Reliability Modeling Considerations for Emerging Cyber–Physical Power Systems

Prepared by Task Force on Reliability Consideration for Emerging Cyber-Physical Energy Systems under IEEE PES Reliability, Risk and Probability Applications Subcommittee

Aravinthan, Visvakumar; Balachandran, Thanatheepan ; Ben-Idris, Mohammed; Fei, Wanghao; Heidari-Kapourchali, Mohammad; Hettiarachchige-Don, Anton; Liu, Chen-Ching ; Stefanov, Alexandru; More Authors

DOI
10.1109/PMAPS.2018.8440331

Publication date
2018

Document Version
Final published version

Published in
IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)

Reliability Modeling Considerations for Emerging Cyber-Physical Power Systems

Prepared by Task Force on Reliability Consideration for Emerging Cyber-Physical Energy Systems under IEEE PES Reliability, Risk and Probability Applications Subcommittee

Visvakumar Aravinthan, Thanatheepan Balachandran, Mohammed Ben-Idris, Wanghao Fei, Mohammad Heidari-Kapourchali, Anton Hettiarachchige-Don, John N. Jiang, Hangtian Lei, Chen-Ching Liu, Joydeep Mitra, Ming Ni, Milorad Papic, Masood Parvania, Mojtaba Sephary, Channan Singh, Anurag Srivastava, Alexandru Stefanov, Hongjian Sun, and Simon Tindemans*

***Abstract*—Power system operation considering an increasingly complex cyber infrastructure may be one of the key factors of the next generation power systems. The effective operation of a power system in a massively deployed cyber network environment will be affected by cyber network reliability. Therefore, it is vital not only to understand the operation of a cyber network and its reliability, but also it is critical to integrate the interdependency of cyber and power systems into power system planning and operations. This requires a three-layer approach to reliability modeling and evaluation. The cyber and power layers are interconnected by the information layer. The objective of this paper is to define the three-layer model and report a generalized framework for combined reliability modeling.**

Keywords—cyber-physical power system; dependent system reliability modeling; cyber reliability; cyber-intrusion

I. INTRODUCTION

Modernization of the power system has gained substantial momentum in the last decade. As part of this modernization, automation and increased dependency on real-time tools are expected to improve power delivery [1]. This requires the availability of information and communication technologies at every level. For example, at the bulk level, grid operators can replace preventive control actions by corrective actions on the basis of grid visibility and real-time control actions. Distribution system operations can be improved by aggregators establishing virtual power plants with contracted distributed resources and end-user appliances to optimize their behavior according to price and control signals.

This work is produced as a part of the Reliability Consideration for Emerging Cyber-Physical Energy Systems task force report.

* ***Author names appear in alphabetical order***

Contributor affiliations: Chair: V. Aravinthan, *Wichita State University, USA*; Secretary: M. Ni, *State Grid EPRI, China*; T. Balachandran, *Wichita State University, USA*; M. Ben-Idris, *University of Nevada, Reno, USA*; ; Wanghao Fei, *University of Oklahoma, USA*; M. Heidari-Kapourchali, *Wichita State University, USA*; A. Hettiarachchige-Don, *Wichita State University, USA*; John Jiang, *University of Oklahoma, USA;* H. Lei, *University of Idaho, USA*; Chen-Ching Liu, *Virginia Polytechnic Institute and State University, USA*; J. Mitra, *Michigan State University, USA*; M. Papic, *Idaho Power, USA*; M. Parvania, *University of Utah, USA*; M. Sephary, *Wichita State University, USA*; C. Singh, *Texas A&M University, USA*; A. Srivastava, *Washington State University, USA*; A. Stefanov, *ESB Networks, Ireland*; H. Sun, *Durham University, UK*; S. Tindemans, *TU Delft, The Netherlands*

The objective of the power system is to supply the entire load on a system at all times [2] and a measure of fulfilling this objective is defined as reliability. The communication and decision tools are expected to improve the reliability of the power system. This should be achieved by both increasing the speed of reaction and improving preventative decisions in the anticipation of abnormal events.

The resulting system combining power and cyber layers is known as the cyber-physical power system (CPPS), and the availability of communication and decision tools will affect the reliability of the power network. The emerging CPPS is much more complex than traditional power systems, and traditional methods for assessing its reliability needs to be reviewed [3].

Traditional power system reliability modeling and evaluation considers the failure of various components as independent events. Communication and decision tools can be sources of failure for the following reasons:

- ***Component Failure***: Both cyber and decision tools, such as routers and servers, can fail. When this happens, communication may be interrupted, or decisions may not be made appropriately in the power system operation, thus affecting power system reliability.
- ***Cyber Unavailability***: Even without physical failure of cyber equipment, communication may not be interrupted due to packet loss, link unavailability, and packet delay. This could negatively affect the decision process, thereby deteriorating power system reliability.
- ***Cyber Intrusion***: Malicious manipulation of information could disrupt the decision process. Therefore, the effect of cyber intrusion on power system reliability needs to be incorporated.

Contrary to the power carrying components, communication and decision equipment cannot be modeled as independent components. For example, a communication link failure could result in multiple sensors not being able to send real-time information to decision centers, thereby resulting in an impact on decisions made by the control center. Therefore, cause-effect modeling could be utilized to model the CPPS by evaluating the following: (i) *threats*: external factors that could impact the reliability of the CPPS, (ii) *vulnerability*: the extent to which threats will affect the power system operation, and (iii)

978-1-5386-3596-4/18/$31.00 ©2018 IEEE

consequence: impacts to power system customers [5]. Reliability modeling and evaluation of the future power grid must take all of these into consideration.

The objective of this paper is to suggest approaches that could facilitate the reliability modeling and identify future needs. Different methods used in interdependent CPPS modeling for power system reliability computation are summarized in this work. Component-level and system-level reliability evaluation approaches are presented, and the future needs for CPPS reliability modeling along with industry standards, as defined by the North American Electric Reliability Corporation (NERC), are identified.

II. Cyber-Power System Model

The need for sensors, communication, and real-time decision making are intensifying in order to meet future needs, especially those involving system automation. In addition, external information affects, directly or indirectly, the control decisions of the power system. To better understand the interconnected complex CPPS network, a multi-dimensional heterogeneous system similar to [6] can be utilized, the framework for which is shown in Fig. 1.

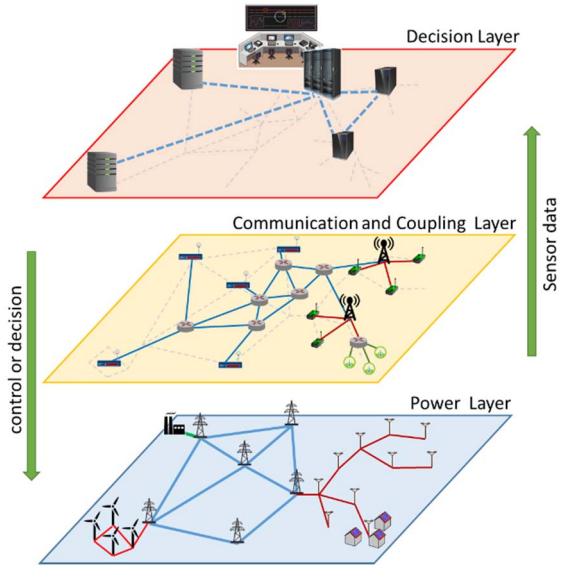

Fig. 1: Framework for cyber-physical power system

The CPPS-based analysis focuses on whether decision-making functions are performed to enhance the performance of the power system. For better understanding the interaction, three heterogeneous layers are utilized. The middle layer, consisting of the communication network, sensors and actuators bridges the decision-making (control) functions (top layer) and the physical power systems (bottom layer). The operational decision functions (EMS, protection, stability control, AGC/AVC, etc.) are included in the model through the top decision layer. The following subsections provide details for each layer:

A. *Power (Physical) Layer*

The power layer, which consists of all physical devices (e.g., generators, power lines, transformers, circuit breakers, power electronic devices, energy storage, loads, smart appliances, etc.), is connected to the communication and coupling layer through state awareness (sensors) and command execution devices. Conventional reliability modeling techniques can be used to model reliability of the power layer.

B. *Communication and Coupling Layer*

The communication and coupling layer is composed of interface devices (e.g., remote terminal units-RTU) and a communication network. The measurement from the power layer and the control command to the power layer are both carried by interface devices. The decision-making functions in the decision layer are also carried by these devices. The communication network, which connects the interface devices, consists of various communication devices and the links between them. The failure or malfunction of the interface devices and communication network will impact the accuracy of the decision-layer functions. Therefore, modeling the impact of communication and coupling layer is key for effectively operating a CPPS.

To illustrate the importance of the communication and coupling layer, synchro-phasor measurement units (PMUs) are considered as an example. PMUs, which are installed in selected buses [7] for providing related measurements, are used to monitor the entire power grid operation. By building on this infrastructure, potential smart grid applications, such as real-time stability management [8], can be facilitated [9]. To guarantee power system reliability, it is very important to maintain a certain degree of redundancy in terms of the placement of PMUs in order to address their random failures. For example, a primary and backup (P&B) method proposed in [9] involves two independent sets of PMUs, both of which can provide full observability of the entire power grid. In order to ensure that PMU data is useful, it is also important to improve the freshness of acquired data; thus, a stringent latency (time delay) requirement is involved. Delay in the arrival of measurements could result in lowering the value of data and potentially impact grid performance. However, time delay cannot be avoided in practical communication systems, including both wireless and wired systems [11]. In addition to the component failure, the delay in data arrival beyond the threshold and data loss should be considered as data unavailability for reliability modeling purposes.

Another illustrative example is the supervisory control and data acquisition (SCADA) system, which relies on information and communication systems [12]. SCADA interface modules can be treated as part of the communication and coupling layer for reliability modeling, with similar issues in terms of failure and data unavailability.

C. *Decision Layer*

The decision layer contains a variety of functions (e.g., renewable generation control, energy management system, demand management, etc.), which are desired for seamless operation of a power system. Estimated conditions of operating states from real-time measurements are used for this purpose [13]. Failure of the decision tools, including servers, will affect power system reliability.

Furthermore, the modernization of the grid involves automation via a communication infrastructure. An attacker

with malicious intention may launch cyber-attacks by hacking a few sensors and distort the measurements. Moreover, communication links are vulnerable to false data-injection attacks, where measurements may be altered during data transmission [14]. This could lead to incorrect decisions that can cause major malfunctions or even a blackout. It is important to model the malicious data injection into the network and ensure that it is not utilized in decision processes [15].

In addition to failure of the decision equipment, correctness of the decision can also affect power system reliability. The effect of cyber intrusion on power system decisions must be considered as a decision error for reliability modeling purposes.

Based on the discussion about each CPPS layer, reliability modeling for the heterogeneous framework could be modeled as shown in Fig. 2. This state transition diagram shows the different possible states of each layer. It should be noted that the power system is a combination of these three layers. Therefore, a detailed modeling is needed to include all possible states. This kind of modeling can be done at the component level or at the system level.

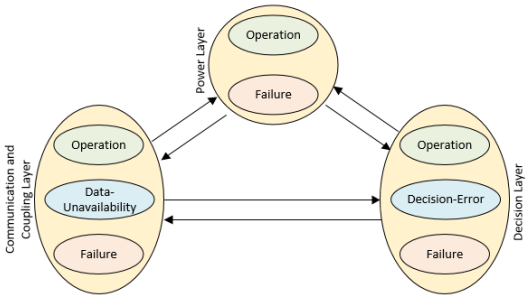

Fig. 2: Framework for cyber-physical power system reliablity modeling

III. Cyber Unavailability vs. Vulnerability

A. *Cyber Unavailability*

Communication may undergo a forced outage, even if the communication and coupling layer components are operating. This could occur for several reasons, including signal attenuation, loss of communication packet, time delay in communication packets, or jitter. Fig. 3 shows such forced outages for four different PMUs at different times in a day during a four-minute window from a U.S. utility [16].

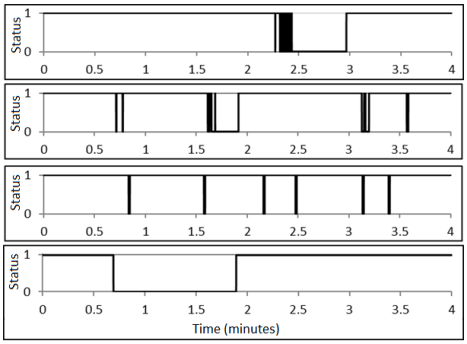

Fig. 3: Data unavailablity from different PMU units

From Fig. 3, it can be seen that the forced outage duration is typically shorter than a power equipment failure. However, the frequency of occurrence is relatively very high. Based on PMU data from 261 units for a 13-month period, the average rates are provided in Table 1.

TABLE 1: MISSING DATA STATISTICS

Data Availability	0.96
Missing Data Rate	3.22 failures per day
Recovery Rate	0.36 second

Based on this data, the frequency of missing data is very high compared to the power component failure. One of the challenges here is that the missing data rate does not follow an exponential distribution. It is important to further investigate and develop appropriate data unavailability model. Fig. 4 shows the missing data rate for certain PMUs.

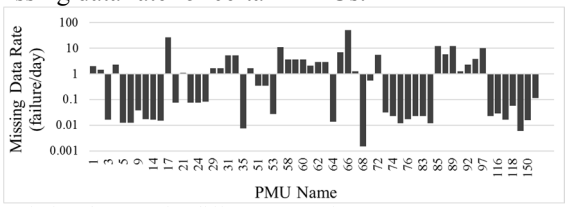

Fig. 4: Missing data rate for different PMUs in system

Furthermore, even for a single PMU, the missing data rate is not constant as shown in Fig. 5.

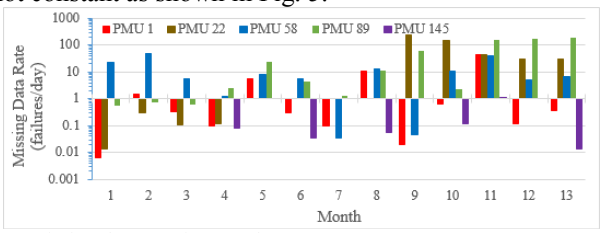

Fig. 5: Missing data rate for sample PMUs

Since the missing data rate is not consistent with different PMUs, it is critical to further analyze the data outage and develop more reasonable models for CPPS reliability analyses.

B. *CyberAttack Modeling*

Malicious intrusion into the cyber infrastructure has the ability to affect control decisions in power systems. Cyber intrusion could occur through either communication and coupling layer or the decision layer. However, for the purpose of efficient reliability modeling, the cyber intrusion needs to be modeled as a part of the decision error.

Cyber-attacks can be classified as follows:

- Availability: An attack may impact data availability by interfering with the original source or its transmission, for example, due to loss of communication (which includes detected data corruption).
- Integrity: Attacks to data integrity are those that could result in undetected modification and insertion of data. This could cause anything from data corruption to remote control of breakers.
- Confidentiality: Data confidentiality is compromised when data are accessed without permission. This usually has no direct impact on power system performance, but the threat to long-term performance is substantial. This includes reconnaissance attacks, which observe weak points in the cyber infrastructure, or attempts to intercept passwords and encryption keys. Also, leaks of privacy-sensitive material may result in severe regulatory consequences.

The models for cyber security (malicious attacks initiated on the cyber infrastructure) are presented in [17]. The most

common analytical method applied to cyber security threat models is the concept of the attack tree [18]. Attack trees work backwards from a goal that the attacker wishes to achieve, by identifying steps that lead to that goal. By assigning probabilities to the rate or probability of initial threats and the transitions, an attack graph is constructed, which can be analyzed numerically.

The threat of an intelligent attacker makes it difficult to deduce which specific threats are imposed to a model. It is also difficult to assign probabilities to the successful exploitation of vulnerabilities. As a result, risk modeling is often done using a high-level conceptual model such as the ISO/IEC Common Criteria standard. Recently, the domain-specific modelling language CySeMol [19] was developed as an alternative that allows better expression of causal relations and the likelihood of transitioning between attack steps.

CPPS constitute both discrete and continuous control and operational decisions, which are best captured by a hybrid control model [20]. Hybrid control models capture the normal operation of power systems, which can be used to detect attacks or anomalies on the system [20], [20].

An analytical framework using a generalized stochastic Petri net model is proposed in [22] to quantify vulnerabilities of the SCADA system for cyber security investigations. It systematically evaluates the SCADA vulnerabilities at three levels: system, scenarios, and access points. Then vulnerabilities are computed using the steady-state probabilities that the SCADA system is attacked through specific access points and the impact factors.

A modified semi-Markov process is used in [23] to model cyber-attacks against a substation. The success probabilities and mean time to compromise are calculated using the Colonel Blotto game [23]. Bayesian attack graphs are used in [24] to model attack procedures and quantitatively evaluate the probabilities and average frequencies of successful attacks.

IV. Cyber-Power Reliability Modeling

A Single failure in the communication and coupling layer or the decision layer could affect multiple devices in the power layer. Therefore, it is critical to model the sequence of consequences from events in the communication and coupling layer or the decision layer to power system layer failures.

Steps in the reliability computation process should include:

i. Model the communication and coupling or decision layer event propagation using section III.
ii. Develop an interdependency framework for the impact of communication and coupling layer or decision layer events on power system components (a transition from a sequence of cyber events to power layer events)
iii. Using the interdependency framework, determine the power system reliability matrices.

The following sections describe the modeling of parts ii and iii:

A. Cyber-Power Interdependacy Modeling

Because of the dimensionality and complexity, it is difficult to directly incorporate cyber components into the power grid reliability evaluation. A methodology that decouples the analysis of the cyber part from the physical part with the use of a cyber-physical interface matrix (CPIM) has been proposed in [25]. The CPIM can be described as follows.

$$CPIM = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,1} & p_{m,2} & \cdots & p_{m,n} \end{bmatrix}$$

where, rows represent the various initiating contingencies (in the physical system), and the columns correspond to the final outcomes, once possible cyber-failures have been taken into account. Elements of the matrix are therefore conditional probabilities of physical outcomes, given a specific initiating event. As a result, the probabilities in each row must add up to 1. With this methodology, reliability analysis is first performed at the substation level to evaluate cyber failures and their impact on the physical system. Such impact is summarized as probabilities in the CPIM. The cyber components do not directly appear in the matrix. The matrix summarizes the probability of possible causes and outcomes.

The resulting CPIM is utilized in the transmission system-level reliability evaluation without the need to consider cyber configuration details. In practical applications, another matrix called the consequent event matrix (CEM) is used to identify the specific physical components affected in each event. An implementation on the extended Roy Billinton Test System (RBTS) has been presented in [26]. The results clearly show the impact of cyber failures on power grid reliability. Studies in [25] and [26] mainly focus on the aspect of protection because protection hidden failures are common causes of cascading outages [27], [28]. A similar conditional probability matrix was used in [29] to model the effects of failures in generation rejection schemes, and to determine their impact on optimal system operation.

B. Component-Level Modeling

Component-level modeling requires a better understanding of the cyber power interaction. A general framework for cyber power interaction has been developed in [26] using the concept of smart components. Here, the power layer and the communication and coupling layer are combined to develop the smart component. In the work presented in [26], the decision layer is included with the communication and coupling layer. The electrical equipment could be in four states (normal, failed, preventive, and maintenance), and the communication layer has three states (normal, failed, unavailable). Markov model for the smart component with state transition rates is shown in Fig. 5.

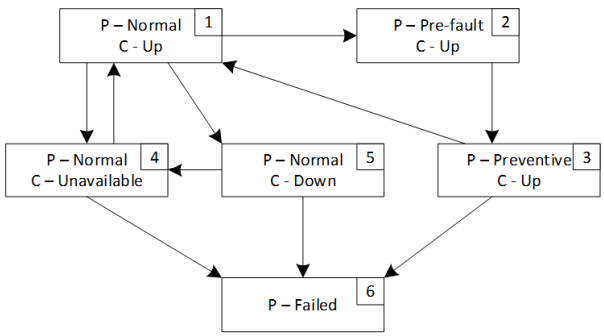

Fig. 5: State model for smart components [30]

This model needs to be further enhanced to incorporate the cyber unavailability and cyber-attack to better represent the communication and coupling layer and the decision layer. One of the challenges of the CPPS state model is the higher number of possible states. Once the state model is developed, it is necessary to develop reduced state models for computational effectiveness. Due to the dissimilarity in the operation of the smart components, a single framework will not be sufficient. For example, the communication and coupling layer and the decision layer have a dissimilar impact on a device used for health monitoring compared to real-time measurements.

C. System-Level Modeling

Enhanced component models demand improved CPPS reliability modeling and analysis. Two approaches are proposed in the literature.

The *first approach* is to use a combined state-space model for each component and then evaluate the power system reliability [31]. Several communication and coupling layer devices could fail for the same reason. The work presented in [31] uses common-cause failure (CCF) based probabilistic reliability assessment. Two main factors are required for a CCF to occur: a root cause and a coupling factor that makes multiple components susceptible to the same cause. The set of equipment affected by a single cause is known as the common cause component group [31]. A probabilistic method similar to the alpha factor model [32] can be used to determine simultaneous failure probability of an equipment. A four-step approach to determine a component failure rate with basic event probability of occurrence is presented in [31]. This method needs to be further improved for the large system analysis.

The CCF power system reliability analysis requires the following considerations: (*i*) the probability of a large number of components failing for a single cause is low, and (*ii*) when an event occurs in the power system, the component close to the event will act first, and if it fails, then the adjacent components will react

In the case where exact power system reliability is impossible to determine, the worst-case reliability can be computed [33]. Minimal cut sets for data transmission from one node to another can be computed. In order to reduce the complexity, the worst-case probability can be determined by placing all minimal cut sets in a series [33]. This method is very useful for very large networks.

The *second approach* uses the characteristic matrix method. Similar to [25], the characteristic matrix for both the communication and coupling layer and the decision layer can be modeled. For the communication and coupling layer, element (*i*,*j*) of the interface matrix corresponds to the performance of cyber-link between nodes *i* and *j* and given by

$$C = \begin{array}{c} \\ 1 \\ \vdots \\ i \\ \vdots \\ m \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & \cdots & j & \cdots & m \end{array} \\ \begin{bmatrix} C_{11} & \cdots & C_{1j} & \cdots & C_{1m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ C_{i1} & \cdots & C_{ij} & \cdots & C_{im} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ C_{m1} & \cdots & C_{mj} & \cdots & C_{mm} \end{bmatrix} \end{array}$$

The diagonal elements in *C* correspond to the performance of the node. Each element is comprised as $c_{ij} = (T, P_a, P_m)$, where T is the time delay, P_a is the interruption probability, and P_m is the disruption probability. The decision-layer interface matrix will be represented by *S*. Each element comprises S = (*T*, *P*), where *T* is the delay, and *P* is the decision error probability. Similar to the communication and coupling layer, the diagonal elements correspond to the device performance. If there are no connections, then all elements are zeros (c_{ij} = (0, 0, 0) or S_{ij} = (0, 0)). Similarly, the interaction between layers can be modeled using the interface matrix, which can be used for reliability computation.

V. Enhancing Reliability Standards

Power system reliability modeling requires a modification to its standardization due to the complexity of CPPS. The enhancement to monitoring, control, and protection through CPPS changes the means of failure and recovery of power system components. Both bulk and distribution system reliability modelling must be changed.

A. Bulk Industry Standards

The planning and operation of bulk power systems have been traditionally driven by reliability criteria and standards (NERC standards, regional reliability criteria) [34]. The North American Electric Reliability Corporation has developed mandatory and enforceable standards for planning (e.g., TPL-001-4) and operation (e.g., TOP-002-4, IRO-017-1) to ensure reliable operation of the power grid. Critical infrastructure protection (CIP) standards (e.g., CIP-002-5), which deal with the cyber side of the power system, are mandatory and enforceable [34].

Developed methodologies and tools to assess system performance have served the industry very well in the past [35]-[37]. However, it is becoming more apparent that reliable operation of the power system is highly dependent on the reliability of the associated cyber system, and failure in the cyber system can result in undesirable consequences. New reliability tools for joint modeling and performing the reliability analysis by taking into account the performance of "cyber" and "physical" elements are needed. Contingencies on the cyber side may lead to inappropriate control commands, which will influence the physical power system.

B. CPPS Standadization Approach

In addition to the power system failure and recovery measures, it is vital to determine the direct effects of the CPPS on power system operations. Some of the measures that could quantify the direct effect of CPPS on the power system are identified in the literature [1], [38]–[39]. Some examples are presented as follows.

The effect of the cyber infrastructure on power system reliability can be modeled similar to IEEE Std. 1366 [40] based on the following indices proposed by [1]:

- *Average Cyber Failure Frequency Index:* The number of missed decisions on the power layer due to failure of the communication and coupling layer and the decision layer as a fraction of the total decision:

$$ACIFI = \frac{\text{Total missed decsions}}{\text{Total decisions in a unit time}}$$

- *Energy Not Served due to Cyber Failure:* The amount of energy not served due to failure of the communication and coupling layer and the decision layer as a fraction of the total energy not served at the same time:

$$ENS_C = \frac{\text{Total energy not served due to missed decisions}}{\text{Total energy not served in a unit time}}$$

On the other hand, indices for specific applications should be developed. For example, when the power system operations are managed via the CPPS, transient stability of the system could be detected via the measurements. The ability to detect the transient stability against faults is developed in [38] as part of the power system reliability evaluation.

- *Expected Transient Instability Index*: The measure for the probability of the system being in an unstable state:

$$ETI = \sum_{i=1}^{n_u} p\{x_{i-1,i}: x_{i-1,i} \in X_u\}$$

where $p\{x_{i-1,i}: x_{i-1,i} \in X_u\}$ is the probability of the system being unstable while transitioning from state $x_{i-1,i}$ to state x_i, x_i is the system new state, X_u is the set of unstable transitions ($X_u \subset X$), X is the set of all system states, and n_u is the number of unstable transitions.

- *Expected Transient Stability Robustness Index*: The measure of the ability of a system to withstand the following fault events:

$$ETSR = \sum_{i=1}^{n_{st}} p\{x_{i-1,i}: x_{i-1,i} \in X_{st}\}.EM\{x_{i-1,i}: x_{i-1,i} \in X_{st}\}$$

where $p\{x_{i-1,i}: x_{i-1,i} \in X_{st}\}$ is the probability of the system being stable while transitioning from state $x_{i-1,i}$ to state x_i, $EM\{x_{i-1,i}: x_{i-1,i} \in X_{st}\}$ is the energy margin of a stable transition from state $x_{i-1,i}$ to state x_i, X_{st} is the set of stable transitions ($X_{st} \subset X$), and n_{st} is the number of stable transitions.

- *Expected System Risk of Instability Index*: The measure of the risk of a system being unstable against fault events:

$$ESRI = \sum_{i=1}^{n_u} p\{x_{i-1,i}: x_{i-1,i} \in X_u\}.\left|EM\{x_{i-1,i}: x_{i-1,i} \in X_u\}\right|$$

where $\left|EM\{x_{i-1,i}: x_{i-1,i} \in X_u\}\right|$ is the energy margin of an unstable transition from state $x_{i-1,i}$ to state x_i.

VI. Future Needs

Cyber-physical interdependencies exist extensively in various aspects of the power grid. To further enhance existing reliability evaluation models and methodologies, considerable research effort and input from both academia and industry are needed.

Two challenges for improved reliability analysis of the CPPS are as follows: (i) test systems that allow standardization of results and (ii) simulation tools that address the needs of modeling CPPS interactions.

A. Test Systems

The IEEE Reliability Test System [41] and the Roy Billinton Test System [42] are used for modeling and analysis of power system reliability. However, due to the lack of appropriate failure models for cyber- and decision-layer equipment, the authors use customized models, which limit the ability to compare the CPPS reliability framework. The following need to be incorporated into the test systems:

- Possible states for communication and coupling-layer equipment,
- Possible states for decision-layer equipment,
- State transition rates for new states from communication and coupling layer and also the decision layer,
- Cyber-physical interface matrix model.

B. Simulation Tool

Software developed for the power system domain is rarely flexible enough to enable customization using complex modules. A notable exception for distribution system analysis is the open-source package GridLAB-D [43]. Since this is an open-source software, the reliability analysis component could be incorporated. Simulation tools should allow users to incorporate possible communication architecture and decision schemes because they are critical for effective reliability calculations. Two separate models for an interconnected transmission system and possible extension to a software tool, such as GE MARS, are necessary. Similarly, the second model should focus on the distribution system reliability computation.

It is vital that the simulation tools should be able to model seven layer OSI communication model, associated vulnerabilities, and possible defense mechanism including different possible communication and data exchange protocols.

C. CPPS Resiliency

In extreme events, it is not possible to keep up the reliability of power grids and the emphasis changes to enhance the grid resiliency. Keeping the power on to critical facilities such as hospitals and fire department during extreme events is essential and, additionally, the ability of the system to supply power to the critical loads can be defined as resiliency.

It is important to analyze the impact of possible cyber-attacks on the power grid and develop defense mechanisms. Cyber-physical resiliency analysis needs to be performed to minimize the impact of the potential cyber-attacks on the grid.

Similar to CPPS reliability, there is a need for formal metrics to quantify resiliency of the CPPS and a tool to study the cyber-physical resiliency.

VII. Conclusion

This paper summarizes the current status and needs for cyber-physical power systems reliability evaluation. It is essential to standardize the CPPS modeling for reliability computation based on three layers: power layer, communication and coupling layer, and decision layer. The possible states of each model and the interaction between layers can to be captured using an interface matrix, for example. It is also vital to develop test systems and simulation platforms to enhance future CPPS reliability studies to benefit the industry.

References

[1] V. Aravinthan, B. Karimi, V. Namboodiri, and W. Jewell, "Wireless Communication for Smart Grid Applications at Distribution Level—

Feasibility and Requirements," in *Proc. IEEE PES General Meeting*, July 2011.

[2] E. Bompard, T. Huang, Y. Wu, and M. Cremenescu, "Classification and Trend Analysis of Threats Origins to the Security of Power Systems," *Int. J. Electr. Power Energy Syst*., vol. 50, pp. 50-64, 2013.

[3] K. R. Davis, et. al., "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464-2475, May 2015.

[4] R. Billinton and S. Jonnavithula, "A Test System for Overall Power System Reliability Assessment," *IEEE Trans. Power Systems*, vol. 11, no. 4, Nov. 1996.

[5] G. H. Kjølle and O. Gjerde, "Vulnerability Analysis Related to Extraordinary Events in Power Systems," in *Proc.PowerTech 2015*, Eindhoven, 2015.

[6] Y. Xue, M. Li, J. Luo, M, Ni "Coupling Modeling Method for Cyber Physical Power Systems Based on Correlation Characteristic Matrix," Journal of Automation of Electric Power Systems, vol. 42, No. 2, 2018.

[7] K. G. Khajeh, E. Bashar, A. M. Rad, and G. B. Gharehpetian, "Integrated Model Considering Effects of Zero Injection Buses and Conventional Measurements on Optimal PMU Placement," *IEEE Trans.Smart Grid,* vol. 8, no. 2, pp. 1006–1013, March 2017.

[8] C. D. Vournas, C. Lambrou, and P. Mandoulidis, "Voltage Stability Monitoring from a Transmission Bus PMU," *IEEE Trans. Power Systems*, vol. 32, no. 4, pp. 3266-3274, July 2017.

[9] A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications*, vol. 1, Springer, 2008.

[10] X. Bei, Y. J. Yoon, and A. Abur, "Optimal Placement and Utilization of Phasor Measurements for State Estimation," in *Proc. 15th Power systems Computation Conference*, Liege, Belgium, August 22-26, 2005.

[11] M. You and H. Sun, "Realising Energy-Aware Communication over Fading Channels under QoS Constraints," in *Proc. IEEE International Conference on Ubiquitous Wireless Broadband*, China, Oct. 2016.

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012.

[13] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis," *IEEE Systems Journal*, vol. 10, no. 2, pp. 532-543, June 2016,.

[14] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids," *IEEE Trans. Industrial Informatics*, vol. 11, no. 5, pp. 1198-1209, Oct. 2015.

[15] J. Jiang and Y. Qian, "Defense Mechanisms against Data Injection Attacks in Smart Grid Networks," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 76-82, Oct. 2017.

[16] A. C. S. Hettiarachchige-Don and V. Aravinthan, "Estimation of Missing Transmission Line Reactance Data Using Multiple Linear Regression," in *Proc. 2017 North American Power Symposium (NAPS)*, WV, 2017

[17] CIGRE Working Group D2.31, "Security Architecture Principles for Digital Systems in Electric Power Utilities," , 615: 2015

[18] K. R. Davis, et. al "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464-2475, Sept. 2015.

[19] CySeMol, available online at https://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/cc/cysemol/description-1.432380 (accessed September 6, 2015).

[20] M. Parvania, et. al. "Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems," in *Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 23, 2014.

[21] G. Koutsandria, et. al. "A Hybrid Network IDS for Protective Digital Relays in the Power Transmission Grid," in *Proc. 5th IEEE International Conference on Smart Grid Communications*, Nov. 3-6, 2014.

[22] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Trans. Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[23] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Trans. Power Systems*, vol. 31, no. 6, pp. 4379-4394, Nov. 2016.

[24] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations," *IEEE Trans.Smart Grid*, vol. 6, no. 4, pp. 1707-1721, July 2015.

[25] H. Lei, C. Singh, and A. Sprintson, "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194-2202, Sept. 2014.

[26] H. Lei and C. Singh, "Power System Reliability Evaluation Considering Cyber-Malfunctions in Substations," *Electric Power Systems Research*, vol. 129, pp. 160-169, Dec. 2015.

[27] D. C. Elizondo, J. De La Ree, A. G. Phadke, and S. Horowitz, "Hidden Failures in Protection Systems and Their Impact on Wide-Area Disturbances," in *Proc. IEEE Power Engineering Society Winter Meeting*, vol. 2, January/February 2001, pp. 710–714.

[28] H. Lei and C. Singh, "Incorporating Protection Systems into Composite Power System Reliability Assessment,"in *Proc. IEEE Power and Energy Society General Meeting*, July 26-30, 2015, pp. 1-5

[29] J.Calvo, S.Tindemans and G. Strbac, "Incorporating Failures of System Protection Schemes into Power System Operation," Elsevier Sustainable Energy, Grids and Networks, Vol. 8 Dec. 2016

[30] M. Heidari-Kapourchali and V. Aravinthan, "Component Reliability Evaluation in the Presence of Smart Monitoring," in *Proc. 2013 North American Power Symposium (NAPS)*, Manhattan, KS, 2013, pp. 1-6.

[31] M. Heidari Kapourchali, M. Sepehry, and V. Aravinthan, "Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network," *IEEE Trans. Smart Grid*, available as early acess article.

[32] A. Mosleh, D. M. Rasmuson, and F.M. Marshall, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," INEEL/EXT-97-01327, 1998.

[33] S. Chakraborty, T. Balachandran, and V. Aravinthan, "Worst-Case Reliability Modeling and Evaluation in Cyber-Enabled Power Distribution Systems," in *Proc. 2017 North American Power Symposium (NAPS)*, Morgantown, WV, 2017, pp. 1-6.

[34] North American Electric Reliability Corporation, "Reliability Standards for the Bulk Electric Systems of North America," June 2011, available online at http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

[35] M. Papic and O. Ciniglio, "Prediction and Prevention of Cascading Outages in Idaho Power Network," in *Proc. IEEE PES General Meeting*, July 2014.

[36] M. Papic, O. Ciniglio, and M. Vaiman, "Practical Experience in Assessing the Effects of Extreme Contingencies with Respect to Standards TPL-001-4 and CIP-014-1," in *Proc.IEEE PES General Meeting*, July 2015.

[37] M. Papic and O. Ciniglio, "Prevention of NERC C3 Category Outages in Idaho Power's Network: Risk-Based Methodology and Practical Application," in *Proc.IEEE PES General Meeting*, July 2013.

[38] M. Benidris, J. Mitra, and C. Singh, "Integrated Evaluation of Reliability and Stability of Power Systems," *IEEE Trans. Power Systems*, vol. 32, no. 5, pp. 4131-4139, Sept. 2017.

[39] S. Wang, Z. Li, L. Wu, M. Shahidehpour, and Z. Li, "New Metrics for Assessing the Reliability and Economics of Microgrids in Distribution System," *IEEE Trans. Power Systems*, vol. 28, no. 3, pp. 2852-2861, Aug. 2013.

[40] IEEE Std. 1366-2003, Guide for Electric Power Distribution Reliability Indices.

[41] C. Grigg et. al. "The IEEE Reliability Test System-1996. A Report Prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Trans. Power Systems*, vol. 14, no. 3, pp. 1010-1020, Aug. 1999.

[42] R. Billinton and S. Jonnavithula, "A Test System for Teaching Overall Power System Reliability Assessment," *IEEE Trans. Power Systems*, vol. 11, no. 4, pp. 1670-1676, Nov. 1996.

[43] D. P. Chassin, J. C. Fuller, and N. Djilali, "GridLAB-D: An Agent-Based Simulation Framework for Smart Grids," *Journal of Applied Mathematics*, vol. 12,