Information Inconsistencies in Smart Distribution Grids under Different Failure Causes modelled by Stochastic Activity Networks

Romina Muka
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
romina.muka@ntnu.no

Fredrik Bakkevig Haugli
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
fredrik.haugli@ntnu.no

Hanne Vefsnmo
SINTEF Energy Research
Trondheim, Norway
hanne.vefsnmo@sintef.no

Poul E. Heegaard
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
poul.heegaard@ntnu.no

***Abstract*—The ongoing digitalization of the power distribution grid will improve the operational support and automation which is believed to increase the system reliability. However, in an integrated and interdependent cyber-physical system, new threats appear which must be understood and dealt with. Of particular concern, in this paper, is the causes of an inconsistent view between the physical system (here power grid) and the Information and Communication Technology (ICT) system (here Distribution Management System). In this paper we align the taxonomy used in International Electrotechnical Commission (power eng.) and International Federation for Information Processing (ICT community), define a metric for inconsistencies, and present a modelling approach using Stochastic Activity Networks to assess the consequences of inconsistencies. The feasibility of the approach is demonstrated in a simple use case.**

***Index Terms*—smart grid dependability, cyber-physical system modelling, dependability taxonomy, stochastic activity networks**

I. Introduction

The pace of digitalization in energy is increasing and is helping to improve the safety, productivity, accessibility and sustainability of energy systems, but it is also raising new security and privacy risks [1]. Adding more and new Information and Communication Technology (ICT)-devices into the electricity distribution grid and smart meters to homes, gives opportunities to operate, plan and maintain the electricity distribution grid smarter. New sensors and communication equipment will give more timely and precise information about the system state, which will enable automation, e.g., for restoration of supply after a fault, the so-called self-healing [2]. This will result in faster restoration, shorter interruption duration, reduction in interruption cost and simplify the resource management. It should be kept in mind that this functionality targets the frequent occurrences, which are anticipated in the system design.

However, this is achieved by the introduction of a new functionality, partly distributed as in Intelligent Electronic Device (IED), and partly centralised by enhancing the surveillance and control system (in this paper referred to as Distribution Management System (DMS)). This increases the total complexity and creates an interdependent system [3] of ICT and power grid (PG) functionality.

Such a (cyber-physical) system will not only have additional features, but unfortunately also new failures causes (faults), failure modes, and failure semantics [4], [5], and they may also manifest a more fragile behaviour in critical situations [6], [7]. Figure 1 illustrates a risk curve where the events with high "probability" have low consequences, and the events with low "probability" have high consequences. The introduction of the ICT-based support system, e.g., an ICT-based surveillance and control system with distributed sensors and controllers to operate critical infrastructure such as *Smart Grid*, is expected to reduce the consequences and probability of the frequent events. At the same time, the complexity and interdependency in the total system will increase, with a potential increase in the probability of critical events with extensive, and long lasting consequences. Such events might affect large parts of the system, and will take long time to recover from because of the lack of understanding the complexity, or the lack of the maintenance support and coordination between the different subsystems and domains. As indicated in the figure, it is not only necessary to increase the focus and manpower on the events with larger consequences, but also increase the competence of the operation personnel.

The novelty introduced in this paper is its focus on the dependability [9] of a smart distribution grid, operated by the support of an advanced surveillance and control system with distributed sensors and controllers (IEDs). The main objective is to investigate the causes of inconsistencies between the state of the power grid and the state view in the DMS, and to propose a modelling approach for assessment of these inconsistencies.

Section II presents related work, while Section III introduces the necessary taxonomy which includes terms from both the ICT and PG domains. A model used to illustrate the point of information inconsistencies is described in Section IV with

This paper has been funded by CINELDI - Centre for intelligent electricity distribution, an 8 year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners.

978-8-8872-3745-0

This is the accepted version of an article published in 2019 AEIT International Annual Conference
http://dx.doi.org/10.23919/AEIT.2019.8893378

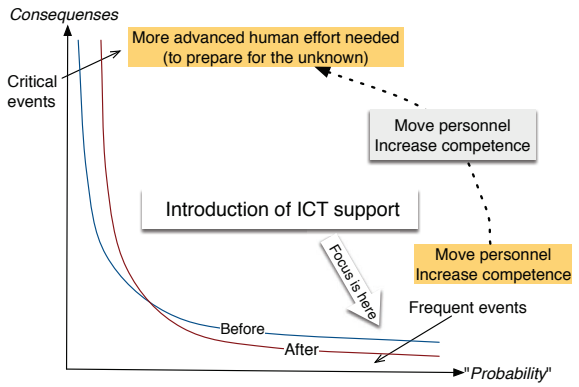
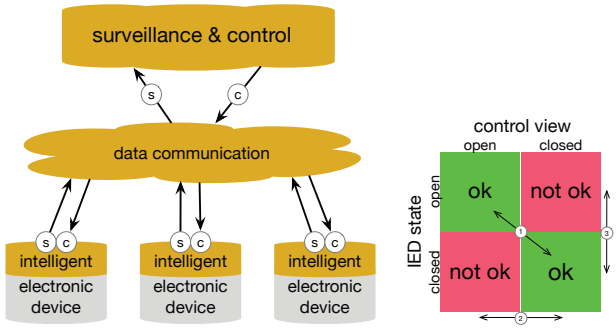


Fig. 1. Introducing ICT operations' support might increase the overall risk [8]



(a) IED control (b) Inconsistent view

Fig. 2. Inconsistencies between control view and IED state

results and discussions in Section V, before the paper is concluded in Section VI.

II. Related work

The consequences of incorrect information in control systems have been studied primarily from the information security point of view. Several authors have used state estimation techniques in order to detect anomalous data injected with the intent of causing disruptions. A review of False Data Injection attacks against modern power systems is given in [10]. In [11], a new architecture to provide local advanced measurement information to the Distribution System Operator is introduced. The *Next Generation Open Real Time Smart Meter* (NORM), can be used to monitor the data grid inconsistencies to detect cyber security threats to secure the grid operations and continuous supply of energy to end-customers.

Several methods for cyber security risk assessment have been proposed. In [12], a review and classification of twenty-four methods for risk assessment methods for Supervisory Control And Data Acquisition (SCADA) systems is presented. Other works have studied reliability assessment of smart grid considering cyber-power interdependencies [13] and of cyber physical distribution system [14].

In [15], Petri Nets are used to model the information flow in a SCADA system and to analyze system for attack vectors. The actual state of a valve and its state representation in the SCADA system is modelled by two different places, but does not evaluate the probability of inconsistencies.

Sensor faults are studied in [16]. The focus is on transient sensor faults in real deployments, and four different fault detection techniques were implemented. The results demonstrate the data corruption problem, emphasizing the importance of studying data inconsistencies to provide a high-confidence sensor fault detection in the power grid.

Different failure modes in smart grid communication have been investigated in [17]. The focus is on the effect of value failures on control signals.

III. Failure causes for inconsistencies

The integrated ICT and PG system studied in this paper is defined to include the DMS, the data communication network, the software in the IEDs, and physical elements in the power grid (e.g., breakers, power lines, disconnectors). In this section we introduce the necessary terminology to describe the causes of failures in such an integrated system, and the consequences of inconsistencies between ICT view and PG state.

A. Inconsistencies between DMS view and IED state

The DMS depends on correct view of the state of physical devices (and power flows and voltage quality). Correct state view is crucial in order for the *controller* to trigger the correct action and to change the state of the electric grid when needed, as well as for the human operators to correctly assess the state of the grid. In Figure 2(a) a principle sketch of the system considered in this paper is given. Intelligent electronic devices (IEDs) are assumed to contain sensors (s) and a controller (c), which are interconnected and also connected to a surveillance and control system via a data communication network. E.g., the state of the electronic device is observed by a sensor. The signal is sent via the data communication network to the surveillance and control system, which processes it and decides whether actions need to be taken to change the state of the electronic device (or other actions to restore power supply, regulate voltage, change the power flow). An appropriate control message is then sent to the IED via the same data communication network.

Figure 2(b) shows an example of inconsistencies (in red) between the surveillance and control view and the state of, e.g., a physical disconnector position of an IED. The disconnector can be closed, while the surveillance and control system believes it is open, and vice versa. In the following, different causes of such inconsistencies (indicated with (2) and (3) in the figure) are discussed.

B. Taxonomy

To describe the causes and consequences of failures, both the power grid (IEC-60050-192) and ICT domain (IFIP WG 10.4) have defined a set of terms.

In IEC-60050-192 [9] the following terms are defined

This is the accepted version of an article published in 2019 AEIT International Annual Conference
http://dx.doi.org/10.23919/AEIT.2019.8893378

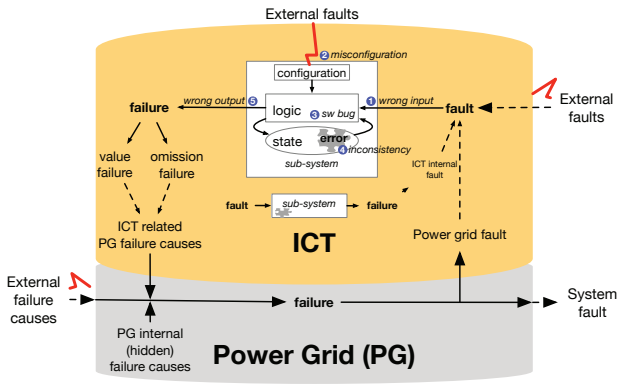


Fig. 3. Terminology

- *Failure cause* - set of circumstances that leads to failure [IEC60050-192-03-11]
- *Fault (of an item)* - inability to perform as required, due to an internal state [IEC60050-192-04-01]
- *Failure (of an item)* - loss of ability to perform as required [IEC60050-192-03-01]

Correspondingly, IFIP WG 10.4 [18], [19] defines

- *Fault* - adjudged or hypothesized cause of an error
- *Error* - part of the system state which is liable to lead to a failure
- *Failure* - deviation of the delivered service from compliance with the specification; transition from correct service to incorrect service (e.g., the service becomes unavailable)

In an ICT system, the definitions of fault, error and failure is implicitly a sequence ("pathology") of events. Errors are initially confined within the ICT system and may be interpreted as something wrong in the internal state of the system. When a fault produces an error, it is said to be active. An internal fault which has not produced errors is said to be dormant. Similarly, an error which is not detected, is said to be latent (confer hidden failure in next section). When the error becomes visible at the system boundary (e.g., a system can be a sub-system inside the ICT system), we have a failure.

Most software in today's ICT systems is continuously operating and has an internal state which is maintained across several inputs (e.g., sensor data, controller commands). Examples of such systems are surveillance and control systems, and the software logic in IEDs in the power grid. The subsystem in the ICT part of Figure 3 is using what is referred to as a Moore/Mealy model [20], [21] to describe the failure mechanisms relevant to the software that is modelled in this paper. In a Moore/Mealy model, any combination of a wrong input signal (e.g., sensor data) (denoted (1) in blue), a misconfiguration (2), or a faulty logic of the software (3), will introduce an error in the state space of the software, e.g., an inconsistency (4) in the data of the system. This will again lead to a wrong output signal (5) (e.g., a control command). Note that the fault activation may be conditioned by a specific (set of) internal states of the software, and hence, it is the combination of the internal state and the input signal, logic, and configuration, which causes the fault activation.

After a latency period this error may cause a failure of the software system, and give rise to a failure that can eventually be an ICT related power grid failure cause. The failure (semantics) is either:

- *Omission* (incl. timing) failure - the signal is lost, e.g., sensors are not sending data or sensor data is not received, corrupted, or delayed
- *Value* failure - the signal is incorrect but valid, e.g., data from a sensor or controller is changed to a legit/valid (not corrupted), but incorrect value

C. Failure causes

A large number of different *failure causes* (denoted *faults* in the ICT terminology) will affect different parts of the system in Figure 2(a). In Norway, the power system failure causes are standardized and reported through the Norwegian data management system, FASIT [22]. FASIT distinguish between *external* and *internal* failure causes related to what the grid company can control itself. In this paper we use external and internal failure causes as follows: the external failure causes include *environment* (weather-related causes), *operating stresses* (stresses above critical level, e.g., excessive load of ICT system), and *human errors* performed by people outside of the organization, either (i) intended, such as malicious attack and intrusion, or (ii) unintended). Environment causes account for approximately 50% of the failures in the Norwegian distribution grid 1-22 kV [23]. The major weather-related causes are wind, vegetation and lightning.

The internal failure causes are related to components themselves or the grid or telecom operator. It includes internal fault in an equipment (e.g. a stuck disconnector), or interaction or operational mistakes, accidentally made by staff or hired personnel that are operating or maintaining a system. An internal failure is a *hidden* failure cause when it is dormant and not visible until it is needed (e.g., a stuck disconnector is not detected until it should be switched).

These failure causes are leading to permanent (solid, persistent), transient (present short time) or intermittent faults (comes and goes). A *permanent fault* is a fault that will remain unless it is removed by some intervention [IEC60050-192-04-04]. A *transient fault* is a fault that disappears without intervention [IEC60050-192-04-05]. The disappearance may be due to self-recovery. A transient fault for instance on a power line will disappear after an automatic reclosure of the circuit breaker. An *intermittent fault* is a transient fault that recurs [IEC60050-192-04-06]. An intermittent fault can develop into a permanent fault, e.g., a crack in an insulator that result in flash-over in damp weather.

Design (logical) faults are human made faults during specification, design and implementation of hardware and software. Software faults are commonly referred to as *bugs*, and are logical mistakes or inadequacy during specification design or development, or dynamics in the deployed software processes

This is the accepted version of an article published in 2019 AEIT International Annual Conference
http://dx.doi.org/10.23919/AEIT.2019.8893378

described in the Moore/Mealy model above. A software bug is either *Bohrbugs* (easily reproducible), *Mandelbugs* (seemingly non-reproducible), and *Aging-related bugs* (software performance degraded due to e.g., memory leakage, data corruption, unreleased file locks), see [24] for more details.

IV. Intelligent Electronic Device model

To illustrate and assess the causes of information inconsistencies, a modelling approach is taken, using the Stochastic Activity Net (SAN) formalism. This is applied to an example with a remotely controlled disconnector, which is a rather simple but illustrative example with only two disconnector states (position open or closed), see Figure 2(b). We assume that the disconnector is remotely controlled and has a sensor that registers if the disconnector is open or closed. This model distinguishes between the actual state of the disconnector, the state observed by the control system (DMS) and the state commanded by the control system. This allows the inconsistencies between the true and observed state of the disconnector to be measured. Possible sources of inconsistencies are value failures in the sensor and communication failures, as well as software bugs internally in the control system.

A. Stochastic Activity Net

SAN [25] is an extension to the Stochastic Petri Net formalism, allowing more flexibility in the preconditions of transitions (called activities), as well as the effects of a transition. This allows for more expressive power, as well as more compact and succinct models. The model is developed using the Möbius tool [26]. It offers a modular formalism by defining submodels (atomic models) and composing them to form the overall model of the system. The full model is composed of several atomic models, each implemented as a SAN and joined together by shared places. This makes each part of the model easier to follow, and extend or simplify in the future. The following sections will explain the atomic models used to compose the full model. In general, places with the same name are shared between the atomic models, allowing them to see relevant portions of the state of other atomic models.

B. DMS view and software bugs

Figure 4 shows the atomic model of the DMS view of the disconnector. It has two states: *Closed* and *Open*. Transitions between these states are caused either by correct operation (the disconnector has switched state and the sensor and communication system works correctly), by a value failure in the sensor causing it to transmit the wrong state or by an internal software bug in the DMS. The two former cases are handled by the input gates in the model.

Note that we make no assumptions about where the monitoring and control system (DMS) is located. It can either be in a central control centre, locally in the IED or anywhere in between (substations, embedded in Platform-as-a-service solutions in the communication infrastructure, etc).

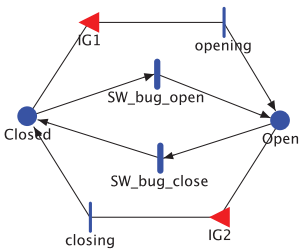


Fig. 4. An atomic model of the DMS view

C. Sensor and communication faults

We assume that the communication infrastructure consisting of all components required to send information between the sensor and the DMS is either working or not, with Poisson distributed failure and repair processes. The sensor itself may also stop sending measurements, and it may also start to send the wrong value (closed when the disconnector is open and vice versa). This value failure can occur due to firmware error, improper physical installation, calibration/configuration failure etc. We combine the sensor and communication infrastructure into one model with three places: *OK*, *OmissionFailure* (either the communication or the sensor is down) or *ValueFailure* (the sensor is sending incorrect but valid information). Transitions between these places happen with exponentially distributed intervals independently of the rest of the system. The model is shown in Figure 5. Packet losses are not included in the model, as we assume that the transmission protocol either uses retransmissions on missing acknowledgement, or that similar mechanisms are in place. The delay incurred by a retransmission of a missing packet would be negligible on the timescales we operate on, and is therefore omitted.

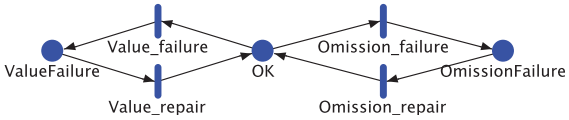


Fig. 5. An atomic model of sensor and communication

D. Faults in the disconnector

In order to include the possibility of the disconnector not responding, faults in the physical disconnector are also included in the model. In reality, this can for example be due to welding of the contactors, bad connection in the control signal or a software bug in the firmware that causes the disconnector to not react to commands.

This failure model is shown in Figure 6. Initially, the *DisconnectorOK*-place is marked, meaning that the disconnector works as it should. After an exponentially distributed interval, a transition moves the token to the *Stuck*-place. This means that the disconnector is stuck without anyone knowing, as we can only discover that it is stuck once it is attempted to operate it. The disconnector has a so-called *hidden fault*, as defined

This is the accepted version of an article published in 2019 AEIT International Annual Conference
http://dx.doi.org/10.23919/AEIT.2019.8893378

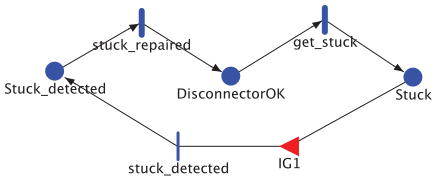


Fig. 6. An atomic model of the physical status of the disconnector

in Section III-C. When an opening or closing operation is attempted, the token is moved to the *Stuck_detected*-place. Here, the operators are aware of the problem and will initiate repair, and the token returns to the *DisconnectorOK*-place after an exponentially distributed repair time.

E. Actual state of the disconnector

An atomic model is developed for showing the actual state of the disconnector, closed or open represented by two places *Real_Closed* and *Real_Open* respectively, as shown in Figure 7. Transitions between these two places are caused by commands sent by the DMS when the sensor and communication is working, so there are no omission failures (see Figure 5), and in addition the physical status of the disconnector is not stuck (see Figure 6). *Real_opening* and *Real_closing* places are introduced in this atomic model to describe the fact that the disconnector might be stuck while attempted to operate it (see Section IV-D).

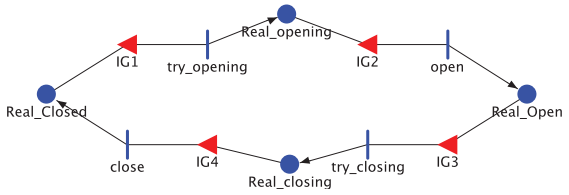


Fig. 7. An atomic model of the actual state of the disconnector

F. Disconnector commands

A simple atomic model has been created for the issuing of commands to open and close the disconnector with an exponetially distributed interval. A close-command is only sent when the DMS sees the disconnector as open and vice versa.

Note that we make no assumption of what is the reason to close or open the disconnector. Possible reasons can be fault clearing, maintenance, rerouting of power etc.

V. Results and Observations

To study the effects of the physical disconnector faults, sensor and communication faults, and software bugs in the DMS, a simulation study is conducted for measuring the information inconsistencies between the DMS view and the IED state. The metric that is used in this paper is *sensing inconsistency*, which is the *(stationary) probability that the observed state of a device deviates from the real state of the same device*. In the example in this paper, the device is a disconnector. This is measured as the portion of time when there was an inconsistency between the states *Open* and *Real_Open* or *Closed* and *Real_Closed* in the models of DMS view (Figure 4) and actual state (Figure 7) of the disconnector.

A. Model parameters

The values of the different intensities are presented in Table I, hereafter referred to as the base scenario.

TABLE I
Base scenario parameters

Parameter	Description	Value
$1/\lambda_{dgs}$	mean time to disconnector getting stuck	12 months
$1/\mu_{dgs}$	mean time to stuck diconnector repaired	4 hours
$1/\lambda_{swc}$	mean time to SW bug to closed	12 months
$1/\lambda_{swo}$	mean time to SW bug to open	12 months
$1/\lambda_{v}$	mean time to next value failure	6 months
$1/\mu_{v}$	mean time to value repair	5 minutes
$1/\lambda_{o}$	mean time to next omission failure	6 months
$1/\mu_{o}$	mean time to omission repair	30 minutes
$1/\lambda_{o_{cmd}}$	mean time to next open command	6 months
$1/\mu_{c_{cmd}}$	mean time to next close command	2 days

As these types of systems are not currently widely deployed, there is little available statistics to gather realistic parameters. These numbers are chosen as a base line. A sensitivity analysis was performed and described in Section V-B to determine which parameters had the most impact on the measured inconsistency, and should be investigated more in further work.

As systems generally can be made more reliable by investing (wisely) more money, one use of this model can be to evaluate how reliable the sensors need to be to ensure a given probability of consistent information.

B. Sensitivity analysis

In this section we perform a sensitivity analysis to determine which of the parameters have the highest impact on the information inconsistency. For each simulation, we vary one parameter by multiplying it with a scaling factor of 10 and 0.1, respectively, while keeping the rest of the parameters the same as defined in the base scenario. The results, sorted by the impact of the varied parameter in decreasing order, are presented in Figure 8.

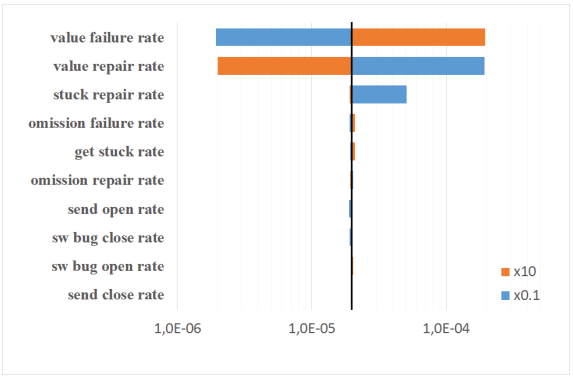


Fig. 8. Sensitivity analysis of the information inconsistency

This is the accepted version of an article published in 2019 AEIT International Annual Conference
http://dx.doi.org/10.23919/AEIT.2019.8893378

The base line result is an information inconsistency of 2×10^{-5}. This corresponds to an expected information inconsistency of around 10 minutes per year. It is marked with the vertical black line. The orange and blue bars show the result of scaling each parameter with 10 and 0.1 respectively.

C. Discussion

The most important parameters are value failure and repair rates. This is to be expected, as they directly influence the correctness of the measurement. The other significant parameter is the get stuck repair rate of the disconnector when it is decreased. This is due to the fact that the sensor will not report its state correctly when the disconnector is under repair. If there is a software bug in the DMS during this time, it will not be corrected until the repair is done.

The rest of the factors have negligible effect on the result. The omission failures will not contribute much to information inconsistencies as the system will not change state when the communication system is down. In future work it would be interesting to introduce operation of the disconnector that was not caused by the system. Under this circumstance, an omission failure would likely lead to the state change not being observed in the DMS.

It is interesting to note that the parameters related to software bugs in the DMS does not effect the information inconsistency. This is likely due to the error being corrected immediately. We have assumed that the disconnectors send their status continuously with some short interval, unless the disconnector is being repaired. If this was not the case, and the disconnectors only sent messages when the state changed, we might see a bigger impact from these internal bugs.

VI. Concluding remarks

The modelling approach proposed in this paper specifically focuses on assessment of causes of information inconsistencies between observed (in DMS) and real state of physical devices (e.g., a disconnector). Stochastic Activity Network has been used to model a simple example with a remotely controlled disconnector. A sensitivity analysis has been performed to identify the most critical parameters affecting this inconsistency. The study has shown the direct and high impact of value failures, i.e., sensor or controller data which are valid but wrong. We have also observed that software bugs in the DMS, have minor effect on inconsistency if continuous disconnector status updates are received. The model is flexible and can be scaled up to assess systems consisting of several IEDs, and add different failure modes and causes.

References

[1] International Energy Agency, *Digitalization and Energy*. IEA, 2017.

[2] P. L. Cavalcante, J. C. Lopez, J. F. Franco, M. J. Rider, A. V. Garcia, M. R. Malveira, L. L. Martins, and L. C. M. Direito, "Centralized self-healing scheme for electrical distribution systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 145–155, 2015.

[3] M. Heller, "Interdependencies in civil infrastructure systems," *The Bridge*, vol. 31, no. 4, 2001.

[4] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power and Energy Magazine*, vol. 7, no. 1, pp. 50–60, Jan. 2009.

[5] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[6] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[7] R. G. Morris and M. Barthelemy, "Interdependent networks: the fragility of control," *Scientific Reports*, vol. 3, 2013.

[8] P. E. Heegaard, B. E. Helvik, G. Nencioni, and J. Wäfler, *Managed Dependability in Interacting Systems*. Cham: Springer International Publishing, 2016, pp. 197–226. [Online]. Available: https://doi.org/10.1007/978-3-319-30599-8_8

[9] I. E. Commission, "Electropedia: The World's Online Electrotechnical Vocabulary - Dependability (IEC-60050-192)." [Online]. Available: http://www.electropedia.org/iev/iev.nsf/index?openform&part=192

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[11] M. Sanduleac, G. Lipari, A. Monti, A. Voulkidis, G. Zanetto, A. Corsi, L. Toma, G. Fiorentino, and D. Federenciuc, "Next generation real-time smart meters for ict based assessment of grid data inconsistencies," *Energies*, vol. 10, no. 7, p. 857, 2017.

[12] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

[13] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1515–1524, 2012.

[14] J. Liu, D. Wang, C. Zhang, Z. Tang, Z. Jiang, J. Liu, and Y. Xiang, "Reliability assessment of cyber physical distribution system," *Energy Procedia*, vol. 142, pp. 2021–2026, 2017.

[15] M. H. Henry, R. M. Layer, K. Z. Snow, and D. R. Zaret, "Evaluating the risk of cyber attacks on scada systems via petri net analysis with application to hazardous liquid loading operations," in *2009 IEEE Conference on Technologies for Homeland Security*. IEEE, 2009, pp. 607–614.

[16] A. B. Sharma, L. Golubchik, and R. Govindan, "Sensor faults: Detection methods and prevalence in real-world datasets," *ACM Transactions on Sensor Networks (TOSN)*, vol. 6, no. 3, p. 23, 2010.

[17] T. Amare and B. E. Helvik, "Dependability analysis of smart distribution grid architectures considering various failure modes," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Oct 2018, pp. 1–6.

[18] "IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance." [Online]. Available: http://www.dependability.org/wg10.4/

[19] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transaction on Dependable and Secure Computing*, vol. 1, pp. 11–33, 2004.

[20] E. F. Moore, "Gedanken-experiments on sequential machines," in *Automata studies*. Princeton University press, 1956, pp. 129 –153.

[21] G. H. Mealy, "A method for synthesizing sequential circuits," *Bell System Technical Journal*, vol. 34, no. 5, pp. 1045–1079, 1955. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1955.tb03788.x

[22] J. Heggset and G. Kjolle, "Experiences with the fasit reliability data collection system," in *2000 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 00CH37077)*, vol. 1. IEEE, 2000, pp. 546–551.

[23] G. Kjølle, H. Vefsnmo, and J. Heggset, "Reliability data management by means of the standardised fasit-system for data collection and reporting," in *Proc. CIRED*, vol. 2015, 2015.

[24] K. S. Trivedi and A. Bobbio, *Reliability and Availability Engineering: Modeling, Analysis, and Applications*. Cambridge University Press, 2017.

[25] W. H. Sanders and J. F. Meyer, *Stochastic Activity Networks: Formal Definitions and Concepts*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 315–343. [Online]. Available: https://doi.org/10.1007/3-540-44667-2_9

[26] S. Gaonkar, K. Keefe, R. Lamprecht, E. Rozier, P. Kemper, and W. H. Sanders, "Performance and dependability modeling with möbius," *ACM SIGMETRICS Performance Evaluation Review*, vol. 36, no. 4, pp. 16–21, 2009.

This is the accepted version of an article published in 2019 AEIT International Annual Conference
http://dx.doi.org/10.23919/AEIT.2019.8893378