uncertainty of the estimated state variables. But, on the other hand, we also found out that the state estimator does not converge in all scenarios. That is the case if measurements from more than one bus are affected by reduced trustworthiness. A solution for this is the main goal of future work.

About this supplement

This article has been published as part of *Energy Informatics Volume 3 Supplement 1, 2020: Proceedings of the 9th DACH+ Conference on Energy Informatics*. The full contents of the supplement are available online at <https://energyinformatics.springeropen.com/articles/supplements/volume-3-supplement-1>.

Authors' contributions

All authors together developed the idea of PSNA-Trust and the trust pyramid. MB was in-charge of developing the ASSE and writing the paper. The co-authors contributed with text and expert knowledge in the field of PSNA. All authors read and approved the final manuscript.

Funding

The research project Smart Grid Cyber-Resilience Lab is funded by the Federal Ministry for Economic Affairs and Energy under the agreement no. 0350008. Publication costs were covered by the DACH+ Energy Informatics Conference Organizers, supported by the Swiss Federal Office of Energy.

Availability of data and materials

There are no sources of data or materials in this article available.

Competing interests

The authors declare that they have no competing interests.

Published: 28 October 2020

References

- Abur A, Exposito AG (2004) *Power System State Estimation: Theory and Implementation*. Marcel Dekker, Inc., New York and Basel
- Brand M, Babazadeh D, Lehnhoff S, Engel D (2019) Trust in control: a trust model for power system network assessment. In: EPJ Web of Conferences, vol. 217. EDP Sciences, Les Ulis Cedex A, Irkutsk. p 01008
- 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 Process Mag* 29(5):106–115
- Greer C, Wollman DA, Prochaska DE, Boynton PA, Mazer JA, Nguyen CT, FitzPatrick GJ, Nelson TL, Koepke GH, Hefner Jr AR, et al. (2014) NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. Technical report, NIST
- Lewis A (2019) Understanding Linux CPU Load - when should you be worried? <https://scoutapm.com/blog/understanding-load-averages>. Accessed 28 May 2020
- Liang G, Zhao J, Luo F, Weller SR, Dong ZY (2016) A review of false data injection attacks against modern power systems. *IEEE Trans Smart Grid* 8(4):1630–1638
- Liu Y, Ning P, Reiter MK (2011) False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans Inf Syst Secur (TISSEC)* 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. *Futur Gener Comput Syst* 49:94–103
- Matei I, Baras JS, Srinivasan V (2012) Trust-based multi-agent filtering for increased smart grid security. In: 2012 20th Mediterranean Conference on Control & Automation (MED). IEEE, Barcelona. pp 716–721
- Nijhuis M, Gibescu M, Cobben J (2015) Assessment of the impacts of the renewable energy and ICT driven energy transition on distribution networks. *Renew Sust Energ Rev* 52:1003–1014
- OFFIS (2017) Smart Grid Cyber-Resilience Laboratory. <https://www.offis.de/en/offis/project/cybreslab.html>. Accessed 08 June 2020
- Pai M, Athay T, Podmore R, Virmani S (1989) IEEE 39-Bus System
- Pillitteri VY, Brewer TL (2014) Guidelines for Smart Grid Cybersecurity. Technical report, NIST
- Rosinger C, Uslar M, Sauer J (2013) Threat Scenarios to evaluate Trustworthiness of Multi-agents in the Energy Data Management. In: *EnvirolInfo*. Shaker Verlag, Aachen. pp 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: *EnvirolInfo*. BIS-Verlag, Oldenburg. pp 373–380
- Stegh fer J-P, Kiefhaber R, Leichtenstern K, Bernard Y, Klejnowski L, Reif W, Ungerer T, Andr e E, H hner J, M ller-Schloer C (2010) Trustworthy Organic Computing Systems: Challenges and Perspectives. In: *International Conference on Autonomic and Trusted Computing*. Springer, Berlin. pp 62–76
- Zheng S, Jiang T, Baras JS (2010) Trust-aware state estimation under false data injection in distributed sensor networks. In: *Proceedings of TECHCON*, Orlando. pp 1–4

Publisher’s Note

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

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

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

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