IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 August 2022, accepted 31 August 2022, date of publication 15 September 2022, date of current version 26 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3206830

SURVEY

A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems

MICHAEL ABDELMALAK[1], (Student Member, IEEE), VENKATESH VENKATARAMANAN[2], (Member, IEEE), AND RICHARD MACWAN[2], (Member, IEEE)

[1]Electrical and Biomedical Engineering Department, University of Nevada Reno, Reno, NV 89557, USA
[2]National Renewable Energy Laboratory, Golden, CO 80401, USA

Corresponding author: Venkatesh Venkataramanan (vvenkata@nrel.gov)

This work was supported in part by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract DE-AC36-08GO28308; and in part by the Laboratory Directed Research and Development (LDRD) Program at NREL.

ABSTRACT The grid of the future will have a higher penetration of grid edge devices that enable increased automation and grid edge intelligence. The current grid models do not account for these grid-edge devices, and the creation of cyber-physical models for the grid is essential to understand the impact of these devices. Although existing cyber-physical power system (CPPS) models have been developed using a wide variety of approaches, a comprehensive review of the validity of these approaches and their suitability for modeling the future grid has not been performed. In a CPPS, the physical layer usually consists of the power grid and protection devices, whereas the cyber layer consists of communication, computation, and control components. This paper provides a review on the existing approaches to model CPPS and to characterize the inter- and intra-actions for distributed autonomous systems. The CPPS models can then be used to perform various analyses, such as cyberattack analysis, threat analysis, and resilience analysis. A qualitative evaluation criteria for the various modeling paradigm is discussed to help researchers understand the trade-offs in choosing the right modeling method for their particular application.

INDEX TERMS Cyber-physical power systems (CPPS), cybersecurity, finite state machines, graph network, modeling techniques, system and control method, test beds.

I. INTRODUCTION

Power grid modernization has gained significant momentum in the last decade. As part of the modernization, advanced communication and automation technologies are being deployed in power systems, and the resulting systems are known as cyber-physical power systems (CPPS), which consist of physical (the power grid) and cyber (e.g., communication and computation systems) layers [1]. CPPS leverage two-way cyber-secure communication systems to improve the monitoring, protection, and control of power system components to achieve a smart grid concept with enhanced reliability, resilience, security, and sustainability [2], [3]. Although advanced technologies in the cyber layer improve the operation and control of power systems, they can expose power systems to multiple types of cyber and cyber-physical attacks [4], [5]. The increase of cyber threats can jeopardize the power system's ability to provide reliable and efficient power supply [6]; therefore, accurate and detailed modeling of CPPS and the dependencies between the physical and cyber systems in a CPPS is a necessary step toward the analysis, evaluation, and enhancement of the CPPS's reliability and resilience.

The associate editor coordinating the review of this manuscript and approving it for publication was Yunfeng Wen.

A. RELATED WORK

Extensive reviews on cyber-physical systems (CPS)—in particular, CPPS—modeling, analyses, evaluations and enhancement methods have been conducted [7], [8], [9], [10]. The authors of [7] provided a review on the architectural modeling of cyber-physical systems (CPS) in general, including integrated, distributed, and mobile systems. The work presented

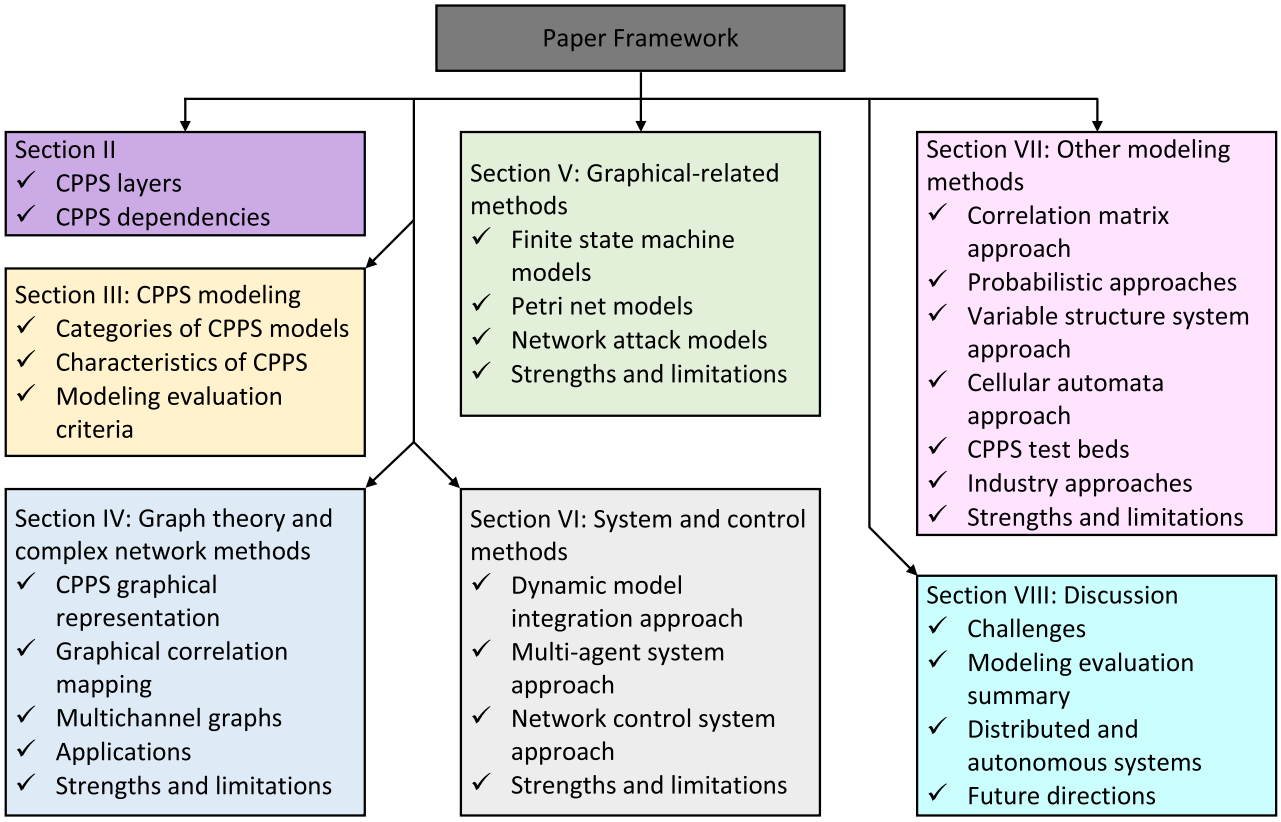

FIGURE 1. Paper framework.

in [8] reviewed CPPS classifications, the difference between cyber and physical systems, cyberattack types and impacts on CPPS, cybersecurity applications in CPPS, and simulation tools of CPPS. In [9], a review included differences between cyber-physical interaction models, such as graphical modeling, mechanism modeling, and probabilistic modeling. Also, the paper discussed the different solution methods used in CPPS studies. The work presented in [10] focused mainly on CPPS test beds. The paper discussed the importance of test beds for cyberattack analysis and cybersecurity studies. Also, the paper reviewed different types of test beds, including offline simulation, power hardware-in-the-loop simulation, rapid controller prototyping, software-in-the-loop simulation, human-in-the- loop simulation, co-simulation, and real-time simulation. In [11], a review on CPPS was provided on the risks and weaknesses in the system caused by cyberattacks. The authors of [12] provided a comprehensive review on the role of power electronics devices in CPPS, highlighting the increased cyber vulnerabilities, sophisticated modeling approaches for the cyber and physical components, and the increased computational burden in obtaining solutions for these models.

Though significant contributions have been provided by these reviews on CPPS classification and approaches, a few research gaps still exist. First, most existing work summarizes the current practices in modeling CPPS without properly aligning these modeling choices to CPPS characteristics. In other words, there are no clear evaluation criteria that measure the suitability of CPPS modeling choices to the requirements of their analyses. Also, these papers do not consider the evolving transition of CPS in general toward more distributed and autonomous environments, specifically in power systems. They give additional attention to cyber-related analysis, including cyberattack modeling, cybersecurity evaluation, cyber-induced impacts, and cyber vulnerabilities, while providing less detail on a deeper review of the technical modeling challenges of CPPS; therefore, this paper is tailored to address some of these gaps and provide a guide the community to better understand the trade-offs and design choices in creating CPPS models, especially considering the transition to distributed and autonomous environments.

B. CONTRIBUTIONS

This paper provides a critical and comprehensive review of existing methods and practices for modeling CPPS. It reviews CPPS layers and as well as the corresponding inter- and intra-dependencies within a CPPS. This paper also evaluates current modeling methods based on a well-defined set of criteria that capture CPPS characteristics. This paper will aid in ongoing efforts to perform detailed analysis on CPPS by helping to better understand modeling trade-offs and choices. The papers selected for this literature survey are based on Kitchenham's guidelines [13], with the primary objective to provide a framework/background to appropriately position

new research. In this case, the survey is undertaken with two primary research questions in mind:

1) What are the advantages and disadvantages in choosing a particular method to model CPPS? How to evaluate the suitability of the approach to the problem in hand?
2) How does the modeling paradigm suit the transition to a more distributed and autonomous power grid?

To address these questions, a detailed literature survey was performed using the search terms ''cyber-physical power systems,'' ''cyber-physical smart grid,'' ''cybersecurity for smart grid,'' and ''cyber-physical model,'' including others. The papers that provided detailed modeling of both cyber and power systems were selected to be included in the survey, avoiding repetitions if any. To capture broader methods, papers that studied purely cyber and physical models were also included to evaluate their suitability to include in the survey. Finally, papers that demonstrated the effects of cyberattacks on CPPS were also included in the initial selection to highlight engineering and intrinsic approaches. These papers were then analyzed and suitably filtered to be included in this survey. The main contributions of this paper can be summarized as follows:

- Reviews several modeling approaches of CPPS, including graphical theory models, graphical-related models, system and control models, correlation models, and probabilistic models
- Provides a critical analysis of strengths and limitations of various CPPS models
- Evaluates the existing models through a five-metric evaluation criteria to measure their capability and applicability to various analyses
- Discusses future directions and recommendations to develop models that cope with the emerging technologies and systems, including big data, resilience, cybersecurity, and real-time simulations.

C. PAPER STRUCTURE

The remainder of the paper is organized as follows. Section II provides a brief summary of CPPS layers and dependencies among system layers. Section III discusses different types of CPPS modeling and unique characteristics of CPS within the energy scope. Also, it explains the proposed evaluation criteria used to measure the capability of CPPS models to capture the system characteristics. Section IV focuses on graph theory and complex network modeling methods; whereas Section V discusses finite state machine (FSM), Petri net, and network attack modeling methods. A deep investigation of system and control CPPS modeling methods is surveyed in Section VI. Section VII summarizes other modeling methods. Section VIII provides a comprehensive analysis on the challenges of CPPS modeling methods, presenting possible future directions for various research-and-development activities and industrial applications. Section IX provides concluding remarks. Fig. 1 provides the framework of the paper.

II. CYBER-PHYSICAL POWER SYSTEMS (CPPS)

CPPS are the result of integrating measurement sensors, communication networks, advanced computational technologies, and intelligent automation systems into power grids. The authors of [14] define CPPS as the integration of information and communication technologies (ICTs) into physical systems. In [6], the penetrations of new communication and computational technologies—including cloud computing, the Internet of Things (IoT), and 5G communication systems—represent the evolving CPPS. Within an embedded systems scope, CPPS is the integration of computing systems through monitoring and control channels to the physical systems [15]. In the past decade, a significant amount of work has been devoted to the classification, characterization, and interaction of the cyber-physical layers of the various domains, including medical systems, transportation systems, agriculture, and power systems [16], [17]. This section summarizes the well-known CPPS models and layers as well as inter- and intra-dependencies among these layers.

A. CPPS LAYERS

CPPS layers are classified in the existing literature as follows. In [18], two layers—the grid and the cyber layers—were considered to study the effect of failures in the control and computation sub-layers on the stability of power systems. Other layers (e.g., sensing, communication, and protection) were assumed to be functioning perfectly. In the case of failure of the computation layer, system operators are assumed to rely only on the measurements (with no assistance from the computation layer), whereas a failure of the control layer means only the local automated control is assumed to function. In [19], CPPS were represented by the physical and cyber layer, where the latter provides three computational functions: wide measurements, protection, and control. In [20], the CPPS layers were classified into two main layers—physical and cyber—and a connecting layer, the wide-area monitoring, protection, and control. CPPS layers were been classified into physical, communication, and cyber layers in [21]. The authors of [22] provided a broader classification of CPPS layers: monitoring, control, communication, and physical layers.

A CPPS model provided in [23] comprised three main layers: the decision layer, the communication and coupling layer, and the physical layer. Each layer might have various operational statuses. The sensing and protection layers are assumed to be perfectly reliable, whereas the control and computation layers are combined in the decision layer. In this CPPS model, only abstract states and main interactions among the three layers are considered.

In [24] and [25], the cyber-physical smart grid was classified into the (a) physical layer, (b) control layer, (c) communication layer, (d) network layer, (e) supervisory layer, and (f) management layers, as shown in Fig. 2. The physical layer can be modeled based on ordinary differential-algebraic equations (DAE), Markov models,

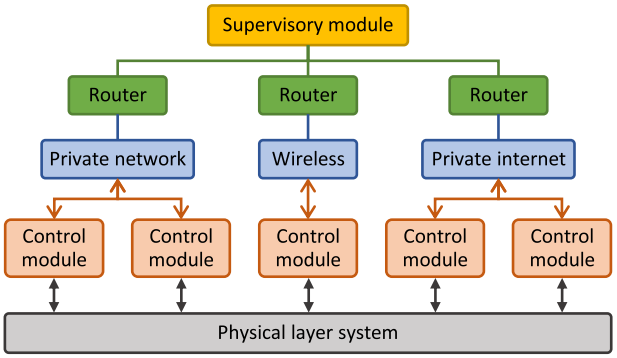

FIGURE 2. Different CPPS layers with local and global control systems.

or model-free statistics. Numerous control components—such as sensors/observers, intrusion-detection systems, other smart control components—are considered under the control layer. The communication layer is between the control and the router through various forms, such as a private network, wireless communications, and Internet. The network layer basically comprises two components: routing and network formation. The supervisory layer supervises all these layers through various commands. The supervisory layer performs the data analysis or fusion to deal with ongoing situations. The final layer is the decision-making management layer, which deals with numerous tasks, such as forming budgets, developing policies to deal with security- and privacy-related concerns, and dealing with the control system issues.

In [9], a comprehensive CPPS model was provided, as shown in Fig. 3. The model comprises three tiers, including the component tier (Tier 1), the communication tier (Tier 2), and the function tier (Tier 3). Though each tier has its own function and characteristics, they all interact cooperatively to maintain stable and reliable operation of CPPS. Tier 1 comprises the primary physical equipment (generator, transformer, transmission line, etc.), secondary equipment (protection relay, sensor, actuator, etc.), and the connected electric devices. All devices are connected together in a specific topology to fulfill their functions. Local controllers are responsible for collecting sensor information and control actuators for the optimal operation of the primary component. In Tier 2, the collected information is passed from Tier 1 to the master control centers through a communication network via wired or wireless communication media. The efficiency and effectiveness of the data transmission relies mainly on the communication technology, network traffic, routing mechanism, and communication topology. Finally, Tier 3 handles the advanced functions and operational decision-making process by storing and processing the data received at control centers. Multiple centers are connected through different typologies to monitor and control the overall system. Such centers include the web server, communication server, application server, database, and human-machine interface, which are connected together through international interface standards to allow easy information exchange and interoperability.

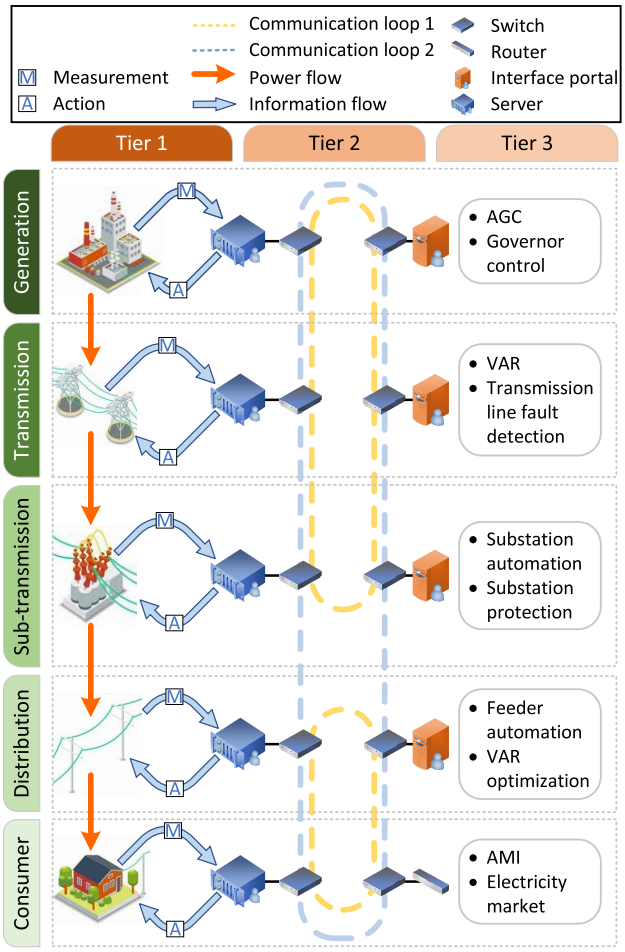

FIGURE 3. Centralized CPPS structure.

Once the distinct layers of a CPPS are defined, the interactions and dependencies between the layers need to be examined. This is discussed next.

B. CPPS DEPENDENCIES

A dependency in CPPS is a bidirectional relationship between two or more layers such that the state of one layer influences or is correlated to the state of the others. Dependencies in CPPS can be classified as inter- or intra-dependencies based on their scale. Interdependencies refer to interactions taking place between groups (layers), whereas intra-dependencies denote interactions within the same group or layer. Because of the complex integration of ICT to all CPPS components, it is challenging to identify the inter- and intra-dependencies among CPPS layers. This subsection describes various types of dependencies as well as various approaches considered in the literature to model interactions in CPPS.

Interactions are usually classified based on the CPPS layers. The authors of [26] provided a detailed guideline and illustration on the interconnections between ICT layers and power systems. The guideline classifies dependencies among CPPS layers into (1) common cause, components of both systems fail because of the same reason, i.e., a substation impacted by a hurricane; (2) cascading, a failure in

one system propagates to other systems causing a ''domino effect'', i.e., the power outage of ICT components; and (3) escalating, an existing failure in one system worsens an independent failure in another system, i.e., failure of protection devices when a failure occurs in the ICT components. The authors of [27] provided a classification based on the correlation between networks and elements into: direct element-element, direct network-element, indirect element-element, and indirect network-element. In [28], the interdependencies between infrastructure layers were categorized according to various dimensions, as follows: the (1) type of interdependencies, (2) infrastructure environment, (3) couplings among layers, (4) infrastructure characteristics, (5) state of operation, and (6) type of failure affecting the infrastructure. In [8], the authors identified three levels of interactions: (1) interactions within local levels, where power system controllers receive information from local protection and communication layers; (2) interactions between physical and communication platforms; and (3) interactions between communication and central computational platforms.

Various methods have been proposed to model the interactions among CPPS layers. The authors of [26] described five main methods to identify and analyze interdependencies: (1) hazard identification methods, (2) causal analysis methods, (3) consequence analysis methods, (4) topological analysis methods, and (5) dynamic analysis methods. In [29], a Markov state model was identified on the component level to model the transitions between the physical and cyber failures. A Petri net model was introduced to model interdependencies between the ICT and the physical layer, where various malicious attacks have been simulated to assess their impacts on the power system [28]. The authors of [30] leveraged the concept of a cyber-physical interface matrix (CPIM) to assess the reliability of power systems against cyber-induced failures. CPIM uses IEC 61850 to build a correlation matrix that induces cyber failures into physical components. In [31], a Bayesian attack model was used to simulate the propagation of cyberattacks into communication and computational layers and their impacts on the tripping breaker in the physical layer. The approach was used to evaluate the reliability of power systems under supervisory control and data acquisition (SCADA) cybersecurity considerations. The authors of [32] provided a detailed illustration of using graph theory integrated with a chaotic levy flight algorithm to model the propagation of a cyberattack leading to the cascading failure of power grids.

III. CPPS MODELING

Modeling is the key challenge to advance the state of the art to understand, assess, analyze, control, improve, and validate the performance of CPPS and the interactions within the system layers. Designing and developing accurate models is an essential step in the design of any system [33], [34]. A CPPS model usually comprises models of physical processes, communication modes, and computational processes. This section provides a brief summary of the existing CPPS modeling approaches. Also, it highlights the main characteristics of CPPS and their corresponding impacts on proper modeling. Then, a five-metric evaluation framework is discussed to evaluate the fitness of each CPPS modeling method to capture the required characteristics.

A. CATEGORIES OF CPPS MODELS

Various methods have been provided to present proper CPPS models that describe system heterogeneity, information system characteristics, and information models. The classification process relies on some main factors, including system time characteristics (continuous versus discrete), component characteristics (physical versus cyber), and scope of study or application (assessment, simulation, optimization, etc.). This section provides a quick illustration of the main CPPS categories.

The authors of [8] provided three main categories of CPPS modeling: interconnection, interaction, and interdependent modeling, as shown in Fig. 4. The interconnection modeling captures the act of the physical and cyber systems in a distinct manner; whereas the interaction modeling focuses on the effect of both systems on each other. The interdependent modeling measures the degree of dependency between both systems. Though it might look difficult to differentiate among the three models, each type focuses on studying CPPS from a different prospective. Note also that interconnection modeling mainly focuses on the component level; whereas interdependent modeling is applied on the system level.

In [9], CPPS models are classified according to the following dimensions: graphical, mechanism, probability, and simulation. In the graphical dimension, graph theory and complex network theory are leveraged. A CPPS model can be converted into a graphical network structure that captures the inner relationship between the network topology parameters and the system behavior. The dynamic behavior between the CPPS and the cyberattack process can be described using FSM models, Petri net models, attack tree models, attack graph models, and state transition diagrams. The mechanism dimension aims to leverage the differential-algebraic equations to analyze the relationship between the cyber failures and the power system components. Such models include analytical models, dynamic system-based models, hybrid system models, variable structure system models, and multi-agent models. The probability dimension focuses on the role of uncertainties in CPPS models, including the predictability of cyberattacks and the stochastic behavior of cyber and power system components. Finally, the simulation dimension builds a simulation model for experimental analysis.

Other studies have provided a simpler classification of CPPS models. In [35], CPPS modeling approaches were classified into: correlation matrix methodology, graph theory, complex network, FSM, mathematical programming, and the cellular automata method. CPPS models were classified into time-driven and event-driven systems in [36]. A more generic classification of CPS models was presented in [37], which

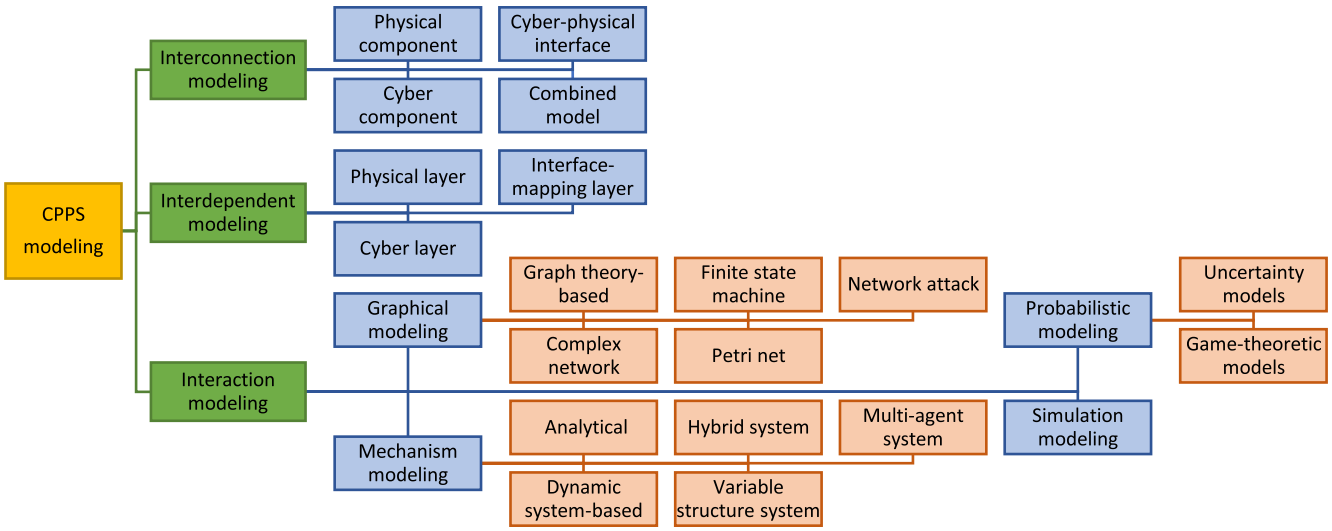

FIGURE 4. CPPS modeling approaches presented in [8].

is divided into three main categories: modeling techniques, modeling requirements, and application domains.

B. CHARACTERISTICS OF CPPS

The inter- and intra-dependencies in CPPS have unique characteristics that set CPPS apart from other CPS and require careful selection of the modeling choices. These characteristics include, but are not limited, to: (1) the massive network topology and system mechanism level, which include the large number of components that are connected together in a nontrivial topology and numerous meshed connections between them and the well-defined operating mechanisms of each system to satisfy their operational constraints; (2) the combination of continuous and discrete events—CPPS are considered systems of systems that are deeply integrated, time-space, multidimensional, heterogeneous systems where the power system belongs to the continuous time domain and the cyber layer lies within the discrete domain; (3) the mixture of static and dynamic behaviors—the power system comprises many dynamic components as compared to the larger number of static components in cyber system; and (4) the role of uncertainties in the decision-making procedure—this includes the impacts of uncertainties from renewable energy system resources, system errors, measurement errors, communication latency, and the lack of bulk energy storage.

Fig. 5 summarizes the main characteristics of both cyber and physical systems [10]. CPPS have a wide spectrum of modeling paradigms as a result of the diverse time, location, and size of the components under study. Physical system components with dynamic behavior are connected to cyber system components with static behavior to maintain the reliable operation of the physical system. Because of the different topologies of both physical and cyber systems, the close dependency between them is a vital and critical coupling point. Also, interoperability between the two systems is a must to exchange information in a timely and actionable frame. Proper CPPS models need to consider the aforementioned characteristics of each system and address the interface challenges of integrating cyber with physical systems to provide grid applications.

These grid applications rely primarily on control and computations enabled by the ICT infrastructure. In [38], a brief summary of the challenges of security in controlling CPS was provided. First, it is required to design a control policy that ensures the stability of the overall system by considering the large number of spatially distributed system components. Second, comprehensive models of communication networks that properly model limited capacity, random delay, packet loss, and intermittent network connectivity are a must to reduce the impacts of denial-of-service attacks [39], [40]. Third, system controller design needs to accounts for the random failure behavior of measurement devices and actuators via fault-tolerant control approaches [41]. Finally, it is required to design distributed algorithms that can perform a global task with local information exchange through advancing distributed estimation [42].

C. MODELING EVALUATION CRITERIA

Despite the significant contributions in the surveyed literature, only a few papers provided a qualitative assessment of CPPS modeling techniques. Besides providing a comprehensive technical review of CPPS modeling, this works develops an assessment framework to measure the pros and cons of each model. The modeling paradigms are assessed over five main criteria: (1) accuracy, (2) scalability, (3) fidelity, (4) ability to model distributed systems, and (5) ability to model dynamics. Each model is assigned a low or high rank based on its performance in a specific criterion. While additional criteria can be used to evaluate CPPS modeling methods, these five represent a comprehensive set of parameters on which existing CPPS modeling methods can be studied, and

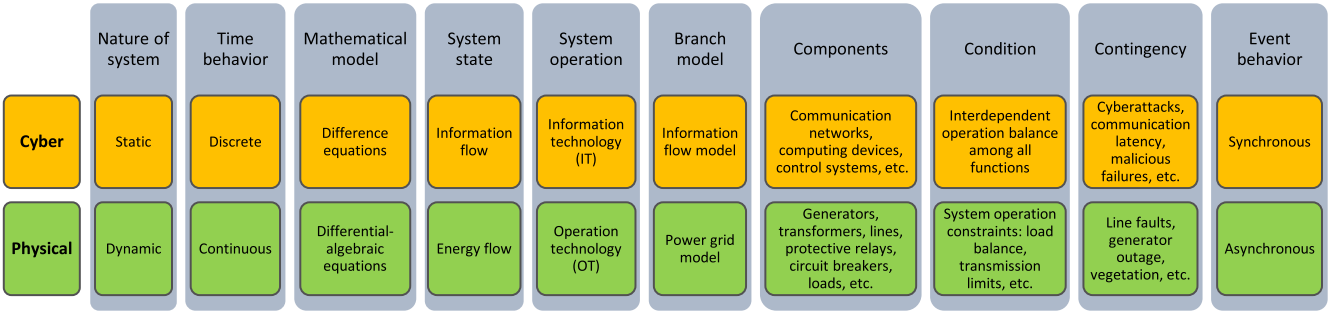

FIGURE 5. Characteristics of cyber and physical systems.

sufficient information is available to determine their suitability for modeling future energy systems. Other criteria, such as the modeling method's suitability to accommodate emerging technologies can also be considered, however there is insufficient information to evaluate their suitability at this time, thus placing it oustide the scope of this work. The model evaluation criteria are explained next.

1) ACCURACY

CPPS model accuracy is the extent to which a modeling paradigm accurately represents the physical manifestation and phenomena and agrees with reproducible and repeatable experimental data. These criteria assess the performance of a model and its consistency over a wide range of scenarios and inputs. The CPPS model should be able to accurately represent various operating conditions and remain consistent over various factors, such as geographic locations, solution techniques used to solve the model, connections to external components, and so on.

2) SCALABILITY

This metric measures the ability of a specific CPPS model to represent large-scale systems. Many existing models can easily model small-scale CPPSs; however, various challenges arise when the system size increases. Some challenges include, but are not limited to, the complicated model conversion process, limited computational power, diverse modeling domains, and technological advancements in cyber and communication systems.

3) FIDELITY

The fidelity of a CPPS model is defined to be the capability of the model to provide equal or semi-equal outcomes to the results collected from real-world systems or scenarios. In other words, minimal discrepancy should be observed between the studied model and the real-world system. This criterion measures the degree to which the CPPS model reproduces the state and behavior of real-world feature or operating conditions. The complexity of achieving this goal in CPPS modeling might be very challenging because of the high nonlinearity levels of several power system components. Also, the adoption of an approximation-based mathematical representation to solve the differential equations representing the behavior of the physical system induces further complexities.

4) DISTRIBUTED SYSTEMS

The electric power grid can be considered a system of systems that spans large numbers of stakeholders. The conventional power system—comprising generation, transmission, and distribution—has expanded to include customers, operation, the energy market, and business services. The capability of CPPS models to capture the distinctive features of these players as well as their dependencies has become a necessity to achieve the smart grid concept. On the other hand, the transition from centralized to distributed generation resources has increased the modeling complexities. Also, the spatially distributed system components have resulted in increased numbers of local control centers. This metric measures the ability of a CPPS model to easily represent the aforementioned distributed structure.

5) DYNAMICAL BEHAVIOR

This criterion evaluates the suitability of the model to accurately capture the system dynamical behavior across various time resolutions. At a fundamental level, the model must be capable of changing from one state to another in response to internal changes and external disturbances, and not remain static across time; however, this criterion evaluates the performance of the model to accurately represent the changing dynamic behavior of a system not only over a specific time horizon but also over a large variety of system changes. For example, a model that is equally capable of representing slow changes over a number of years and also also capable of capturing subsecond dynamics would be ideal. But models come with various trade-offs when evaluating them over various time horizons and this criterion evaluates the flexibility provided by the model to accurately capture both slow changes and subsecond behaviors.

IV. GRAPH THEORY AND COMPLEX NETWORK METHODS

Graph theory is one of the most widely used approaches to model CPPS. Graph models provide a proper visualization-based approach to capture the relationship between physical and cyber systems. In CPPS graphical modeling, each power system component is assumed to map to a node in the cyber layer. This connection is responsible for transmitting measurements from the power system to the control cyber layer

and transferring the control decision in the reverse direction. The mapping between the layers can be a general function, or it can be more restrictive, such as a bijective relationship.

Complex network approaches rely mainly on graph theory. The complex network models are usually adopted as a result of the presence of large numbers of different types of system components across all layers [9]. CPPS can be represented by three layers: the cyber layer, physical layer, and interface-mapping layer. The cyber nodes represent the communication equipment and any independent autonomous system, including operation and monitoring systems. ''One-to-one'' and ''one-to-many'' inter-dependencies are leveraged to model the correlation between the physical and cyber layers based on the existing topology. For instance, a single power station might be responsible for supplying electricity to multiple autonomous cyber systems; hence, the one-to-many model is more convenient. Microscopic mechanisms can be integrated with macroscopic system characteristics to provide detailed analyses of the inter-dependencies among system components [43], [44].

The main difference between graphical-based modeling and complex network-based modeling is the scale of the system under study. Also, graphical-based models can be combined with other modeling methods because they represent actual CPPS topology. On the contrary, complex network-based models usually create an abstracted topology and are suitable only for a single complex network. Finally, complex network-based approaches are convenient to study the relationship between system topology and network evolution.

A. CPPS GRAPHICAL REPRESENTATION

A physical power system is represented by a graph, $\mathcal{G}_{\mathcal{P}} = (\mathcal{N}_{\mathcal{P}}, \mathcal{E}_{\mathcal{P}})$, where $\mathcal{N}_{\mathcal{P}}$ is a set of vertices corresponding to generators, buses, circuit breakers, and loads in the power system; and $\mathcal{E}_{\mathcal{P}}$ is a set of edges connecting system components, such as transmission lines and transformers. Following the same convention, the cyber layer can be represented as a graph, $\mathcal{G}_{\mathcal{C}} = (\mathcal{N}_{\mathcal{C}}, \mathcal{E}_{\mathcal{C}})$, where $\mathcal{N}_{\mathcal{C}}$ is a set of vertices that correspond to communication routers, servers, computing nodes, and control centers in the cyber system; and $\mathcal{E}_{\mathcal{C}}$ is a set of edges representing the communication channels between the information nodes. Both graphs can be either directed or undirected [8]. A directional arrow represents the flow of information in the cyber graph or the flow of power in the power graph. The failure of a physical power connection or a cyber information connection is represented by the removal of a graph edge, whereas the failure of a specific node component is represented by the removal of the corresponding vertex.

The authors of [11] showed the capability of a complex network approach to assess the vulnerabilities in CPPS based on the topological structure and provided a list of factors affecting the network graph modeling, including path redundancy, branch count effect, overlapping branches, switching operations, repetition of sources, and aggregated central point

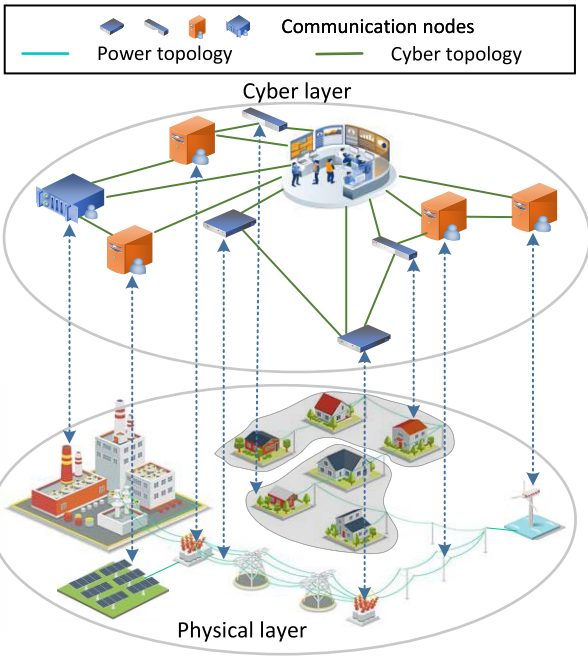

FIGURE 6. One-to-one CPPS mapping.

dominance. Also, the structural characteristics of the graph model representing a power grid were presented in [45]. An assessment framework based on system vulnerability and the associated relative variance was presented in [46] to study and assess the hierarchy of complex networks.

B. GRAPH THEORY-BASED CORRELATION MAPPING

Many studies have focused on the mapping correlation between the physical graph network $\mathcal{G}_{\mathcal{P}}$ and the cyber graph network $\mathcal{G}_{\mathcal{C}}$. The dependencies in CPPS have been modeled in diverse approaches, including one-to-one mapping [47], [48], [49], [50], one-to-multiple mapping [51], and cluster mapping [52]. The one-to-one mapping between the cyber nodes and the physical nodes is the most commonly used approach, as shown in Fig. 6. In [53], the correlation between networks was not assumed to be one-to-one but rather as a few coupling edges connecting both networks at specific nodes.

In [54], one-to-one mapping and two-to-two mapping between the physical and the cyber network was studied. Two strategies were used to reduce CPPS vulnerabilities within the proposed graphical model, including the degree-betweenness interface strategy and the closeness centrality interface strategy. In [55], a one-to-one mapping between the physical and the cyber networks was proposed considering a spatial representation of CPPS. The inter-dependencies between both layers is represented in four basic failure modes: information edge failure, information node failure, power edge failure, and power node failure. In [56], a one-to-one mapping was leveraged to model CPPS where four types of physical nodes are assumed: generation node, consumer node, distribution node, and transformer node. The presented framework was used to measure the robustness of the CPS graph model following a cascading failure impact.

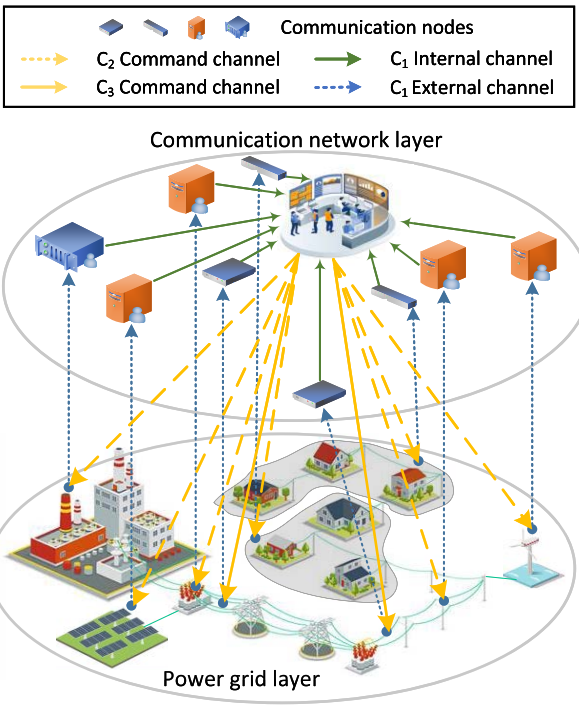

FIGURE 7. CPPS model based on different communication channels.

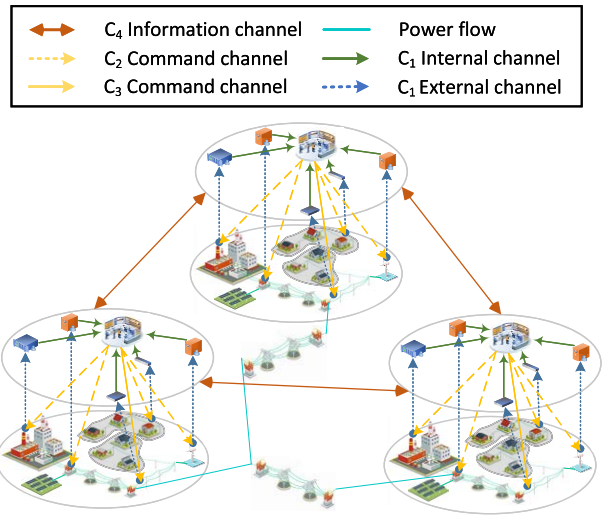

FIGURE 8. Large-scale CPPS model based on different communication channels.

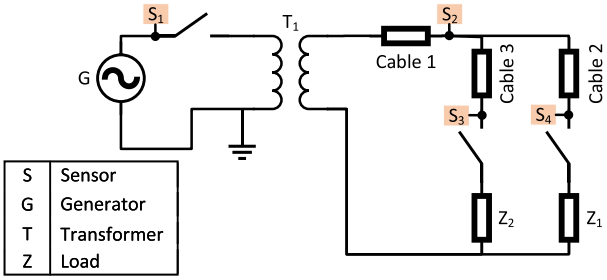

FIGURE 9. Physical model based on component state representation [59].

A one-to-one mapping was used to model the interdependencies between the power and communication networks in [57]; however, the communication nodes were represented as load components in the distribution level to capture the dependency of the communication network on the power grid. Each communication node is assumed to be fully operating if the power supplied exceeds a specific threshold. The dependency of the power grid on the communication network is modeled by assuming the loss of the corresponding communication or control node to the power component.

The authors of [58] developed a graphical network model to assess the cybersecurity level between physical and cyber systems. Communication channels are classified based on three types of transmitted information: C_1, information is uploaded from the power nodes to the communication center; C_2, command controls are transferred from the control center to the power nodes directly; and, C_3, command controls are transmitted to the line breakers. Fig. 7 visualizes the different channels between CPS layers. A one-to-one mapping is assumed between the physical nodes and the cyber nodes. The proposed approach can be adopted to larger CPS by adding another communication channel, as shown in Fig. 8. Large-scale CPS can be divided into smaller CPS based on geographic boundaries such that each small CPS has its own control center. An additional communication channel between control centers is required to maintain observeability of the whole system.

In [59], a cyber-physical graphical model was presented to model the cause-effect relationship between cyber and physical components. Each node represents an associated grid component, such as generators, transformers, loads, circuit breakers, switches, control centers, sensors, and breaker actuators; whereas edges are selected to represent state dependencies among the various components. Directed links are between nodes to visualize the energy flow and the information flow. Each node is associated with a state governed by the dynamical system equations. Fig. 9 and Fig. 10 visualize the presented CPS graph model on a simple generator substation.

The authors of [60] developed a graphical network model by coupling different power grids with a single cyber layer, as shown in Fig. 11. The power system is represented by a undirected graph, and four types of nodes are modeled: supply and load node (SLN), supply node (SN), load node (LN), and neither supply nor load (TN). The communication network is modeled as an undirected graph with three levels of control centers: a regional control center (RCC), an area load dispatch center (ALC), and a local control center (LCC). Two sets of one-way edges are formulated based on the interdependencies represented in Fig. 11.

The authors of [61], [62] created a many-to-one-based graphical model using a graph minor where the power system graph is considered to be a graph minor of the cyber graph, as represented in Fig. 12. This approach considers that there are a number of associated cyber components to a single power system component, thus having a many-to-one relationship. The cyber and power system graphs still have a bjiective relationship, and the underlying topology for both graphs is preserved by assuming that the power system

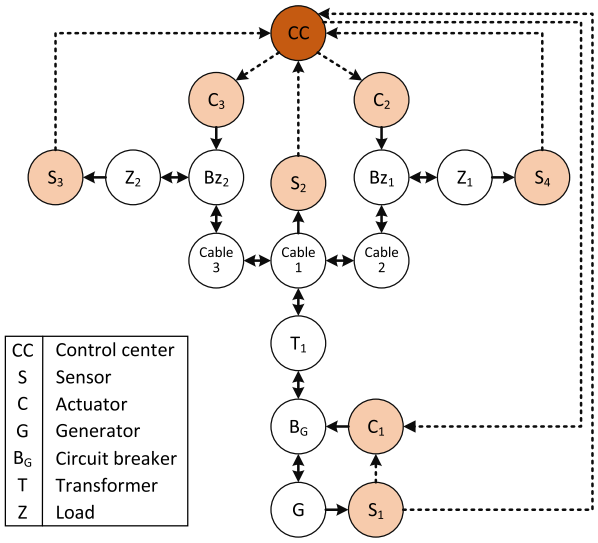

FIGURE 10. CPS modeling based on component state representation [59].

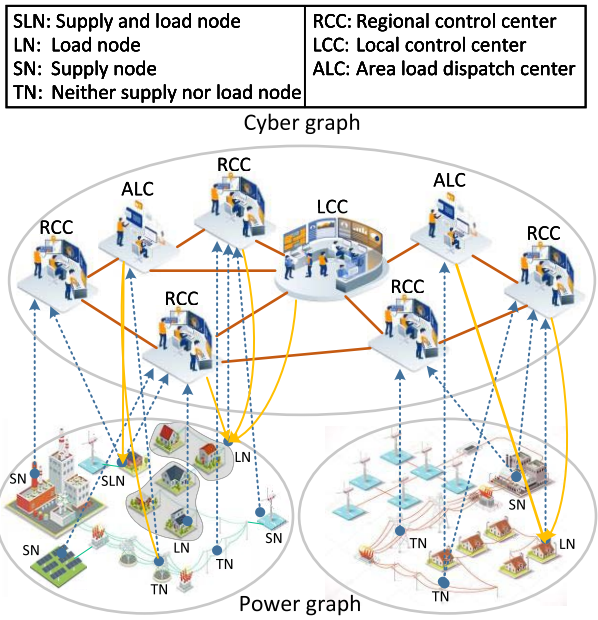

FIGURE 11. CPPS model presented in [60].

graph is a graph minor, which means that the power graph is essentially a reduction of the larger cyber graph.

A scale-free graph approach was developed in [53] to address the scalability issue of large-scale networks, where the cumulative distribution and analytical equivalent methods were used to measure the degree of functionality of the developed graphs.

C. GRAPH THEORY-BASED APPLICATIONS IN CPPS STUDIES

Graphical network representation is considered the most widely used modeling approach of CPPS. Numerous studies have leveraged graph theory-based approaches for various applications. This paper has highlighted only a few studies to show the capabilities of these methods for CPS analysis.

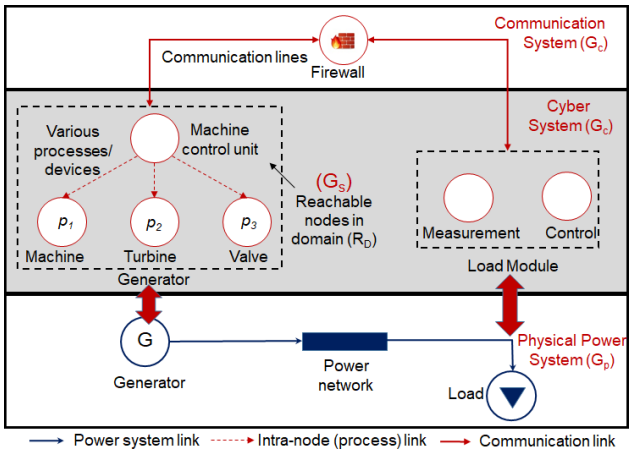

FIGURE 12. Many-to-one relationship presented in [61].

In [53], a coupling framework between the electrical power network and the natural gas network was presented using graphical models. In [63], a graphical model was presented to model CPPS for state estimation studies. A mapping methodology was provided in [64] to convert an electric power system into a transportation map through graphical methods. The developed transportation map was to solve the economic dispatch problem and the available transfer capability problem. The paper suggests leveraging the proposed approach to model similar problems in the cyber layer. In [57], a CPPS graph model was used to mitigate cascading failures of a power network on a communication network via a load-shedding mechanism.

In [65], a cyber-physical data-fusion framework that integrates sensor measurements from CPS and a stochastic information fusion algorithm was proposed to detect intrusions and malicious data for enhanced situational awareness. The proposed method leverages graph network methods to create a connectivity matrix between different system hosts that can be used to identify possible attack graphs. The created attack model was converted into a hidden Markov model to determine the attack path at each time instant based on a set of triggered alerts. The connectivity matrix approach was leveraged in [66] for improved contingency analysis of CPPS. The authors of [67] leveraged one-to-one mapping between power buses and phasor measurement units (PMUs) to improve state estimation caused by a joint cyber and physical attack model. The proposed cyber-physical model in [58] was used to assess the vulnerability of CPPS against physical impact [64]. In [60], the presented CPS model was used to formulate a multistate failure model of physical and cyber components for enhanced recovery caused by cascading failures.

D. GRAPH POOLING AND GRAPH NEURAL NETWORKS

Recently, there has been increasing interest in the concept of graph homomorphism, especially in the areas of constraint satisfaction problems as applied to graphs such as graph colorings. This has been explored for various applications, such as cyber defense mechanisms [68] and sequential

decision-making problems. These constraint satisfaction problems applied to graphs rely on techniques that can properly classify graph nodes, in the context of which graph neural networks (GNNs) have been leveraged. GNNs offer a method to perform graph pooling, in which case neural networks are used to downsample a graph while still retaining the critical features of interest across multiple graphs [69]. This can be used to map CPS where GNNs are used to retain the important graph properties of both the cyber and physical systems while pooling them together for combined analysis [70]. GNNs are then used to deploy various learning mechanisms to support grid applications, as reviewed in the survey [71]. This is an evolving area, where much more research activity is expected going forward.

E. STRENGTHS AND LIMITATIONS

As a results of the simplified models of the physical system characteristics, there is limited capability to use them in operation and control studies [9]. The special physical laws governing the behavior of power systems impose further limitations of graph-theoretic approaches in electric power system studies [72]. Also, the scalability of graph models to large-scale CPPS is still under investigation, with GNNs offering a promising way forward. A main drawback of graphical methods is the incapability to observe dynamic characteristics in power systems. This requires integrating the graph model with differential-algebraic equations in some fashion, which increases the complexity of the model formulation. Though one-to-one mapping provides a fair representation of the dependency between cyber and physical layers, the proper definition of each node representation in both the physical and cyber layers is required to avoid model complexity. In other cases, one-to-one mapping does not provide a convenient approach to model interdependencies in CPPS. The authors of [54] stated that one-to-one mapping does not usually capture the whole spectrum of cyber capabilities, and advanced one-to-many and many-to-one coupling provide a pathway to more comprehensive analysis. On the other hand, prioritization algorithms need be applied in one-to-many graphical representations to capture real system control behavior.

Based on the proposed evaluation criteria, graph theory and complex network models are characterized as having ***high accuracy, high scalability, low fidelity, are highly distributed, and have low dynamical behavior levels***. First, they provide accurate topological representations of both the cyber and physical layers as well as the inter- and intra-dependencies among both layers. Also, they have shown high ability to properly model large-scale CPPS, with even some of the largest models being smaller or comparable to graphs from other domains, such as social networks. As a result, they have been widely used for transmission systems, distribution systems, and integrated transmission/distribution systems. Such models are well suited to model the spatially distributed structure of CPPS. On the other hand, their fidelity level is low as a result of the lack of their ability to model the dynamic-differential and discrete-difference equations of system components. They also exhibit some limitations for time-varying behavior analysis and studies.

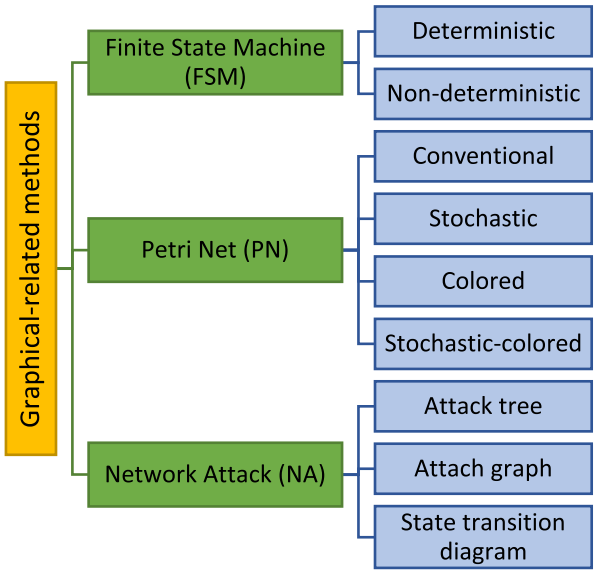

FIGURE 13. Categories of graphical-related methods.

V. GRAPHICAL-RELATED METHODS

These are modeling methods that leverage graph theory approaches on the system-level representation rather than the component-level representation. In other words, nodes of the graph model usually present a system state, and branches of the model capture the transition behavior between system states. These methods are classified into three main categories, as shown in Fig. 13.

A. FINITE STATE MACHINES MODELS

An FSM, or sometimes simply called a state machine model, is a mathematical model that represents the discrete-behavior computational process [73]. In FSM, a list of sequential actions is executed based on a sequence of events to change from one state to another. In other words, an input triggers the system to go from one state to another based on a predefined transition function. In CPPS, transitions occur in the physical layer, in the cyber layer, and between the cyber and physical layers for different triggering events [74].

An FSM is a widely used mathematical approach to model the interaction process of a CPPS based on the state description of the dynamic behavior. It is characterized by the ability to express the limited state and the relationship between transitions [75]. A state chart diagram is usually the outcome of applying an FSM, which provides a visualization of the system dynamic behavior. State chart diagrams have been a key factor to analyze the qualitative cyber-physical interactions.

FSMs are classified into deterministic and non-deterministic based on the problem formulation [8]. An FSM-based problem can be represented as follows:

$$(Q, \sigma, \delta, q_o, F) \tag{1}$$

where Q is a finite set of states, σ is a finite non-empty input, δ represents a series of transition functions, q_o is the initial state, and F includes the set of final states. In deterministic FSMs, there exists only one transition for each state; whereas multiple transitions occur in non-deterministic FSMs.

B. PETRI NET MODELS

A Petri net is described to be a network that captures the relationship between conditions and events. In other words, Petri nets are used to represent a system organization and the control behavior. In CPPS, Petri nets are used to simulate the interaction behavior between continuous dynamics of the physical system and the discrete information of the cyber system [76], [77], [78]. The authors of [28] illustrated a conversion procedure to create a Petri net model from a predefined FSM model. The proposed approach was used to understand the propagation mechanism of failure events in CPS.

Several Petri net models have been developed to assess the impacts of cyberattacks. Stochastic Petri net models have been used to model cyber-intrusion processes to assess the stochastic behavior of cyberattacks [79]. Colored Petri net models have been introduced to distinguish different attackers in the model by assigning a unique token color to each data value (type and operations). The authors of [80] leveraged colored Petri net models to analyze false data injection cyberattacks for improved intrusion detection. A quantitative assessment framework of a cyberattack propagation in CPS was developed by integrating stochastic and colored Petri net models [81]. In [82], a Petri net model integrated with game theory was used for CPS risk assessment. Also, a time-based Petri net model was leveraged in [83] to model the means of attack and attack information transmission route in CPS.

A Petri net model can be represented graphically or by using set notations, as follows:

$$(P, T, I, O, MP) \tag{2}$$

where P is a set of places, T is a set of transitions, MP is the marking of places with tokens, and I and O represent the input and output function for all transitions, respectively.

C. NETWORK ATTACK MODELS

A network attack is a graphical-related approach used to model diverse cyberattacks. Network attack models have been introduced into CPS studies as a result of the rapid integration of information and communication technology to power systems, introducing additional vulnerabilities. Such models are very useful to identify the sources of cyber vulnerabilities, apply proper mitigation and isolation strategies, and create more resilience for CPS. These methods are classified mainly into: attack tree, attack graph, and state transition diagrams [84].

1) ATTACK TREE

An attack tree is a graphical description of all possible paths of a cyberattack. Attack trees aim to visualize the multistage cyber network intrusion behavior and to capture the structure characteristics of a specific attack [85], [86]. The authors of [87] developed a cyber-physical threat model using attack trees for risk assessment and resilience enhancement. In [88], a security assessment framework was introduced to quantify the impacts of cyberattacks on the cyber and physical layers using attack tree.

2) ATTACK GRAPH

An attack graph describes the attacking policy of an attacker, including the correlation between different exploitation strategies. In an attack graph, the network topology and identified vulnerabilities are used to compute the probability of an attacker for a successful penetration attack. Attack graphs are system-independent, providing a proper way to model a complex combined network using an automatic generation method [9]. The authors of [89] used an attack graph to assess the security of the communication network in a CPS. In [90], an attack graph was used to analyze the impact of cascading failures in CPS. An automated attack graph generator was introduced in [91] to integrate the role of the Internet of Things in CPS for risk assessment.

3) STATE TRANSITION DIAGRAM

This model leverages the Markov decision process (MDP) to model the attack behavior of a cyberattack. The transition probabilities between Markov states are computed using the component vulnerabilities [66], [92]. Two advantages of using this model is their capability to extensively describe all types of attacks from a detection prospective and the possibility to define multiple system states based on the CPS safety levels [9]. This model features the adaptability to changing trends in system states and stochastic attack behavior. In [93], a state transition diagram was used to evaluate the reliability of CPPS against communication failures. Also, an automated cognition model was introduced in [94], leveraging a semi-MDP to model CPPS for risk assessment.

D. STRENGTHS AND LIMITATIONS

Though FSM models can provide advanced features—including composite state, entry and exit actions, state transitions, and guard conditions—there still exist a few challenges in the process of implementation, including poor reusability, difficult maintenance, and unsuitable quantization.

Petri net models are very convenient to capture the condition of the system change and the corresponding consequences on the system state, but such methods lack the capability to provide changes in data values or system attributes. Also, the scalability of Petri net models to large complex systems is still a challenge. As the system size increases, the computational time exponentially increases as a results of the increased environment restrictions.

Though network attack models have been widely used to model cyberattacks, a few challenges still exist. For instance, attack tree models are convenient for limited types of attacks, specifically sequential-based attacks. Attack tree

models have limitations on simultaneous attacks or multiple compound attacks. The formation and structure of an attack tree becomes more complicated for some complex modeling objects. On the other hand, state transition diagrams lacks the scalability feature to larger systems with increased numbers of vulnerable components.

The graphical-related methods can be ranked as having ***high accuracy, low scalability, high fidelity, low distributed, and high dynamical behavior*** characteristics. These methods have the capability to capture realistic system transition states considering the dynamic characteristics of the physical system as well as the meshed network structure of cyber systems. As a result, they can provide good visualization of real system behavior under different cyberattacks. On the other hand, scaling these models to larger systems is still challenging as a result of the exponential increase in the number of system states as the number of components increases. Also, their adaptability to the distributed environment is still a limitation.

VI. SYSTEM AND CONTROL METHODS

The hybrid dynamical system theory integrates the differential equations representing the continuous-time behavior of the physical system with the difference equations capturing the discrete-time behavior of the cyber systems [95]. The importance of advancing control systems to cope with the rapid integration of distributed energy resources (DERs) and ICTs in power systems was presented in [96].

A. DYNAMIC MODEL INTEGRATION APPROACH

The authors of [62], [97] introduced a CPPS modeling approach based on a cyber-based dynamical model formulation to integrate cyber technologies into the dynamic equations governing the behavior of the physical components. The model considers the actions of end users for control applications. First, each type of system components is represented as a cyber-physical model capturing the physical and cyber input-output signals, internal dynamics, local sensing, and actuation. The generator-turbine-generator model is used as a reference to build cyber-physical-based models of DERs and load components. Each component in the system is represented as a single module, including: (1) the internal states and the interaction variables between the module and the rest of the system and (2) the internal cyber signals and the-interaction cyber signals between the module and the rest of the cyber network. Then, a feasible integration between modular components is carried out based on the network constraints and topology. A discrete-time state-space DER model can be formulated as follows:

$$\dot{x_G} = \begin{bmatrix} -D_G/J_G & 1/J_G & e_T/J_G \\ 0 & -1/T_u & K_t/T_u \\ -1/T_g & 0 & -r/T_g \end{bmatrix} x_G + \begin{bmatrix} 0 \\ 0 \\ 1/T_g \end{bmatrix} u_G + \begin{bmatrix} -1/J_G \\ 0 \\ 0 \end{bmatrix} P_G \tag{3}$$

$$x_G = \begin{bmatrix} \omega_G & P_T & a \end{bmatrix}^T \tag{4}$$

where P_T and P_G are the mechanical and electrical powers of the turbine and the generator, respectively; J_G, D_G, and T_g are the moment of inertia, the damping factor, and the time constant of the generator; T_u is the time constant of the turbine; e_T is the valve position coefficient; and ω_G and a are the generator output frequency and the valve opening, respectively.

Following the same convention, a model of the cyber-physical load module can be formulated as follows:

$$x_{L,k} = \begin{bmatrix} 1 - \Delta T D_l/J_L & -\Delta T E_L/J_L \\ 0 & \phi_L \end{bmatrix} x_{L,k-1} + \begin{bmatrix} -\Delta T/J_L \\ 0 \end{bmatrix} P_{L,k-1} + \begin{bmatrix} 0 \\ E_L^T \end{bmatrix} \omega_L \tag{5}$$

$$x_{L,k} = \begin{bmatrix} \omega_{L,k} & L_k^T \end{bmatrix}^T \tag{6}$$

where L is the discrete load energy; P_L is the electrical energy delivered by the network to the load; J_L and D_L are the parameters of a converted load model, with ω_L representing its local physical state; ΔT is the sampling period; E_L is a zero array, with one at the corresponding time instant; and L_k is the sequence of the load values preceding the current time instant.

The presented model in [62] and [97] can capture the controllability and observability of the system under study. In [98], a hypothetical investigation of the CPPS dynamic model on a large scale was provided. A multilayered organization of complex CPPS was presented that captures both the local interactions among subsystem components and the intraactions between subsystems.

B. MULTI-AGENT SYSTEM APPROACH

In a multi-agent system, each physical entity or physical subsystem is represented by a single agent. Internal agent information is exchanged among all agents through communication networks. This approach is very convenient for distributed systems because it provides an effective control approach for various DERs in a flexible and timely manner. Also, the multi-agent approach features excellent autonomy, flexible adaptability, easy coordination, and social stability.

A control-based approach based on flocking theory for CPPS was proposed in [99]. The presented framework aims to improve the stability of a power system after a cyberattack considering the interactions between the cyber and physical layers. An exploration method was provided to synergistically harness the information and the physical couplings, then a control method was formulated to control the DERs for enhanced stability. CPPS is split into clusters, each represented by a few agents that capture the local system interactions and the local control information. The state-space model of each agent is formulated using a set of dynamic equations capturing the behavior of the assigned cluster. Agents with high physical coherency are grouped into the same cluster. The dynamics of the presented framework for stability-based studies are formulated as follows:

$$M_i\dot{\omega}_i = -D_i\omega_i + P_{m,i} - E_i^2 G_{ii}$$

$$- \sum_{j=1, j\neq i}^{N} P_{ij} \sin\left(\theta_i - \theta_j + \phi_{ij}\right) + \alpha_i u_i \quad (7)$$

where i corresponds to a specific agent, u represents the cyber coupling, and P and ϕ capture the physical coupling.

Further investigation into agent-based coupling for CPPS-based control studies was provided in [100]. A multi-agent framework was proposed to capture the physical and cyber couplings for centralized and decentralized control schemes. A single agent comprises a synchronous generator, a local generator sensing device, a distributed controller, and a fast-acting energy storage device. The agents are coupled physically through transmission line connections and in cyber form through the communication network. Each agent captures its own state and the other agents' interaction caused by the cyber-physical couplings. The proposed framework aims to improve the transient stability of a physically coupled CPPS leveraging fast-acting energy storage systems.

Other studies have also adopted multi-agent system modeling specifically in distribution systems. In [101], a holonic multi-agent system was developed to control the reactive power of solar panels considering the impacts of a cyber system. A load restoration strategy was introduced in [102] using multi-agent modeling of DERs considering proper communication and coordination among agents. The authors of [103] provided a cybersecurity framework of CPPS to improve the detection and isolation techniques of vulnerable components caused by a cyberattack. The proposed approach provides a comprehensive monitoring platform for improved situational awareness. In [104], a multi-agent framework was developed to detect anomalous grid operation and provide proper remedial actions for enhanced resilient operation of CPPS.

C. NETWORK CONTROL SYSTEM APPROACH

In [105], [106], and [107], a novel cyber-physical architecture was proposed to model CPPS using an arbitrated network control system approach. The proposed framework splits the power grid into multiple areas, wherein each operate by a different system operator or utility. The PMU measurements within each area are transmitted to a local phasor data concentrator (PDC). Each PDC is communicating with a corresponding cloud network that comprises a set of virtual machines (VMs). Each PMU is assigned to a specific VM that is responsible for the computation and analysis. All VMs then communicate with each other to generate a control input for each generator in the whole system. A co-design framework leveraging an arbitrated network control system was developed in [108] to achieve optimal control performance and efficient resource utilization considering communication delays.

A cloud-based CPPS model was used in [109] to provide a delay-aware architecture for wide-area control. The approach addressed the importance of local, intra-, and inter-area communication delays. A state-space model was formulated to include such delays in the input signals to the CPPS. A detailed illustration of a global and local closed-loop feedback system was presented, highlighting the scalability on larger systems.

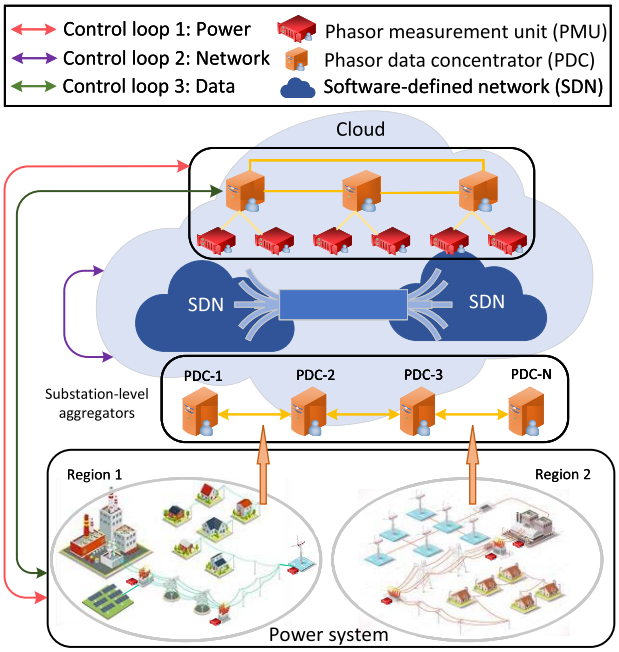

FIGURE 14. Cloud-based CPS model [110].

A distributed framework of a network control system was provided in [110] for the wide-area measurement application of CPPS, as shown in Fig. 14. The proposed framework comprises three control loops: (1) distributed state estimation and control, (2) software-defined networking (SDN)-based real-time communication network, and (3) cloud-based collection and processing. All loops operate independently and cooperatively to maintain stable and reliable operation of the CPS. The first control loop is responsible for collecting and processing the PMU data and transmitting the control signals back to the system actuators. The second control loop serves the different wide-area applications through SDN network implementation. Finally, the spatial distribution of the PMUs with different data rates to improve the data latency and the fault latency of the second loop is managed by the third layer.

In [111], a control-based framework was presented to include the role of renewable energy systems and demand response in a CPPS. The proposed methodology formulates the state-space models of CPPS at the primary, secondary, and tertiary control levels. The proposed framework was integrated with machine learning methods to determine the optimal delay assignment [112].

D. STRENGTHS AND LIMITATIONS

In the dynamic system model approach, the scalability presents a major problem, considering the computational burden to solve a large set of system equations. Though the authors provided a basic guideline to implement the approach on a large scale, there are no applied research or case studies from actual deployments. Though the framework provides a unified modeling method, a few challenges still need to be

addressed, including: (1) The integration of system models with regulatory stakeholders (such as utilities, government, regulatory bodies) is a challenge [98], (2) the creation of such system models often requires deep technical understanding and large amounts of data and testing before they can be validated, and (3) disconnection between the cyber and physical models leads to non-provable model performance.

Though the multi-agent approach has been extensively applied to control various DERs integrated through CPPS, further investigation is still required to address diverse communication protocols. Also, the capability to integrate the distributed multi-agent model with the conventional centralized control mode is still challenging.

A main challenge in network control system approaches is the large number of control variables, which increases the numerical computation of the system under study. As the number of inter-area computations, representing each subsystem of the physical layer, increases, the complexity dramatically increases. Some network control system approaches adopt a centralized state-feedback control design that might need to become more distributed fashion to improve the scalability feature.

System and control methods have ***very high accuracy, low scalability, low fidelity, are highly distributed, and have high dynamical*** characteristics. The high accuracy level is attained as a result of the presence of fully developed control-based theories that have been extensively studied and validated. Also, control-based methods can capture the dynamic characteristics of the system under study through the various developed state-space models. On the other hand, they show a very low scalability feature because the number of discrete equations representing each component will increase dramatically as the number of components increases as well as the dynamic model complexity of each component. These models provide high modeling fidelity for the physical system but low modeling fidelity for the cyber system, where things such as packet drops and latency can be well modeled, but advanced access control and vulnerability modeling presents a challenge; therefore, they might not be convenient to provide realistic emulation of CPPS from the cyber prospective.

VII. OTHER MODELING METHODS

This section provides a concise summary of other modeling approaches that have gained less interest or are still being developed.

A. CORRELATION MATRIX APPROACH

The correlation matrix approach aims to create a matrix that captures the correlation characteristics between the power and cyber components, including the communication layer. In [113], three main matrices were combined to form the overall system correlation matrix. Matrix decomposition methods have been used to build sub-matrices that capture the interdependencies within a specific layer [114], for instance, modeling communication network routers that are not directly connected to cyber nodes interfacing the power system component. An upstream and downstream architecture methodology was used to propagate the information signals between the bottom power layer and the top control center.

The authors of [54] used one-to-one mapping between the cyber and physical network to build an adjacency correlation matrix, as shown in (8).

$$A = \begin{bmatrix} A_p & A_{pc} \\ A_{pc}^T & A_c \end{bmatrix} \tag{8}$$

where A is the CPPS correlation matrix, A_p is the correlation matrix of the power system components, A_c is the correlation matrix of the cyber and communication components, and A_{pc} is the correlation matrix describing the connection between the power and cyber components.

In [115], the concept of the cyber-physical incident matrix (CPIM) was introduced to capture the impact of cyber failures on the physical system components. CPIM uses the available communication scheme, IEEE 61850, to build a correlation matrix that introduces cyber failures into physical components. Each row in the CPIM defines scenarios of the cyber component failure modes; whereas each column refers to the scenarios of the physical parts that are out of service caused by the cyber failure modes. The elements of the CPIM are the probabilities of the interface events, which can be extracted using the predefined failure rates of the cyber and protection components.

A compact version of the CPIM was introduced in [116] by eliminating the off-diagonal zeros. Each row in the modified CPIM represents a physical component, and each columns provides the probability of a consequent event given that a primary fault occurred on this physical component. Consequently, the sum of all row values should be one. Also, a consequent event matrix was developed to trace the source of failure in each physical component. It also summarizes all possible consequent events when a primary fault occurs at a particulate physical component.

The use of a Kronecker product can also be considered a correlation approach; it offers the flexibility of operating on matrices of arbitrary sizes, thus removing the one-to-one mapping constraint that is often present when working with strict matrix models. A Kronecker product has been used for power grid applications to understand the effect of cyber failures, such as packet drops on system stability [117], [118].

B. PROBABILISTIC APPROACHES

Probabilistic quantification approaches are used to quantify the stochastic behaviour of events impacting the performance of CPPS [119]. These approaches are mainly classified into uncertainty models and game-theoretic models.

Uncertainty models leverage diverse probabilistic models to assess the direct impacts of cyber vulnerabilities [120] and the indirect impacts of monitoring and protection systems caused by cyber malfunctions [121]. Such probabilistic models include numerical and sampling methods, analytical methods, approximate methods, and hybrid methods [122].

Various evaluation approaches have been applied to assess the reliability of CPPS, including a probability table [120], [121], a state transition diagram [116], minimal cut set-based [123], and Monte Carlo [124]. Most applied studies have not been applied to large-scale systems as a result of the restrictive computational limitations.

On the other hand, game-theoretic models use an attack-mitigation model in which rational participants make decisions for their own benefits based on the existing information [9]. Various models have been used, including zero-sum game [125], [126], Colonel Blotto game [92], [127], and stochastic game [128], [129]. A bi-level mathematical programming method was used to model an attacker-defender game to mitigate the impact of a cyberattack on a distribution system in [130]. Most game-theoretic models do not capture the actual physical behavior of the system components and the ideal performance of all controls.

C. VARIABLE STRUCTURE SYSTEM APPROACH

The variable structure approach aims to identify and locate the vulnerabilities of CPPS resulting in topology reconfiguration. Mathematical deduction theory is integrated with the value of the switching signals to determine the weakness points caused by a rapid continuous change in the topology of the system under attack [131]. The authors of [132] presented a variable structure-based CPPS model for transient stability control assessment and enhancement.

D. CELLULAR AUTOMATA APPROACH

Based on cellular automata theory, any device in CPPS consists of power cells and information cells [133]. The power cells usually include power primary components, such as generators, transformers, transmission lines, and loads; whereas information cells include secondary equipment associated with the primary equipment, such as the monitoring host, microcomputer protection device, measurement units, and control actuators. Each cell can hold a specific operating status based on the operating conditions. The transitions between cells and changing cell status can be used to model the interactions between the power and information cells.

E. CPPS TEST BEDS

Cyber-physical test beds are widely used for the creation of environments for the analysis and demonstration of novel technologies. The mapping techniques widely used in the creation of these test environments are primarily based on engineering judgement. As a first step, the placement of intelligent electronic devices that act as both the measurement and control devices for the power system are assigned to different breaker locations in the power system model. Along with the intelligent electronic devices, the mapping also accounts for controllers that are directly connected to grid control devices, such as regulators and capacitors. These devices form a primary interface between the cyber and physical layers in the test bed environments.

CPPS test beds have shown significant capabilities to evaluate the synergistic relationship between the physical and cyber system components, specifically in controlled environments. Also, they have been widely used in cybersecurity assessments, vulnerability analysis, intrusion detection, and mitigation strategy evaluations. The authors of [134] provided an extensive review on the recent simulation techniques of power systems, highlighting the importance of hybrid simulation and co-simulations to cope with the rapid integration of communication networks into power systems. The authors of [135] studied the various interfacing techniques between test bed components suited for different types of studies. The authors of [10] provided an extensive review on CPPS test beds detailing different types of platforms and the corresponding convenient scope of study. Also, an outlook of the future CPPS test beds was provided.

F. INDUSTRY APPROACHES

Note that information on CPPS modeling approaches used in the industry at utilities, regulatory bodies, and other stakeholders is not easily available in the literature. It is well known that power system control centers run complex algorithms, such as state estimation and optimal power flow, over large areas regularly using measurements from ICT infrastructure; however, combined analysis in terms of CPPS is still rare. Power grid operators concern themselves with the evaluation of the stability of systems using contingency analysis methods, such as "N-1" criterion, whereas information technology network operators at these control centers deploy traditional information technology monitoring tools, such as intrusion detection systems, to protect against cyberattacks. Although the study of cyber-induced power system failures and physics-informed information technology/operational technology system protection is gaining traction, implementations in the industry still seem to be building toward a common framework toward CPPS modeling. Most industrial deployments seem to rely on a one-to-one mapping between the cyber and physical components to perform CPPS studies.

G. STRENGTHS AND LIMITATIONS

The presented models in this section show varied levels of accuracy but rank low in overall CPPS accuracy because they specialize in one system (power or cyber) over the other. From a scalability point of view, correlation matrix approaches can be applied on large-scale systems, especially with advancements in high-performance computing for computing over large matrices; however, cellular automata and variable structure methods require extensive mathematical procedures for large-scale systems. The computational burdens of probabilistic methods significantly increase at larger scales.

The fidelity feature also varies across methods. For instance, cellular automata methods have high cyber fidelity and acceptable physical fidelity, whereas correlation matrix methods and probabilistic methods have low-fidelity modeling based on the adopted level of approximations in system

component modeling; however, variable structure methods have high physical, low cyber fidelity characteristics because they focus mainly on the impact of the network reconfiguration on power system dynamics. Among these methods, cellular automata, correlation matrix, and probabilistic methods are not usually convenient for dynamic-based studies.

Because of the limited number of studies leveraging variable structure methods and cellular methods, it might be difficult to evaluate such methods from the distributed prospective. Further investigation is still required to develop a better understanding of these methods from the proposed evaluation framework.

VIII. DISCUSSION

This section summarizes the main existing challenges to present a realistic comprehensive modeling approach of CPPS. First, it describes some previously mentioned challenges that still require further investigation. Then, it highlights some recent challenges facing CPPS modeling considering big data, renewable energy system integration, and communication technologies. A brief summary regarding the strengths and limitations of these modeling approaches is also provided. Finally, some potential future directions are provided to help the stakeholder community advance the modeling techniques of CPPS.

A. CHALLENGES

Besides the previously mentioned limitations on each modeling technique, a brief summary of some CPPS modeling challenges that have been raised by other researchers is discussed. First, a simplified comparison between different CPPS modeling approaches was presented in [9], highlighting the main characteristics and studied applications of each model. This comparison provides a guideline to understand the cyber-physical interactions for a specific scope of study. In [11], various research gaps were identified to assess the vulnerabilities in CPPS, including the trade-off between computational complexities and the scalability of CPPS, the multi-hazard modeling in different domains, the high meshed interdependencies among CPPS, the absence of a general resilience metric for CPPS, and the existence of proper measurement of performance. The authors of [12] provided a list of foundational issues and challenges in CPPS modeling, including coordination, energy data co-transfer, real-time evaluation, reliability, resilience, and scalability. On the other hand, purely graph-based approaches do not sufficiently model the state changes within the physical system [136]. Also, graph models do not account for the unique characteristics of the system at various timescales nor do they capture the physical modeling [136]. Because of the high sensitivity of the communication network to failures propagated from the power network, additional studies are required to enhance the robustness of communication systems [56].

Some major challenges in CPS modeling were addressed in [137]; however, further investigation of these challenges in CPPS is still required. First, models should have a deterministic solution rather than multiplicity of behaviors. Most numerical solvers dynamically adjust the step size, yielding biased solver-dependent behavior based on the selected step size. Also, Zeno behavior can be realized in some models as a result of the occurrence of an infinite number of events in a finite time interval. Having a deterministic, non-solver-dependent, and non-Zeno behavior model provides a robust and reliable testing and validation method. Consistency among the model components must be achieved to reduce the risk of divergence. As the CPS model becomes bigger, the possibility of misconnected model components increases. Validation approaches should be used to ensure correctness of connections among system components. Realistic consideration of the implementation details, including data latency and computational time, on the software level should be considered. Moreover, CPS modeling should consider the distributed nature behavior of the system components. This adds a few issues, such as disparities in time measurements, network delays, imperfect communication, consistency of the system state, and distributed consensus.

Although there has been rapid evolution and improved progress in the field of modeling CPPS, several issues are still under investigation. First, many studies model the communication or cyber layer for separate parts of the power grid, giving less interest to the interconnected communication network for generation, transmission, and distribution. Some studies do not fully observe the specific communication network topology and communication transmission mechanisms, yielding less realistic modeling. The rapid advancement in communication technologies has resulted in more efficient, low-latency, and cost-effective methods and systems, which calls for extensive efforts to adapt and integrate recent communication technologies, including 5G and wireless sensor networks, to CPPS.

B. MODELING EVALUATION SUMMARY

Table 1 summarizes the rank of each modeling approach using the proposed evaluation criteria. It is obvious that each modeling approach outperforms in some characteristics, and there is no single modeling approach that fulfills all criteria. The reason behind using graph theory and complex network methods is their capability to satisfy many required characteristics for proper CPPS modeling. This table also provides a guideline on possible integration techniques for improved modeling. For example, FSM methods can be integrated with control-based methods through proper handling of ordinary differential equations. Future research should explore combinations of different modeling paradigms to suit the specific scenario or use case under study. In addition, techniques in the modeling process can be further refined to address the enumerated weaknesses.

C. DISTRIBUTED AND AUTONOMOUS SYSTEMS

As noted, CPPS are transitioning to highly distributed, autonomous systems [138]. In this context, it is important for CPPS models to support distributed system modeling

TABLE 1. Summary of CPPS modeling evaluation.

Method	Accuracy	Scalability	Fidelity	Distributed	Dynamical
Graph theory and complex network	High	High	Low	High	Low
FSM, Petri net, and network attack	High	Low	High	Low	High
Control-based	High	Low	Low for cyber, High for power	High	High
Correlation matrix	High	High	Low	Low	High
Probabilistic	Low	Low	Low	–	Low
Variable structure	Low	Low	Low	–	–
Cellular automata	Low	Low	High	–	Low

and analysis. This requires the system model to support the computational capabilities at the edges of a system, instead of using a centralized or hierarchical architecture, while also modeling the necessary communication infrastructure to enable this transition. In addition, because of the size of the systems that need to be studied in greater detail with high fidelity, it is essential that the modeling paradigm supports a distributed solution mechanism by either dividing the problem into multiple smaller subproblems or enabling parallel computations using high-performance computing techniques.

For autonomous systems, it is essential that the model supports more complex computations, both at the grid edge and in centralized/hierarchical deployments, while also modeling the underlying communication infrastructure with high fidelity to better understand interdependencies. Increased autonomy comes with an increased risk surface to cyberattacks because there are higher numbers of controllers and attack points for malicious actors. The CPPS model not only needs to be able to accommodate the attack vectors but also must be capable of demonstrating the effectiveness of the security and mitigation mechanisms deployed.

D. FUTURE DIRECTIONS

Because of the importance of CPPS modeling in various technical and socioeconomic environments, some emerging research directions should be addressed. These include resilience, big data, cloud computing, DER market participation, and technology advancements.

From the CPPS modeling perspective, several studies have provided insightful contributions, as follows. In [134], some criteria were suggested to provide a reliable and robust model of CPPS, including structural properties, scalability, validation, and model aggregation. The structural properties describe the hybrid nature of continuous dynamic power systems and discrete static cyber system. Also, component reflectivity should be maintained to improve the modularity of the model. The authors of [38] identified a few potential criteria to develop secure control algorithms of CPS, including: (1) designing robust control and estimation algorithms considering realistic attack models from a security point of view, (2) developing approaches that estimate the indicators of the quality of service and the integrity of the communication network based on available network data, (3) combining physical and analytical redundancies with security principles to adapt the system operation during an attack, and (4) including trust management schemes with different components of CPS. Also, some potential solutions for improved CPPS modeling include hybrid system modeling and simulation, heterogeneous and concurrent computational models, and functionality-architecture joint models [137].

The severe impact of extreme weather events calls for comprehensive resilience-based studies of CPPS. Because conventional $N-1$ or even $N-2$ contingencies are not sufficient in very tight operating conditions, the interoperability features and characteristics of CPPS might yield better system performance for $N-k$ (i.e., $k>1$) contingencies. Also, cyber resilience evaluation and enhancement methods have become a necessity. Further intensive analysis is still required to assess simultataneous and coordinated cyberattacks against multiple targets in CPPS. This also calls for introducing resilience metrics to measure and assess the performance of CPPS during severe events.

The rapid growth in integrating intelligent systems into conventional power system components has resulted in exponential increases in data sizes and rates. Also, the large amounts of data transferred from PMUs has pushed toward using data mining techniques for improved monitoring and control of CPPS. Developing a CPPS control strategy that has the capability to organize, manage, analyze, and assess the spatiotemporal-based big data has become a necessity. Data fusion approaches are being studied to overcome data problems and to improve knowledge extraction for enhanced observability.

With the issuing of FERC Order 2222 and allowing energy participation from distributed energy resources, a few emerging factors and actions are required to be addressed. This includes incorporating the role of DER aggregators and residential energy consumers in communication and cyber systems and conducting cybersecurity assessment analysis against the induced vulnerabilities in CPPS from DER aggregators. The impact of integrating renewable energy sources and electric vehicles on CPPS still requires further investigation under the cyber-physical security framework to achieve cyber-physical transactive energy systems.

One of the biggest challenges of CPPS modeling is the fast aging of the developed model. Operation and planning engineers often update power grid information several times per year. It is time-consuming to repeat the whole modeling process for every update in the original CPPS model;

therefore, it is more efficient to have a fast and efficient way to update the developed CPPS model based on new data. This can be achieved by creating and leveraging match-and-compare algorithms in different tools and platforms.

Developing and building test beds for CPPS has gained significant interest during the last decade. These simulation test beds have shown convenient platforms in many applications, including impact analysis of cyberattacks on power systems, vulnerability assessments of CPPS against single or coordinated cyberattacks, and hardware-in-the-loop testing and simulations; however, the capability to study large-scale CPPS on these test beds is still very limited. Though co-simulation techniques have shown a potential solution, specifically as applied to power systems, efforts are still required to validate their adaptability for CPPS. Also, building an integrated model of CPPS considering the behavioral characteristics of all components and the sophisticated self-adaptability of both cyber and physical systems will provide a more experimental realistic significance. Most existing test beds focus on a single CPPS domain, giving less interest to multi-perspective domains.

IX. CONCLUSION

This paper provided a critical review on current practices of CPPS characteristics and an up-to-date survey on cyber-physical modeling techniques. A thorough investigation of CPPS modeling methods, including the strengths and limitations of each approach, has been provided. Also, a qualitative evaluation framework was proposed and used to measure the capability of each model to capture CPPS characteristics. Further, this paper identified research gaps and associated challenges, proposed potential solutions, and provided future directions for developing CPPS models considering the evolving autonomous and distributed environments. Note that this paper highlights only some typical research work. The work presented in this paper is intended to contribute toward the development of realistic CPPS models with high accuracy, scalability, fidelity, and distributed and dynamical features. Also, comprehensive modeling of CPPS components and dependencies between and within the system is a necessary step toward achieving a smart grid concept with improved reliability, resilience, security, and sustainability.

ACKNOWLEDGMENT

The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

REFERENCES

[1] N. Bhusal, M. Abdelmalak, M. Kamruzzaman, and M. Benidris, "Power system resilience: Current practices, challenges, and future directions," *IEEE Access*, vol. 8, pp. 18064–18086, 2020.

[2] M. M. Rana, W. Xiang, and E. Wang, "Smart grid state estimation and stabilisation," *Int. J. Elect. Power Energy Syst.*, vol. 102, pp. 152–159, Nov. 2018.

[3] X. Guillaud, M. O. Faruque, A. Teninge, A. H. Hariri, L. Vanfretti, M. Paolone, V. Dinavahi, P. Mitra, G. Lauss, C. Dufour, and P. Forsyth, "Applications of real-time simulation technologies in power and energy systems," *IEEE Power Energy Technol. Syst. J.*, vol. 2, no. 3, pp. 103–115, Sep. 2015.

[4] V. Sultan and B. Hilton, "A spatial analytics framework to investigate electric power-failure events and their causes," *ISPRS Int. J. Geo-Inf.*, vol. 9, no. 1, p. 54, Jan. 2020.

[5] B. Obama. (Feb. 12, 2013). *Presidential Policy Directive 21—Critical Infrastructure Security and Resilience*. Whitehouse.gov. Accessed: Sep. 19, 2022. [Online]. Available: https:// obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[6] Q. Li, S. Meng, S. Zhang, M. Wu, J. Zhang, M. T. Ahvanooey, and M. S. Aslam, "Safety risk monitoring of cyber-physical power systems based on ensemble learning algorithm," *IEEE Access*, vol. 7, pp. 24788–24805, 2019.

[7] S. Sen and P. Pang, "Architectural modeling and cybersecurity analysis of cyber-physical systems-a technical review," *Int. Res. J. Eng. Technol.*, vol. 5, no. 12, pp. 56–2395, 2018.

[8] 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. 151019–151064, 2020.

[9] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electr. Power Syst. Res.*, vol. 163, pp. 396–412, Oct. 2018.

[10] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, J. Zhao, and V. Terzija, "A specialized review on outlook of future cyber-physical power system (CPPS) testbeds for securing electric power grid," *Int. J. Electr. Power Energy Syst.*, vol. 136, Mar. 2022, Art. no. 107720.

[11] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley, and J. Barnett, "O vulnerability and resilience of cyber-physical power systems: A review," *IEEE Syst. J.*, vol. 16, no. 2, pp. 1–12, Jun. 2021.

[12] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, Y. Zhao, J. A. Ramos-Ruiz, P. N. Enjeti, P. R. Kumar, and L. Xie, "A review of current research trends in power-electronic innovations in cyber-physical systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5146–5163, Oct. 2021.

[13] B. Kitchenham, S. Pfleeger, L. Pickard, P. Jones, D. Hoaglin, K. El Emam, and J. Rosenberg, "Preliminary guidelines for empirical research in software engineering," *IEEE Trans. Softw. Eng.*, vol. 28, no. 8, pp. 721–734, Aug. 2002.

[14] M. Bessani, R. Z. Fanucchi, A. C. C. Delbem, and C. D. Maciel, "Impact of operators' performance in the reliability of cyber-physical power distribution systems," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 11, pp. 2640–2646, Aug. 2016.

[15] T. Facchinetti and M. L. Della Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 689–698, Nov. 2011.

[16] 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, 2020, pp. 489–497.

[17] 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, Germany: Springer, 2008, pp. 46–54.

[18] J. Mitra, M. Benidris, and N. Nguyen, "Dynamic contingency analysis and remedial action tools for secure electric cyber-physical systems," *Cyber-Phys.-Social Syst. Constructs Electr. Power Eng.*, vol. 2, p. 97, Oct. 2016.

[19] Y. Han, C. Guo, S. Ma, and D. Song, "Modeling cascading failures and mitigation strategies in PMU based cyber-physical power systems," *J. Modern Power Syst. Clean Energy*, vol. 6, no. 5, pp. 944–957, Sep. 2018.

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

[21] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.
[22] 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*. Berlin, Germany: Springer, 2015, pp. 43–74.
[23] V. Aravinthan, T. Balachandran, M. Ben-Idris, W. Fei, M. Heidari-Kapourchali, A. Hettiarachchige-Don, J. N. Jiang, H. Lei, C.-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 *Proc. IEEE Int. Conf. Probabilistic Methods Appl. to Power Syst. (PMAPS)*, Jun. 2018, pp. 1–7.
[24] Q. Zhu, C. Rieger, and T. Basar, "A hierarchical security architecture for cyber-physical systems," in *Proc. 4th Int. Symp. Resilient Control Syst.*, Aug. 2011, pp. 15–20.
[25] Q. Zhu, *Multilayer Cyber-Physical Security and Resilience for Smart Grid*. Cham, Switzerland: Springer, 2019, pp. 225–239.
[26] 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," *Appl. Comput. Informat.*, vol. 14, no. 1, pp. 17–27, Jan. 2018.
[27] B. Falahati and Y. Fu, "A study on interdependencies of cyber-power networks in smart grid applications," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8.
[28] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Berlin, Germany: Springer, 2007, pp. 54–67.
[29] M. Heidari-Kapourchali and V. Aravinthan, "Component reliability evaluation in the presence of smart monitoring," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2013, pp. 1–6.
[30] H. Lei and C. Singh, "Non-sequential Monte Carlo simulation for cyber-induced dependent failures in composite power system reliability evaluation," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1064–1072, May 2017.
[31] 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, Jul. 2015.
[32] Z. Qu, Y. Dong, N. Qu, L. Wang, Y. Li, Y. Zhang, and S. Mugemanyi, "Survivability evaluation method for cascading failure of electric cyber physical system considering load optimal allocation," *Math. Problems Eng.*, vol. 2019, pp. 1–15, Jul. 2019.
[33] J. Sztipanovits and G. Karsai, "Model-integrated computing," *Computer*, vol. 30, no. 4, pp. 110–111, Apr. 1997.
[34] B. Selic, "The pragmatics of model-driven development," *IEEE Softw.*, vol. 20, no. 5, pp. 19–25, Sep. 2003.
[35] H. Fan, M. Ni, L. Zhao, and M. Li, "Review of cyber physical system and cyber attack modeling," in *Proc. 12th IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Sep. 2020, pp. 1–5.
[36] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Automat. Sinica*, vol. 9, no. 5, pp. 784–800, May 2022.
[37] I. Graja, S. Kallel, N. Guermouche, S. Cheikhrouhou, and A. H. Kacem, "A comprehensive survey on modeling of cyber-physical systems," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 15, p. e4850, 2020.
[38] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495–500.
[39] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.
[40] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.
[41] M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, and J. Schröder, *Diagnosis and Fault-Tolerant Control*, vol. 2. Berlin, Germany: Springer, 2006.
[42] R. Olfati-Saber, "Distributed Kalman filter with embedded consensus filters," in *Proc. 44th IEEE Conf. Decis. Control*, Dec. 2005, pp. 8179–8184.
[43] J. Hu, J. Yu, J. Cao, M. Ni, and W. Yu, "Topological interactive analysis of power system and its communication module: A complex network approach," *Physica A, Stat. Mech. Appl.*, vol. 416, pp. 99–111, Dec. 2014.
[44] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 451–463, Mar. 2014.
[45] A. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Anal.*, vol. 26, no. 4, pp. 955–969, 2006.
[46] V. Gol'dshtein, G. A. Koganov, and G. I. Surdutovich, "Vulnerability and hierarchy of complex networks," 2004, *arXiv:cond-mat/0409298*.
[47] M. Ouyang and Z. Wang, "Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis," *Rel. Eng. Syst. Saf.*, vol. 141, pp. 74–82, Sep. 2015.
[48] A. D. González, L. Dueñas-Osorio, M. Sánchez-Silva, and A. L. Medaglia, "The interdependent network design problem for optimal infrastructure system restoration," *Comput.-Aided Civil Infrastruct. Eng.*, vol. 31, no. 5, pp. 334–350, May 2016.
[49] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.
[50] Y. Zhang and O. Yagan, "Robustness of interdependent cyber-physical systems against cascading failures," *IEEE Trans. Autom. Control*, vol. 65, no. 2, pp. 711–726, Feb. 2020.
[51] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," in *Proc. IEEE 8th Conf. Ind. Electron. Appl. (ICIEA)*, Jun. 2013, pp. 1023–1028.
[52] J. Zhou, S. Tsianikas, D. W. Coit, and F. A. Felder, "Resilience based optimization for western U.S. transmission grid against cascading failures," 2019, *arXiv:1912.02887*.
[53] J. Beyza, E. Garcia-Paricio, and J. Yusta, "Applying complex network theory to the vulnerability assessment of interdependent energy infrastructures," *Energies*, vol. 12, no. 3, p. 421, Jan. 2019.
[54] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, p. 87, Jan. 2017.
[55] Z. Dong, M. Tian, and L. Ding, "A framework for modeling and structural vulnerability analysis of spatial cyber-physical power systems from an attack–defense perspective," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1369–1380, Mar. 2021.
[56] H. Tu, Y. Xia, J. Wu, and X. Zhou, "Robustness assessment of cyber–physical systems with weak interdependency," *Phys. A, Stat. Mech. Appl.*, vol. 522, pp. 9–17, May 2019.
[57] M. Parandehgheibi, E. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2014, pp. 242–247.
[58] Y.-N. Wang, Z.-Y. Lin, X. Liang, W.-Y. Xu, Q. Yang, and G.-F. Yan, "On modeling of electrical cyber-physical systems considering cyber security," *Frontiers Inf. Technol. Electron. Eng.*, vol. 17, no. 5, pp. 465–478, May 2016.
[59] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *Int. J. Secur. Netw.*, vol. 6, no. 1, pp. 2–13, 2011.
[60] G. Wu, M. Li, and Z. S. Li, "Resilience-based optimal recovery strategy for cyber–physical power systems considering component multistate failures," *IEEE Trans. Rel.*, vol. 70, no. 4, pp. 1510–1524, Dec. 2021.
[61] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, Mar. 2020.
[62] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber–physical energy systems for distributed sensing and control," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.
[63] Y. Weng, R. Negi, and M. D. Ilic, "Probabilistic joint state estimation for operational planning," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 601–612, Jan. 2019.
[64] P. Huang, Y. Wang, and G. Yan, "Vulnerability analysis of electrical cyber physical systems using a simulation platform," in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2017, pp. 489–494.
[65] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[66] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 3–13, Jan. 2014.

[67] S. Soltan, M. Yannakakis, and G. Zussman, "Power grid state estimation following a joint cyber and physical attack," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 499–512, Mar. 2018.

[68] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5405–5415, Sep. 2019.

[69] X. Wang, M. Zhu, D. Bo, P. Cui, C. Shi, and J. Pei, "AM-GCN: Adaptive multi-channel graph convolutional networks," in *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2020, pp. 1243–1253.

[70] K. Zhou, Q. Song, X. Huang, D. Zha, N. Zou, and X. Hu, "Multi-channel graph neural networks," in *Proc. 29th Int. Joint Conf. Artif. Intell.*, Jul. 2020, pp. 1352–1358.

[71] W. Liao, B. Bak-Jensen, J. R. Pillai, Y. Wang, and Y. Wang, "A review of graph neural networks and their applications in power systems," *J. Modern Power Syst. Clean Energy*, vol. 10, no. 2, pp. 345–360, 2022.

[72] S. Cvijic and M. Ilic, "On limits to the graph-theoretic approaches in the electric power systems," in *Proc. North Amer. Power Symp.*, Aug. 2011, pp. 1–6.

[73] S. Korotunov, G. Tabunshchyk, K. Henke, and H.-D. Wuttke, "Analysis of the verification approaches for the cyber-physical systems," *Comput. Model. Intell. Syst.*, vol. 2353, pp. 950–961, Aug. 2019.

[74] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*. Cambridge, MA, USA: MIT Press, 2016.

[75] W. Li, L. Xie, Z. Deng, and Z. Wang, "False sequential logic attack on SCADA system and its physical impact analysis," *Comput. Secur.*, vol. 58, pp. 149–159, May 2016.

[76] K. Schneider, C.-C. Liu, and J. P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.

[77] O. Gursesli and A. A. Desrochers, "Modeling infrastructure interdependencies using Petri nets," in *Proc. IEEE Int. Conf. Syst., Man Cybern. Conf. Theme Syst. Secur. Assurance (SMC)*, Oct. 2003, pp. 1506–1512.

[78] H. Hu, J. Yu, Z. Li, J. Chen, and H. Hu, "Modeling and analysis of cyber–physical system based on object-oriente generalized stochastic Petri net," *IEEE Trans. Rel.*, vol. 70, no. 3, pp. 1271–1285, Sep. 2021.

[79] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[80] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sep. 2015.

[81] X. Liu, J. Zhang, and P. Zhu, "Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory," *Int. J. Crit. Infrastruct. Protection*, vol. 16, pp. 13–25, Mar. 2017.

[82] J. Qian, P. Shi, and Q. Mu, "Based on random game Petri net model CPS risk assessment and defense decision of distribution network," in *Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE)*, Mar. 32021, pp. 764–767.

[83] Y. Xu and R. Fu, "Petri net-based power CPS network attack and impact modeling," in *Proc. 5th IEEE Int. Conf. Cloud Comput. Intell. Syst. (CCIS)*, Nov. 2018, pp. 1107–1110.

[84] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[85] P. A. Khand, "System level security modeling using attack trees," in *Proc. 2nd Int. Conf. Comput., Control Commun.*, Feb. 2009, pp. 1–6.

[86] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594, 2007.

[87] 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 Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015.

[88] F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, and Y. Gao, "Security analysis on cyber-physical system using attack tree," in *Proc. 9th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2013, pp. 429–432.

[89] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010.

[90] W. Yufei, G. Kunlun, Z. Ting, and Q. Jian, "Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph," *Proc. CSEE*, vol. 36, no. 6, pp. 1490–1499, 2016.

[91] A. T. Al Ghazo, M. Ibrahim, H. Ren, and R. Kumar, "A2G2 V: Automatic attack graph generation and visualization and its applications to computer and SCADA networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 10, pp. 3488–3498, Oct. 2020.

[92] 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 Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

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

[94] P. Bogdan and M. Pedram, "Toward enabling automated cognition and decision-making in complex cyber-physical systems," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–4.

[95] D. B. Rawat, J. J. Rodrigues, and I. Stojmenovic, *Cyber-Physical Systems From Theory to Practice*. Boca Raton, FL, USA: CRC Press, 2015.

[96] T. Samad and A. M. Annaswamy, "Controls for smart grids: Architectures and applications," *Proc. IEEE*, vol. 105, no. 11, pp. 2244–2261, Nov. 2017.

[97] L. Xie and M. D. Ilic, "Module-based modeling of cyber-physical power systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 513–518.

[98] M. D. Ilic, "Toward a unified multi-layered modeling and simulation paradigm for electric energy systems," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[99] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.

[100] E. Hammad, A. Farraj, and D. Kundur, "On cyber-physical coupling and distributed control in smart grids," *IEEE Trans. Ind. Informat.*, vol. 15, no. 8, pp. 4418–4429, Aug. 2019.

[101] A. Pahwa, S. A. DeLoach, B. Natarajan, S. Das, A. R. Malekpour, S. M. S. Alam, and D. M. Case, "Goal-based holonic multiagent system for operation of power distribution systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2510–2518, Sep. 2015.

[102] W. Li, Y. Li, C. Chen, Y. Tan, Y. Cao, M. Zhang, Y. Peng, and S. Chen, "A full decentralized multi-agent service restoration for distribution network with DGs," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1100–1111, Mar. 2020.

[103] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436–447, Apr. 2017.

[104] P. Wang and M. Govindarasu, "Multi-agent based attack-resilient system integrity protection for smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3447–3456, Jul. 2020.

[105] A. Chakrabortty, "Wide-area damping control of power systems using dynamic clustering and TCSC-based redesigns," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1503–1514, Sep. 2012.

[106] A. M. Annaswamy, D. Soudbakhsh, R. Schneider, D. Goswami, and S. Chakraborty, "Arbitrated network control systems: A co-design of control and platform for cyber-physical systems," in *Control of Cyber-Physical Systems*. Berlin, Germany: Springer, 2013, pp. 339–356.

[107] A. Annaswamy, S. Chakraborty, D. Soudbakhsh, D. Goswami, and H. Voit, "The arbitrated networked control systems approach to designing cyber-physical systems," *IFAC Proc. Volumes*, vol. 45, no. 26, pp. 174–179, Sep. 2012.

[108] D. Soudbakhsh, L. T. X. Phan, A. M. Annaswamy, and O. Sokolsky, "Co-design of arbitrated network control systems with overrun strategies," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 128–141, Mar. 2018.

[109] D. Soudbakhsh, A. Chakrabortty, and A. M. Annaswamy, "A delay-aware cyber-physical architecture for wide-area control of power systems," *Control Eng. Pract.*, vol. 60, pp. 171–182, Mar. 2017.

[110] A. M. Annaswamy, A. Hussainy, A. Chakraborttyz, and M. Cvetkovic, "Foundations of infrastructure-CPS," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2016, pp. 2649–2664.

[111] A. Kiani and A. Annaswamy, "Distributed hierarchical control for renewable energy integration in a smart grid," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8.
[112] P. Pauli, S. M. Dibaji, A. M. Annaswamy, and A. Chakrabortty, "Optimal delay assignment in delay-aware control of cyber-physical systems: A machine learning approach," in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, Dec. 2019, pp. 4583–4588.
[113] Y. Xue, M. Li, J. Luo, M. Ni, Q. Chen, and T. Yi, "Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix," *Dianli Xitong Zidonghua/Automat. Electr. Power Syst.*, vol. 42, pp. 11–19, Jan. 2018.
[114] M. Li, M. Ni, Y. Xue, X. Chen, and W. Ding, "Hybrid calculation architecture of cyber physical power system based on correlative characteristic matrix model," in *Proc. IEEE 8th Annu. Int. Conf. CYBER Technol. Autom., Control, Intell. Syst. (CYBER)*, Jul. 2018, pp. 584–588.
[115] 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, Sep. 2014.
[116] H. Lei and C. Singh, "Power system reliability evaluation considering cyber-malfunctions in substations," *Electr. Power Syst. Res.*, vol. 129, pp. 160–169, Dec. 2015.
[117] H. Ye, W. Gao, Q. Mou, and Y. Liu, "Iterative infinitesimal generator discretization-based method for eigen-analysis of large delayed cyber-physical power system," *Electr. Power Syst. Res.*, vol. 143, pp. 389–399, Feb. 2017.
[118] D. Shi, R. J. Elliott, and T. Chen, "On finite-state stochastic modeling and secure estimation of cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 65–80, Jan. 2017.
[119] Y. Han, Y. Wen, C. Guo, and H. Huang, "Incorporating cyber layer failures in composite power system reliability evaluations," *Energies*, vol. 8, no. 9, pp. 9064–9086, Aug. 2015.
[120] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012.
[121] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014.
[122] B. R. Prusty and D. Jena, "A critical review on probabilistic load flow studies in uncertainty constrained power systems with photovoltaic generation and a new approach," *Renew. Sustain. Energy Rev.*, vol. 69, pp. 1286–1302, Mar. 2017.
[123] M. Eliassi, A. K. Dashtaki, H. Seifi, M. Haghifam, and C. Singh, "Application of Bayesian networks in composite power system reliability assessment and reliability-based analysis," *IET Gener., Transmiss. Distrib.*, vol. 9, no. 13, pp. 1755–1764, Oct. 2015.
[124] W. Liu, Z. Lin, L. Wang, Z. Wang, H. Wang, and Q. Gong, "Analytical reliability evaluation of active distribution systems considering information link failures," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4167–4179, Nov. 2020.
[125] P. Zhang, Y. Yuan, Z. Wang, and C. Sun, "A hierarchical game approach to the coupled resilient control of CPS against Denial-of-Service attack," in *Proc. IEEE 15th Int. Conf. Control Automat. (ICCA)*, Jul. 2019, pp. 15–20.
[126] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.
[127] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, "A colonel Blotto game for interdependence-aware cyber-physical systems security in smart cities," in *Proc. 2nd Int. Workshop Sci. Smart City Oper. Platforms Eng.*, 2017, pp. 7–12.
[128] Y. Guo, Y. Gong, L. L. Njilla, and C. A. Kamhoua, "A stochastic game approach to cyber-physical security with applications to smart grid," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 33–38.
[129] F. Miao and Q. Zhu, "A moving-horizon hybrid stochastic game for secure control of cyber-physical systems," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 517–522.
[130] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.
[131] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.
[132] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.
[133] X. Ye, F. Wen, J. Shang, and Y. He, "Propagation mechanism of cyber physical security risks in power systems," *Power Syst. Technol.*, vol. 39, no. 11, pp. 3072–3079, 2015.
[134] A. Chakrabortty and A. Bose, "Smart grid simulations and their supporting implementation methods," *Proc. IEEE*, vol. 105, no. 11, pp. 2220–2243, Nov. 2017.
[135] V. Venkataramanan, P. Wang, A. Srivastava, A. Hahn, and M. Govindarasu, "Interfacing techniques in testbed for cyber-physical security analysis of the electric power grid," in *Proc. Workshop Model. Simul. Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2017, pp. 1–6.
[136] M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," in *Proc. IEEE/PES Power Syst. Conf. Exposit.*, Mar. 2009, pp. 1–6.
[137] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2011.
[138] B. D. Kroposki, E. Dall-Anese, A. Bernstein, Y. Zhang, and B. S. Hodge. (2017). *Autonomous Energy Grids: Preprint*. [Online]. Available: https://www.osti.gov/biblio/1399662

MICHAEL ABDELMALAK (Student Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Alexandria, Egypt, in 2012, and the M.Sc. degree in electrical engineering and the M.B.A. degree in strategic management and accounting from The German University in Cairo, Cairo, Egypt, in 2017 and 2019, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the University of Nevada, Reno, USA. He was an Assistant Lecturer with the Department of Information and Electrical Engineering, The German University in Cairo. His research interests include power system reliability, stability, resilience, renewable energy resources, optimization, and reinforcement learning.

VENKATESH VENKATARAMANAN (Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering and computer science (EECS) from Washington State University, Pullman, WA, USA, in 2015 and 2019, respectively. He was a Postdoctoral Research Associate at the Massachusetts Institute of Technology, from 2019 to 2021. He is currently a Research Engineer working in cybersecurity at the National Renewable Energy Laboratory (NREL). His research interests include cyber-physical system resilience, smart grid modeling, analysis, and operation, electricity markets, and cyber-physical testbeds.

RICHARD MACWAN (Member, IEEE) received the master's degree in electrical engineering with a specialization in power systems from the New York University Polytechnic Institute. He is currently a Senior Researcher with the National Renewable Energy Laboratory (NREL), Energy Security and Resilience Center, Cybersecurity Science and Simulation Group. His research interests include the development of game theory and physics-based algorithms for increasing the cyber resilience of power grids, leveraging formal methods for OT security, and development of realistic cyber-physical test bed environments for the assessment of such technologies.