Cyber-Physical Power System Layers: Classification, Characterization, and Interactions

Michael Abdelmalak
Electrical & Biomedical Eng.
University of Nevada-Reno
Reno, NV, USA
mabdelmalak@nevada.unr.edu

Narayan Bhusal
Electrical & Biomedical Eng.
University of Nevada-Reno
Reno, NV, USA
bhusalnarayan62@unr.edu

Mukesh Gautam
Electrical & Biomedical Eng.
University of Nevada-Reno
Reno, NV, USA
mukesh.gautam@unr.edu

Mohammed Benidris
Electrical & Biomedical Eng.
University of Nevada-Reno
Reno, NV, USA
mbenidris@unr.edu

2023 IEEE Texas Power and Energy Conference (TPEC) | 978-1-6654-9071-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/TPEC56611.2023.10078602

***Abstract*—This paper provides a strategy to identify layers and sub-layers of cyber-physical power systems (CPPS) and characterize their inter- and intra-actions. The physical layer usually consists of the power grid and protection devices whereas the cyber layer consists of communication, and computation and control components. Combining components of the cyber layer in one layer complicates the process of modeling intra-actions because each component has different failure modes. On the other hand, dividing the cyber layers into a large number of sub-layers may unnecessarily increase the number of system states and increase the computational burden. In this paper, we classify system layers based on their common, coupled, and shared functions. Also, interactions between the classified layers are identified, characterized, and clustered based on their impact on the system. Furthermore, based on the overall function of each layer and types of its components, intra-actions within layers are characterized. The strategies developed in this paper for comprehensive classification of system layers and characterization of their inter- and intra-actions contribute toward the goal of accurate and detailed modeling of state transition and failure and attack propagation in CPPS, which can be used for various reliability assessment studies.**

***Index Terms*—Cyber-Physical Power Systems, Resilience, real-time simulation.**

I. Introduction

The advancements in communication and automation technologies have increased significantly in the last decade resulting in widespread integration and deployment in power systems. Grid modernization approaches created what is now known to be cyber-physical power systems (CPPSs). Such systems are composed mainly of cyber layer, i.e., communication and control systems, and physical layer referring to the power system. Despite the noticeable added benefits of cyber layer on power systems achieving reliable, secured, and economic operation, increased vulnerabilities against cyber threats and attacks are always being associated with the level of integration. Also, the reliance to leverage user-friendly human interface platforms, cloud computation, and smart artificial-intelligence devices create further complexities to analyses of CPPSs. Therefore, it has become a necessity to accurately model the state transitions and propagation behaviors in CPPSs for improved evaluation and enhancement of their resilience and performance.

Recently published research in [1]–[3], provides a comprehensive review of CPPSs from the perspective of modeling, simulation, and analysis with cyber security applications. This paper also provides literature survey on cyber attacks and cybersecurity measures for CPPSs. This work describes the CPPS as the coupled network of cyber and physical systems. Cyber layer consists of computation, communication, and control systems. Physical system, on the other hand, consists of a physical power grid governed by physics-based rules. In [4], key features of cyber-physical systems in multi-layered architecture are conceptualized. This work characterizes the cyber physical system into physical layer, cyber-physical layer, and the cyber layer. Physical layer consists of physical components and their dynamics, physical measurements, and physical operators. Cyber-physical layer includes programmable controllers, real-time communication networks, sensors, and actuators. Cyber layer is formed by a combination of cyber communication networks, supervisory computers, and supervisors.

Cyber layer can be identified as the layer responsible for the computation, analysis, and assessment of the power system on the regional and global scale. Defining the boundaries of a cyber layer within a CPPS model is not a straightforward process. First, the advancements in information and communication technology have resulted in embedded smart computation processors in all power system components. This raises a concern whether such computation parts are system or component involved. Also, some system computational tasks take place at the local level such as protection decisions; whereas other wide-area analyses are handled in the energy management systems [5]. This raises a concern whether the cyber layer is composed of a single layer or can be split into several layers. The cyber layer comprises all required applications to maintain reliable and economical operation of the power system. Some of these applications are run in the local level prior to passing to global level such as automatic generation control, remedial action schemes, and protection protocols. Other global applications include but are not limited to state estimation, real-time contingency analysis, security constrained optimal power flow, unit commitment, and energy market optimization. Determining the proper input data into diverse applications causes a confusion on boundaries of the cyber layer.

Whereas the power grid represents only a physics-governed

978-1-6654-9071-9/23/$31.00 ©2023 IEEE

physical layer, the cyber layer consists of several layers such as sensor, protection, communication, computation, and control layers. Combining the components of the cyber layers in one layer complicates the process of modeling intra-actions because each component has different failure modes. On the other hand, dividing the cyber layers into a large number of sub-layers may unnecessarily increase the number of system states and increase the computational burden. Therefore, rigorously identifying system heterogeneous layers (cyber and physical) and comprehensively characterizing their inter- and intra-actions are essential to (1) establish accurate models for state transitions; (2) identify chains of failure propagation within and between layers; and (3) develop efficient and practical reliability and resilience analysis, evaluation, and enhancement methods and strategies for CPPSs. Further research is inevitable for the maturity of CPPS classification, characterization, and modeling, simulation, and analysis of interactions between and within the CPPS layers.

This paper establishes strategies to identify CPPS layers and sublayers and characterizes their inter- and intra-actions. In this paper, CPPS layers are classified based on their common, coupled, and shared functions. During classification, we start with common intended functions, of which there are many, each of which aggregates several system components. Then, we identify coupling layers (i.e., failure of coupling layers separates two or more layers) such as the communication layer, which couples the heterogeneous physical layer and remaining layers. Next, we identify shared layers such as the sensors' layer—a shared layer between the communication and protection layers. Also, interactions between the classified layers are identified and characterized; possible interactions are discussed and clustered based on their impacts on the system. Furthermore, intra-actions within each layer are characterized based on the overall function of the layer and types of its components. The strategies developed in this paper for comprehensive classification of system layers and characterization of their inter- and intra-actions contribute toward the goal of accurate and detailed modeling of state transitions and failure and attack propagation in CPPS. This is a necessary step toward developing analysis, evaluation, and enhancement methods for CPPS reliability and resilience.

The rest of the paper is structured as follows. Section II provides a survey on existing approaches of classification, characterization, and interaction of cyber-physical layers, and criteria of CPPS modeling. Section III describes the suggested classification, characterization, and interactions between CPPS layers. Section IV provides the concluding remarks.

II. Modeling of Cyber-Physical Power Systems

Modeling of cyber-physical systems across various domains has gained significant interest in the last decade. This includes, but not limited to, biomedical systems, transportation systems, and energy systems [6], [7]. Proper models of CPPSs are necessary for accurate, reliable, and efficient analysis and assessment [8]–[10]. This section summarizes the most recent modeling approaches of CPPSs and the associated dependencies across the model layers. Also, it presents few criteria to measure the capabilities of these models within the Cyber-Physical domain.

A. Existing CPPS Models

The layer classification of the CPPS model varies in the existing literature based on the study or the system. In [11], [12], a two-layer CPPS model has been provided to assess the transient power system stability against control and communication failures. The first layer represents the power grid system, whereas the second refers to the cyber layer. Another two-layer CPPS model has been provided in [13], where the cyber layer is represented by three sub-layers including measurements, protection, and control. Authors of [5] have restructured the CPPS model in [13] to include an intermediate layer between the cyber and physical layers. The connecting layer handles three main applications, wide-area monitoring, protection, and control. The function of the intermediate layer has been changed in [14] to represent only the communication between the physical layer and the cyber layer. A comprehensive four layers CPPS model has been provided in [15] representing physical, communication, control, and monitoring layers.

Fig. 1 represents a three-layer CPPS model in [16]. The bottom layer represents the physical power system; the intermediate layer refers to the coupling communication layer; and the top layer is the decision control layer. The measurement layer is assumed fully reliable, whereas the protection layer is ignored. The mathematical computations are integrated within the control layer. It is worth noting that this model captures only the states and interactions of three main layers neglecting the inter-actions within each layer.

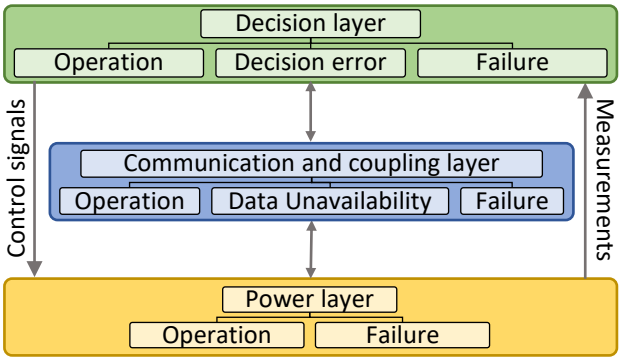

Fig. 1. CPPS model in [16]

A more detailed CPPS model has been developed in [17], [18], as shown in Fig. 2. The model splits the cyber-physical smart grid into a hierarchical six layers including management layer, supervisory layer, network layer, communication layer, control layer, and physical layer. The presented model complies relatively with the NIST smart grid conceptual model [19]. The control layer includes sensors, actuators, and intrusion-detection devices. The communication layer is the connection medium between the control layer and

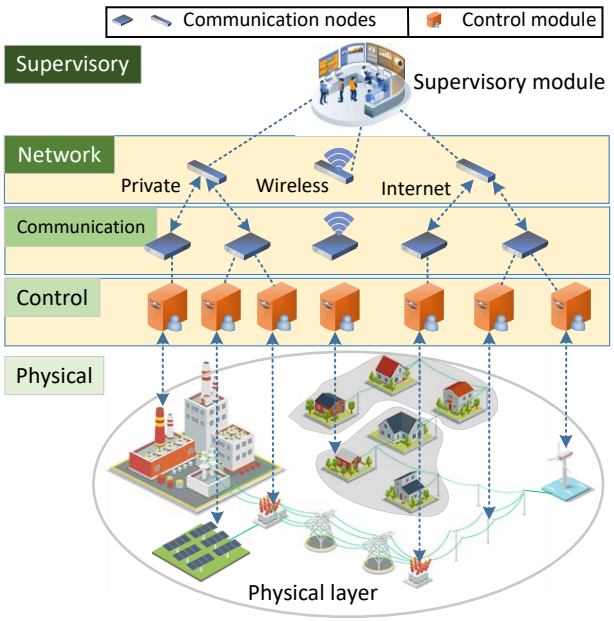

Fig. 2. Different CPPS layers with the control system [17] [18].

various network types. The data routing and network formation are handled in the network layer. The computational data analysis, performed in the supervisory layer, is passed to the management layer for proper decision making. Also, the management layer takes into account the energy market, regulatory policies, and system operation.

B. Dependencies in CPPS Layers

Several studies have been conducted to model dependencies among CPPS layers [20]. Graph theory, complex-network methods, finite state models, Petri net models, correlation methods, and cellular automate methods are some methods to model such dependencies [2]. Five mathematical models have been presented in [21] to analyze interdependencies of CPPS layers including dynamic analysis, topological analysis, consequence analysis, causal analysis, and hazard identification. A graphical network model has been integrated with a chaotic levy flight algorithm to assess the transition of a cyber-attack to a cascading failure scenario of power grids. To model the transition between power and cyber layers on the component level, a Markov state model has been presented in [22]. Authors of [23] have provided a Petri net model to capture the interdependencies between information layer and physical layer against malicious attacks. A correlation matrix approach has been introduced in [24] to study the propagation behavior of cyber-induced failures into power systems. The cyber-physical interface matrix can be calculated using the IEEE-61850 communication scheme and available failure rate of cyber-related components.

Various methods have been presented to classify dependencies in CPPS models. In [25], a classification based on the relationship between network and system elements has been introduced including both direct/indirect element-element and element-network models. Three levels of interactions have been introduced in [2] including computational-communication interactions, communication-physical interactions, and local physical-controller-protection interactions. A comprehensive guideline to model interactions between power system layer and ICT layers has been introduced in [21]. Such interactions are; (1) common cause, where the cause of failure in both systems is the same, e.g., whole substation shutdown, (2) cascading cause, where a failure in one layer propagates to another layer, e.g., power outage of communication systems, and (3) escalating cause, where an existing failure in one layer worsens an independent failure in another layer, e.g., failure in protection layer during a faulted power system. Authors of [23] have classified interdependencies between infrastructure layers into type of interdependencies, infrastructure environment, couplings among layers, infrastructure characteristics, state of operation, and type of failure.

C. Modeling Criteria

Though extensive research has been conducted in modeling CPPSs, only a few papers have given interest to evaluate the developed models. Selecting a particular model is a sophisticated process that requires highlighting the pros and cons of each model. Also, the compatibility of a CPPS model to a specific study or application plays a vital role in the decision process. A few main criteria are used to quantify CPPSs models including: (1) accuracy, (2) scalability, (3) fidelity, (4) application-compatibility, (5) dynamics-adaptability, and (6) topological-suitability. These metrics are explained as follows.

(1) Accuracy: Modeling accuracy refers to the capability of a model to reproduce experimental data that agrees with the physical phenomena precisely. In other words, this criterion measures the consistency of a model against varying scenarios and diverse input data. It is a necessity for CPPS models to maintain consistent outcomes under various constraints and diverse factors such as geographic locations and operating conditions.

(2) Scalability: The scalability feature refers to the capability of a model to adapt to large-scale systems and provide comprehensive representation of the system. Building a scalable CPPS model requires extensive caution with sophisticated conversion procedure, available computational capabilities, different modeling domain, diverse interoperability issues, and fast market technology.

(3) Fidelity: If the model outcomes match the results of real-world systems, then a CPPS model is said to maintain fidelity. In CPPS, high nonlinearity levels in the power system layer impose further complexities to achieve fidelity. Due to modeling approximations, a small discrepancy can be noticed between the CPPS model and the real-world system. Maintaining least discrepancies yields high fidelity models.

(4) Application-compatibility: The level of information and approximation of a particular model may change based

on the application or problem under study. For instance, reliability-based studies of power systems do not usually require dynamic system information. A CPPS model is said to maintain a high level of application-compatibility if it can be used across different types of studies with minimal modifications.

(5) Dynamics-adaptability: Power systems are characterized by high dynamics level. In various studies, it is required to capture the small-time variations in the system dynamics. This criterion aims to quantify the capability of a CPPS model to capture the dynamical behavior, particularly transient and subtransient changes in the power system.

(6) Topological-suitability: The NIST smart grid conceptual model describes future CPPSs in terms of seven main domains including customer, distribution, transmission, generation, market, service providers, and business services. A CPPSs model shall be capable of representing these domains, their distinctive features, and their dependencies. Due to the large-scale integration of distributed energy resources and increased number of local control centers, the system topology is changing from a centralized structure to a distributed structure. The topological-suitability criterion shows the degree of a CPPS model to represent the new meshed distributed system topology.

III. Suggested Model for CPPS

CPPS is the combination of various layers that interact together for a reliable operation of the power grids. The power grid is usually represented as a physical layer, whereas the cyber layer might consist of several layers such as measurement, protection, communication, computation, and control layers. Combining various components of the cyber layers in one layer results in improper modeling of dependencies among components and layers. Also, it complicates the process of modeling intra-actions because each component has different failure modes. On the other hand, dividing the cyber layers into numerous sub-layers may increase the computational complexity due to the large number of system states. Therefore, accurately classifying system layers such that the inter- and intra-actions between and within them while reducing the modeling complexity and computation burden has become important.

By taking the trade-off between the modeling accuracy and computational complexities into consideration, a five-layer CPPS model is identified. These layers are classified based on their common, coupled, and shared functions. The main layers are the physical grid, the global protection layer, the global communication layer, the computation layer, and the monitoring and decision layer as shown in Fig. 3. This architecture also consists of some local layers, for example, local protection, control, and communication layers that are not directly connected to the main monitoring and decision layer. Brief description of these layers is provided as follows.

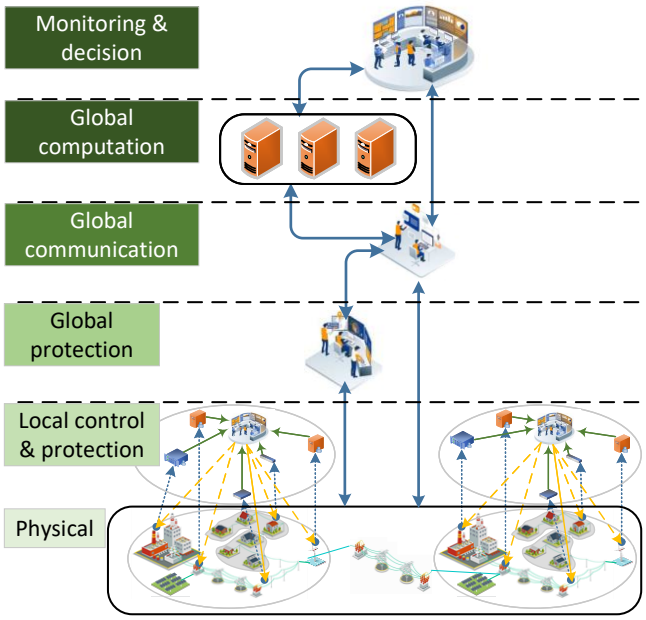

Fig. 3. Proposed CPPS layers.

A. Physical Power Grid Layer

Conventional power grid is the main building block upon which the concept of CPPS has advanced. This layer provides the detailed description of the power system model, its configuration, electrical characteristics, and topology [26]. This layer might include devices such as measurement devices and protection devices that are directly connected to power system components for proper operation and functioning of the system [16]. Each component in the physical layer has unique fundamental functions and electrical characteristics. The physical layer can be further sub-categorized based on type of components into power system components, protection components, and measurements components.

1) Power System Components

This part of CPPS describes the topology of power systems using single line diagrams. The power grid is categorized based on functionality into three main categories: generation, transmission, and distribution. In normal operation, generation level should be sufficient to supply load demands under consideration of all system operating constraints.

2) Protection Devices

The protection layer consists of all the protective devices that either prevent or reduce the impact of disturbances to operation devices. Protective devices such as relays are usually installed on various locations including power transmission lines, bus-bars, generators, transformers, and load nodes. Protective devices are equipped with sensors and act on the local level based on predefined settings that maintain the proper coordination between various relays [5]. For instance, a primary protection relay trips and isolates a faulted transmission line. Also, some components such as turbine-governor units connected to electric generators require very detailed local protection schemes to operate properly.

On the other hand, the global protection scheme focuses on the overall performance of the system without involvement of the local protection. It aims to detect abnormal system behavior, develop corrective actions, and respond in a quick and automatic way to prevent the propagation of a small disturbance to larger-scale events.

3) Measurement Components

Measurement devices are mainly responsible for observing the performance of power system components. Measurement devices can be classified into system (central) measurement and component (local) measurement devices. In the local level, measurements are passed to local controllers via spark communication links. For instance, generator units require an independent and massive measurement layer to monitor and maintain their performance, which could be mechanical, electrical or even physical measurements such as vibration sensors, rotor speed sensors, and magnetic field sensors. Global measurements, on the other hand, assess the performance of the power system as a whole. The transmission of global measurements heavily depends on two-way high-bandwidth communication technologies in order to access the information from the power grid and its components. These measurements are utilized to detect the propagation of a specific event to other components. For example, a faulted generator can be detected by measuring the variations in its reactive power flow [27].

B. Cyber Layer

A cyber layer can be identified as the layer that utilizes information and communication technology (ICT) and computer-aided platforms to gather, assess, and control the operation of power systems. It might be composed of communication channels, computation and control platforms, and monitoring systems.

1) Communication Channels

ICT is a vital connecting bond between measurements and various cyber layers. Interface devices such as RTUs provide a two-way function in CPPS which are: (1) to transfer measured data via the communication layer, and (2) to execute decision-making signals coming from the control layer. RTUs are installed in various locations to capture the observability of the system states [5]. Methods of communication between several components vary according to: system level, system scale, security constraint, priority, and hardware installation [14]. Both local and wide area network environments are accompanied with several communication protocols to provide the proper communication. High capacity fiber optic cables are being widely used to connect between substations and system control centers in the transmission level at high transfer speed [15].

2) Computation and Control platforms

This layer is responsible for providing the proper control actions based on various power system assessment tools. Generally, control centers receive the measurements from field devices and pass them to operational processes, a decision is made and transmitted to actuators that apply a state change in the field devices. Both local and global centers utilize supervisory control and SCADA systems to handle the various computation and control algorithms [5], [15], [28], [29]. Various monitoring screens are integrated to provide real-time information of the system components and status.

Each part of the power system has its own control algorithms, variables, and tools. In generation, terminal voltage and output power are the essential primary control algorithms. On the local level, generators have two control schemes: automatic voltage regulator, and governor control, whereas on the wide-area level, automatic generation control is used [5]. To ensure safe operation of power flow through transmission lines, two control algorithms are utilized in the transmission system: state estimation and voltage-ampere reactive compensation. Two main algorithms are used in the distribution level control namely load shedding control, and advanced metering infrastructure.

C. Interactions and Intra-actions

CPPS dependencies are classified into inter-actions and intra-actions, where the former studies the dependencies between various CPPS layers and the latter focuses on dependencies within a specific layer of a CPPS model. The complex interconnectivity between CPPS layers and the deep integration of ICT across all layers create further challenges to identify inter- and intra-dependencies. This section provides a brief explanation of these dependencies within the suggested CPPS model.

The suggested model takes into consideration previous classifications as follows. The model identifies direct and indirect correlations among layers and sublayers. For instance, an event taking place in the global communication layer might directly propagate into the physical layer, whereas a fault at local protection devices might not be directly reflected in the main computation layer. Both inter- and intra-dependencies have been characterized in the suggested model. For example, steady-state power flow studies, and transient stability studies are utilized to assess the performance of power components in the physical layer. Physical layer and decision layer are dynamically interactive through the global communication layer, whereas results of the computation layer are not directly reflected on the physical layer. The suggested model gives insights on the common cause, cascading and escalating impacts. A power cyber-attack taking place in any cyber layer, either local or global, might cascade into the physical layer.

D. Evaluating the Suggested Model

As previously mentioned, the CPPS evaluation criteria can be used to measure the degree of competence of the suggested CPPS model. First, the suggested model provides a high accuracy outcome due to high matching between the model and the real system model. The suggested model can be scaled up to a specific level where the computational limits are not violated. However, co-simulation approaches can be leveraged to overcome this drawback. Also, the suggested model fulfills the fidelity feature since it provides a more detailed CPPS reducing the degree of approximations between

various layers. High level of application-compatibility and topological-suitability is maintained. Different power system topologies, i.e., meshed and radial, and communication topologies, i.e., ring, star, and meshed, can be modeled. Finally, the suggested model can adapt to dynamic studies with high degree levels. Various time scales can be used for analysis and assessment.

IV. Conclusion

This paper has classified system layers based-on their common, coupled, and shared functions. Also, interactions between the classified layers were identified and characterized, all possible interactions were enumerated, and they have been clustered based on their impact on the system. Furthermore, based on the overall function of the layer and types of its components, intra-action within the layers were characterized. The strategies developed in this paper for comprehensive classification of system layers and characterization of their inter- and intra-actions contributes towards the goal of accurate and detailed modeling of state transition and failure and attack propagation in CPPS. The accurate and detailed modeling of state transition and failure and attack propagation in CPPS is a necessary step towards reliability and resilience analysis, evaluation, and enhancement of CPPSs.

Acknowledgement

This work was supported by the U.S. National Science Foundation (NSF) under Grant NSF 1847578.

References

[1] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, 2022.

[2] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[3] I. Graja, S. Kallel, N. Guermouche, S. Cheikhrouhou, and A. Hadj Kacem, "A comprehensive survey on modeling of cyber-physical systems," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 15, p. e4850, 2020.

[4] N. H. Carreras Guzman, M. Wied, I. Kozine, and M. A. Lundteigen, "Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis," *Systems Engineering*, vol. 23, no. 2, pp. 189–210, 2020.

[5] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389–1407, July 2017.

[6] C. Someswara Rao, R. Shiva Shankar, and K. V. S. Murthy, "Cyber-physical system—an overview," in *Smart Intelligent Computing and Applications*, S. C. Satapathy, V. Bhateja, J. R. Mohanty, and S. K. Udgata, Eds. Singapore: Springer Singapore, 2020, pp. 489–497.

[7] G. Karsai and J. Sztipanovits, "Model-integrated development of cyber-physical systems," in *Software Technologies for Embedded and Ubiquitous Systems*, U. Brinkschulte, T. Givargis, and S. Russo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 46–54.

[8] J. Sztipanovits and G. Karsai, "Model-integrated computing," *Computer*, vol. 30, no. 4, pp. 110–111, 1997.

[9] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A survey of cyber-physical power system modeling methods for future energy systems," *IEEE Access*, vol. 10, pp. 99 875–99 896, 2022.

[10] R. V. Yohanandhan, R. M. Elavarasan, and et al., "A specialized review on outlook of future cyber-physical power system (CPPS) testbeds for securing electric power grid," *International Journal of Electrical Power & Energy Systems*, vol. 136, p. 107720, 2022.

[11] J. Mitra, M. Benidris, and N. Nguyen1, "Dynamic contingency analysis and remedial action tools for secure electric cyber-physical systems," in *Cyber-Physical-Social Systems and Constructs in Electric Power Engineering*, S. Suryanarayanan, R. Roche, and T. M. Hansen, Eds. IET, 2016, ch. 5, pp. 97–132.

[12] J. Mitra, M. Benidris, N. Nguyen, and S. Deb, "A visualization tool for real-time dynamic contingency screening and remedial actions," *IEEE Transactions on Industry Applications*, vol. 53, no. 4, pp. 3268–3278, July 2017.

[13] Y. HAN, C. GUO, S. MA, and D. SONG, "Modeling cascading failures and mitigation strategies in pmu based cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, pp. 944–957, 2018.

[14] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, June 2013.

[15] C. B. Vellaithurai, S. S. Biswas, R. Liu, and A. Srivastava, "Real time modeling and simulation of cyber-power system," in *Cyber physical systems approach to smart electric power grid*. Springer, 2015, pp. 43–74.

[16] V. Aravinthan, T. Balachandran, M. Ben-Idris, W. Fei, M. Heidari-Kapourchali, A. Hettiarachchige-Don, J. N. Jiang, H. Lei, C. Liu, J. Mitra, M. Ni, M. Papic, M. Parvania, M. Sephary, C. Singh, A. Srivastava, A. Stefanov, H. Sun, and S. Tindemans, "Reliability modeling considerations for emerging cyber-physical power systems," in *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, Boise, Idaho, June 2018, pp. 1–7.

[17] Q. Zhu, C. Rieger, and T. Başar, "A hierarchical security architecture for cyber-physical systems," in *2011 4th International Symposium on Resilient Control Systems*, 2011, pp. 15–20.

[18] Q. Zhu, *Multilayer Cyber-Physical Security and Resilience for Smart Grid*. Cham: Springer International Publishing, 2019, pp. 225–239.

[19] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, D. Wollman *et al.*, *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology, 2021.

[20] Y. Yang, S. Wang, M. Wen, and W. Xu, "Reliability modeling and evaluation of cyber-physical system (CPS) considering communication failures," *Journal of the Franklin Institute*, vol. 358, no. 1, pp. 1–16, 2021.

[21] I. A. Tøndel, J. Foros, S. S. Kilskar, P. Hokstad, and M. G. Jaatun, "Interdependencies and reliability in the combined ict and power system: An overview of current research," *Applied computing and informatics*, vol. 14, no. 1, pp. 17–27, 2018.

[22] M. Heidari-Kapourchali and V. Aravinthan, "Component reliability evaluation in the presence of smart monitoring," in *2013 North American Power Symposium (NAPS)*, 2013, pp. 1–6.

[23] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2007, pp. 54–67.

[24] H. Lei and C. Singh, "Non-sequential monte carlo simulation for cyber-induced dependent failures in composite power system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1064–1072, 2017.

[25] B. Falahati and Yong Fu, "A study on interdependencies of cyber-power networks in smart grid applications," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012, pp. 1–8.

[26] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015.

[27] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan 2012.

[28] S. Paul, A. Parajuli, M. R. Barzegaran, and A. Rahman, "Cyber physical renewable energy microgrid: A novel approach to make the power system reliable, resilient and secure," in *2016 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia)*, Nov 2016, pp. 659–664.

[29] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, July 2017.