Electric Power Systems Research 163 (2018) 396–412

Contents lists available at ScienceDirect

Electric Power Systems Research

journal homepage: www.elsevier.com/locate/epsr

Cyber–physical interactions in power systems: A review of models, methods, and applications

Libao Shi*, Qiangsheng Dai, Yixin Ni

National Key Laboratory of Power System in Shenzhen, Graduate School at Shenzhen, Tsinghua University, Shenzhen, China

ARTICLE INFO

Keywords:
Cyber–physical power system
Interdependent network
Infrastructure vulnerability
Cyberattack
Network security
Failure propagation

ABSTRACT

Owing to the advanced metering infrastructure and communication networks, modern power systems have gradually evolved into multidimensional heterogeneous cyber–physical power systems (CPPSs) with continuous coupling interactions between cyber systems and power systems. The rapid development of the cyber infrastructure is leading to a new era of high-level intelligence revolution; however, currently, CPPSs face newly emerging problems such as stability, vulnerability, reliability, and security. Exploring and resolving the nature of these problems while formulating corresponding solutions will depend on the modeling methods and investigation of interaction mechanisms in CPPSs. Accordingly, this study aims to systematically summarize the interaction models and corresponding solution methods in the current CPPS research. First, the interactive features of CPPSs are discussed, and their modeling mechanisms are elaborately reviewed and summarized from the viewpoints of graphic, mechanism, probability, and simulation. In particular, the applicability and characteristics of these models pertinent to specific research issues are discussed technically. Next, the crucial problem-solving strategies are analyzed and concluded comprehensively. Finally, the cutting-edge CPPS research in China is discussed, and the potential research directions in this field are highlighted.

1. Introduction

Exploiting the large-scale sensing measurement systems and more complicated information communication networks, power systems can optimize their operations continually to ensure a safe, stable, and reliable power supply. With the continuous development of power systems, the scale of cyber networks has increased enormously, accompanied by emergence of a large number of intelligent electronic devices (IEDs) deployed in power systems. Meanwhile, the promotion of energy internet (EI) enables increasing external information to influence the control and decision of power systems directly or indirectly through various business channels. In this situation, modern power systems are no longer power infrastructure networks in the conventional sense. Instead, they have gradually evolved into multidimensional heterogeneous complex cyber–physical power systems (CPPSs) coupled by the interaction between cyber networks and power systems.

The powerful functions of cyber systems in CPPSs provide significant technical support for the observability and controllability of power systems. However, the strong coupling of cyber–physical systems makes the performance of cyber systems significantly affect the operating characteristics of physical power systems. Incorporating electrical power infrastructure, information communication technology and computational intelligence, the CPPSs covers all the key domains in power systems including electricity generation, electric power transmission, electric power transformation, electric power distribution, electric power consumption and electricity selling, as shown in Fig. 1. Meanwhile, there are three tiers of CPPS structure considering the information transfer, namely component tier, communication tier and function tier. These aforementioned tiers are abstracted to tier 1, tier 2 and tier 3 respectively as shown in Fig. 1. The tier 1 mainly consists of primary equipment (i.e. generator, transformer, transmission line, circuit breaker, etc.), secondary equipment (i.e. protection relay, sensor, actuator, etc.), and electric appliances, which are all interconnected in a specific topology. The secondary sensor devices would gather the operational information from primary equipment and transmit this information to local controllers, such as local feeder automation controller. This controller may send certain control instruction to actuators that would affect primary equipment for the purpose of optimization or protection. This process forms the first level of interaction in CPPSs. For example, the local feeder automation system, located in the electric power distribution domain shown in Fig. 1, utilizes remoter terminal units to monitor the distribution lines and isolate fault areas that may minimize outage duration. In Ref. [1], authors have investigated how time delay of transmitting measurement data of generators affect the

* Corresponding author.
E-mail address: shilb@sz.tsinghua.edu.cn (L. Shi).

https://doi.org/10.1016/j.epsr.2018.07.015
Received 9 April 2018; Received in revised form 21 June 2018; Accepted 11 July 2018
Available online 23 July 2018
0378-7796/

Nomenclature

AGC	Automatic generation control
AM	Analytical model
AMI	Advanced metering infrastructure
CN	Complex network
CPN	Colored Petri net
CPPS	Cyber–physical power system
CT	Communication terminal
DA	Distribution automation
DER	Distributed energy resource
DMS	Distribution management system
DR	Demand response
DST	Dynamic system theory
EI	Energy internet
EMS	Energy management system
EV	Electric vehicle
FDI	False data injection
FSM	Finite state machine
GM	Game-theoretic model
GT	Graph theory
HS	Hybrid system
IED	Intelligent electronic device
LP	Linear programming
LQR	linear quadratic regulator
MAS	Multi-agent system
MC	Markov chain
MCS	Monte Carlo simulation
MDP	Markov decision process
NA	Network attack
OM	Other model
PDF	Probability density function
PMU	Phasor measurement unit
PN	Petri net
P-Table	Probability table
SA	Substation automation
SCADA	Supervisory control and data acquisition
SCD	State chart diagram
SCPN	Stochastic colored Petri net
SE	State estimation
SMP	Semi-Markov process
SPN	Stochastic Petri net
UM	Uncertainty model
VSS	Variable structure system
ZOH	Zero order hold

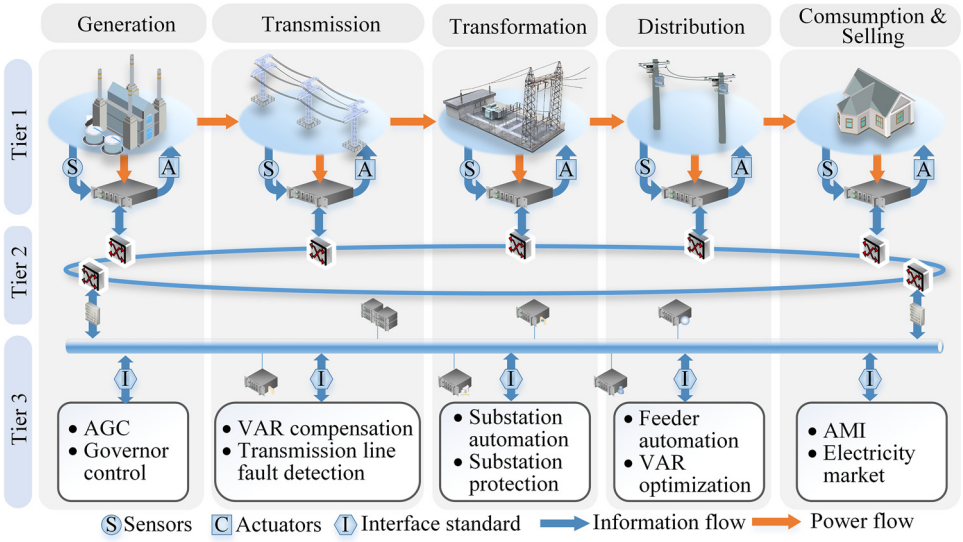

Fig. 1. Structure of CPPSs.

stability of CPPSs. The cascading failure mechanism between cyber system and physical system in the transmission domain is analyzed in Ref. [2]. In Refs. [3,4], the impacts of IED failures and merging unit failures within the substation from the transformation domain on the reliability of composite CPPSs are analyzed.

In the meantime, the acquired information in tier 1 would be transmitted to dispatch master station (or control center) through the communication network in tier 2. Communication architecture that keeps coordination among all components of power systems has always played a crucial role in CPPSs. The commutation technologies (i.e. IEEE 802 series, power line communication, mobile communications, etc.), network traffic, routing mechanism, communication topology would affect communication efficiency and effectiveness, and have further impacts on power systems. This can be considered as the second level of interaction in CPPSs. The authors in Ref. [5] have presented how communication latency jeopardizes the stability of CPPSs in transmission domain. In Ref. [6], the impacts of network traffic between distributed phasor data concentrators on the convergence and accuracy properties of wide-area oscillation monitoring method are investigated.

Finally, all the operational information would be stored and processed in the control center in tier 3. The tier 3 can realize various advanced functions and operational decision-making. There can be multiple stations, and accordingly these stations are interconnected through different topologies. The main elements of master station are web server, communication server, application server, database and human machine interface. Allowing for easier information exchange and interoperability of advanced functions, the information models of each function are integrated into the information bus through the international interface standards. Thus, the calculation and analysis of these functions through the elements of master station can be considered as the third level of interaction in CPPSs. Taking the feeder automation function for example, the integrated feeder automation strategy would implement the optimal instructions that could minimize outage duration and number of switching operations simultaneously. Accordingly, these instructions would be sent to the circuit breakers in tier 1. Obviously, the errors in information modelling, interface for

operation and data processing would directly mislead system operations.

Nowadays, the CPPSs are facing challenges in terms of security and reliability in the aforementioned 3 tiers cyber environments. It should be noted that the internal cyber assets in power systems, such as the IEDs, routers, Ethernet switches, operating systems and business systems, increase the risks from external threats and attacks owing to their own vulnerability. Attackers can exploit the known cyber network vulnerabilities or even previously unknown vulnerabilities to implement coordinated attacks. One major pitfall associated with CPPS interaction is that although cyberattacks cannot directly damage the CPPS infrastructure, the advanced functions of CPPSs could be weakened or destroyed to attain similar physical attack effects, which would further seriously jeopardize the social stability. In 2010, the malicious Stuxnet worm, which was the first worm known to attack SCADA systems, hit the Bushehr Nuclear Power Plant in Iran [7]. In 2014, the Russian hacker group, Dragonfly, used the Havex malware to attack the US and European energy firms [8]. At the end of 2015, there was a cyberattack against critical infrastructure of the Ukrainian power system resulting in power supply outage, which was considered as the largest blackout caused by cyberattacks for the first time in history [9]. In 2016, Israel's electric grid was hit by a malicious cyberattack in which a large number of computers in the power supply system were run offline [10].

Related research has shown that cyber–physical interactions can yield unpredictable cross-system failure propagations. In other words, failures in cyber systems will propagate to physical systems and vice versa, which may lead to cascading failures. Therefore, it is imperative to determine the dynamic behavior and interaction mechanisms of the CPPS systematically and accurately to further improve the controllability and stability of the entire system. Scholars worldwide have conducted extensive research on CPPSs from different perspectives. The early research works mainly focused on how to conduct vulnerability analyses for a CPPS under a cyberattack [11–16]. Given that power system application software is directly or indirectly dependent on real-time operating data of CPPSs, the operating results of other subsystems would be inevitably altered by tampered data, thereby increasing other security issues. Hence, in recent years, an increasing number of scholars have conducted influence and reliability analyses when a power system is under a cyberattack [3,17–19]. In addition, some scholars explored and exploited the methods of identifying cyberattacks from the viewpoint of cyber intrusion and proposed corresponding defense tactics [20–27]. Furthermore, some studies discussed how to effectively improve the stability of CPPSs based on the control point of view [28–31]. Extensive research has shown that the management of a complicated CPPS and the collective behaviors of entire system significantly depend on the tight cyber–physical interactions [32]. However, so far it has been difficult to find a comprehensive literature survey in the study of cyber–physical interactions in power system. This paper aims to systematically review the cyber–physical interactions from viewpoints of modeling mechanism, solution methods and corresponding applications. In particular, the cutting-edge research achievements in this aspect in China are introduced. Some potential future research works are also highlighted.

The rest of the paper is organized as follows. In Section 2, the CPPS interactive models from the perspectives of graphic, mechanism, probability, and simulation are summarized. Section 3 discusses the crucial solution methods for such interactive models and their main applications. In Section 4, the research progress of CPPSs in China is briefly introduced. Finally, the concluding remarks and future work are presented in Section 5.

2. Cyber–physical interaction analysis models

CPPSs can be regarded as the tight integration between cyber systems and power systems at different system scales and levels. These interactions bear the following prominent characteristics:

1. The fusion of network topology and system mechanism. The actual cyber system is composed of massive cyber devices interconnected by different topological communication networks, whereas the power system is an electrical network containing a large number of primary and secondary equipment. The two systems not only bear non-trivial topological features, but also intertwine with each other and follow their specified operating mechanisms. The power systems need to satisfy the operational constraints of power balance, power transmission capacity, and corresponding upper and lower limits, while the cyber systems are requested to comply with the technical requirements, like communication latency and interoperation. The realization of these mechanisms is topology-specific.
2. The combination of continuous and discrete events. The CPPS can be considered as a deeply integrated time-space multidimensional heterogeneous system. The physical power system belongs to a continuous system that has continuous-time behaviors of voltage, current, frequency and power. The cyber system is a typical discrete-state event-driven system that consists of communication network, analysis, and control process aiming to supervise the physical system.
3. The mixture of static and dynamic behaviors. The power system and cyber system have a static topological structure, whereas the power plants, substations and distribution networks have plenty of dynamic components. Internal disturbances occurring in one system will spread to another one through the topological structure and may trigger instability.
4. The inclusion of uncertainties and system decision-making behaviors. The large-scale integration of renewable energy resources with randomness and volatility has undoubtedly imposed uncertainties in power systems. Meanwhile, power devices, power lines, network equipment, and communication lines might experience failure events or cyber-attacks. These situations cannot be precisely predicted to some extent. These increase potential risks for the safe and stable operation of the entire system. In addition, the operational performance of CPPSs heavily depend on the strategy of advanced functions in master station and the decisions made by system operators during control and analysis. In particular, the mitigation decision of coping with unpredictable network attacks (NAs) would determine the stability of system.

Concisely, these aforementioned characteristics complicate the research of cyber–physical interactions in power systems. In order to explore and exploit the impacts of cyber–physical interactions intensively, it is essential to model the CPPS and then make further qualitative analysis and quantitative calculation pertinent to the interactions between power systems and cyber systems. With an extensive and intensive literature review, in this study, the establishment mechanism of a CPPS model is classified into the following four categories according to the different starting points of the research. The first category is summarized from the viewpoint of graphical modeling. Based on the graph theory (GT) and complex network (CN) theory, the CPPS can be converted into a type of network structure, and then the inner relationship between the network topology parameters and system behavior can be analyzed. Moreover, the dynamic behavior of the system and the cyberattack process can be described by finite-state-machine (FSM) models, Petri net (PN) models, attack tree models, attack graph models, and state transition diagrams, which belong to graphical models. The second category is defined as the system mechanism analysis, that is, the system dynamics are described by using differential algebraic equations to analyze the relationship between the cyber system failures and the state of the power system in principle. Additionally, a multi-agent system (MA) architecture is used to make a system security assessment and stability control specifically. The third category is explained from the probability point of view. The failure

probabilities of the cyber and physical components are considered separately, and the predictability of cyberattacks is analyzed as well. Furthermore, the cyberattacks and the corresponding system countermeasures are treated as attack-mitigation game models from the viewpoint of decision-making. The fourth category aims to build a simulation model based on experimental analysis.

The first three models can be classified according to graphic dimension, mechanism dimension, and probability dimension. Based on this classification, existing CPPS pertinent to modeling methods could be represented by the three-dimensional diagram as shown in Fig. 2. Researchers can also propose comprehensive modeling schemes according to their research interests and the characteristics of the models. For example, in Ref. [26], the dynamic system theory (DST)-based model and the game-theoretic model (GM) are combined to build a cyber–physical interaction model for security analysis in smart grids. In Ref. [33], a combination of the GT-based model and the DST-based model is adopted to study the influence of cyberattacks. In Ref. [34], a probabilistic PN and a mixed-strategy game are combined to establish the model of cyber–physical attacks. In Ref. [35], the cyber system model is built based on the GT method, and at the same time, the power system model is established based on the analytical model (AM) to investigate the cyberattack countermeasures. A stochastic game-theoretic approach is proposed in Ref. [36] to analyze how to protect the system against coordinated attacks. Finally, the validity and efficiency of proposed models could be verified by using the fourth simulation models following the existing international standards. On the other hand, one can also directly simulate the working scenarios of CPPS.

2.1. Graphical modeling

Graphical modeling can intuitively visualize the independent relationships between different variables and quantitatively analyze operating state transition of system. To utilize these models, it is imperative to figure out the definition of each graphical symbol and the relationship representing actual physical and cyber scenarios. Then the specific relationship base on the theories of corresponding models can be discussed as follows.

2.1.1. Graph theory based models

In power systems, the electrical primary equipment is connected through the transmission line, and the cyber system is constructed by the cyber components through the communication network. Therefore, the most intuitive way of studying the CPPS internal binary relations would be from the viewpoint of GT.

Based on GT, without loss of generality, the power plant, substation, and load are simulated as vertices V_p, and the transmission lines are regarded as edges E_p. Assuming for simplicity that the specific topologies of the electrical main wiring in the power plant, substation, and distribution network are negligible, the power system can be described as a directed sparsely connected graph with n nodes and k directed edges $G_p = (V_p, E_p)$ [2,37,38]. Furthermore, some studies are carried out with substation nodes ignored [39].

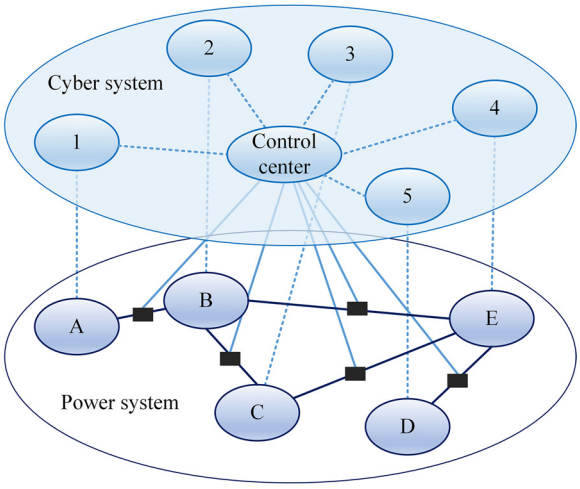

Fig. 3. The interaction relationship in a regional CPPS.

Similarly, the cyber components (such as terminal equipment, routers, and facilities for control center) are simulated as vertices V_c, and the wired or wireless communication lines are regarded as edges E_c. Then, the cyber system can be described as a directed sparsely connected graph with m nodes and g directed edges $G_c = (V_c, E_c)$ [2,37,40].

In order to achieve observability and controllability of the power system, it is assumed that each power equipment (power node) is equipped with a communication terminal (CT) or cyber node, which is used to transmit the state information of the power equipment to the control center through the routers and switches. Once the information is parsed by the control center, the corresponding control commands will be sent to the specific power equipment via routers. A prime example can be seen in Fig. 3 [2]. The nodes in power system layer can represent generators, loads or substations. The black rectangle denotes circuit breakers equipped with cyber devices. The information of power nodes is gathered by cyber nodes in cyber system layer and transmitted to control center.

Given that a one-to-one relationship between the power equipment

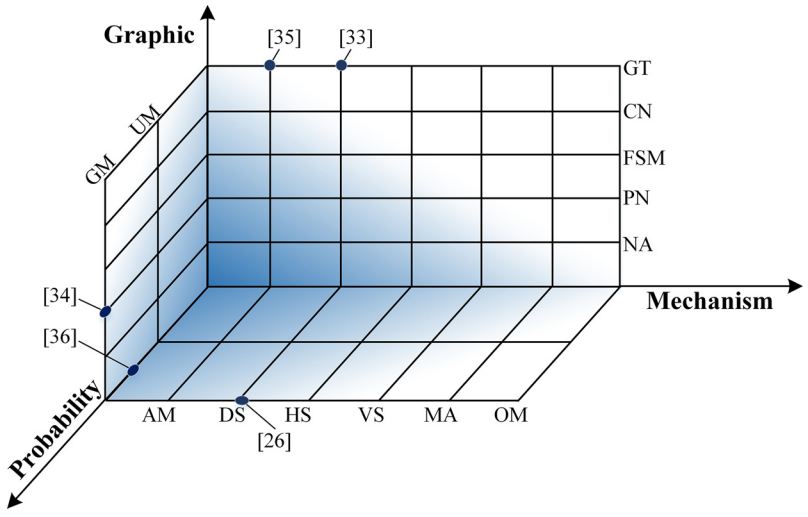

Fig. 2. Three-dimensional diagram of CPPS models.

and communication terminal exists, a CT failure will lead to a malfunction of power node and vice versa. Regarding the graph G_c as mentioned above, an outage of CT or failure under attack would correspond to such scenario that the vertex V_c is removed from G_c. Similarly, an outage of the transmission line or disturbance of the power system topology under attack can be represented as such situation that the corresponding edge E_p is removed from G_p.

From the viewpoint of information flow, the CPPS can be described by a directed topology graph. The state variables in the cyber and physical systems can be abstracted to a "data node," and some important factors such as information processing and information transmission can be abstracted to an "information edge" [41].

Additionally, based on the idea of GT, the generators, transformers, and transmission lines can be abstracted to nodes. Combined with the DST-based model, the GT-based model can be used to fully explore and exploit the impacts of cyber disturbance on the power system equipment [33].

2.1.2. Complex network models

The CPPS consists of a large number of different types of cyber devices and power equipment, which complicates the large network structure, and the connection relationship changes over time. This complicated cyber–physical network structure can be modeled as a scale-free network concerning how the emergence of network collective behaviors is facilitated or impeded by network topology.

The CPPS can be divided into a three-layer structure, namely the cyber layer, physical layer, and interface-mapping layer. The nodes in the physical layer represent the power plants and substations with internal topology ignored. The transmission lines are abstracted to the physical layer edge. The nodes and edges in the cyber layer are explained in the following two different forms:

1. The cyber nodes are the abstraction of the communication equipment and the corresponding algorithm, which represent the monitoring system of the power plants. The network edge is the abstraction of the communication link. Then, each controlled physical node has only one identified cyber node to make contact. This cyber node aims to transmit the information of physical nodes and issues the control commands, and at the same time, all information from the distributed network nodes will be collected into the control center. The interface-mapping layer, thus, has one-to-one correspondence [42]. Given that there may be several autonomous nodes in the actual power network that are not controlled by the control center, a "partial one-to-one correspondence" interdependent network model is proposed [43].
2. The node in the cyber layer represents an independent autonomous system, including an operation center and a monitoring center. In power systems, the power plants and substations are controlled by

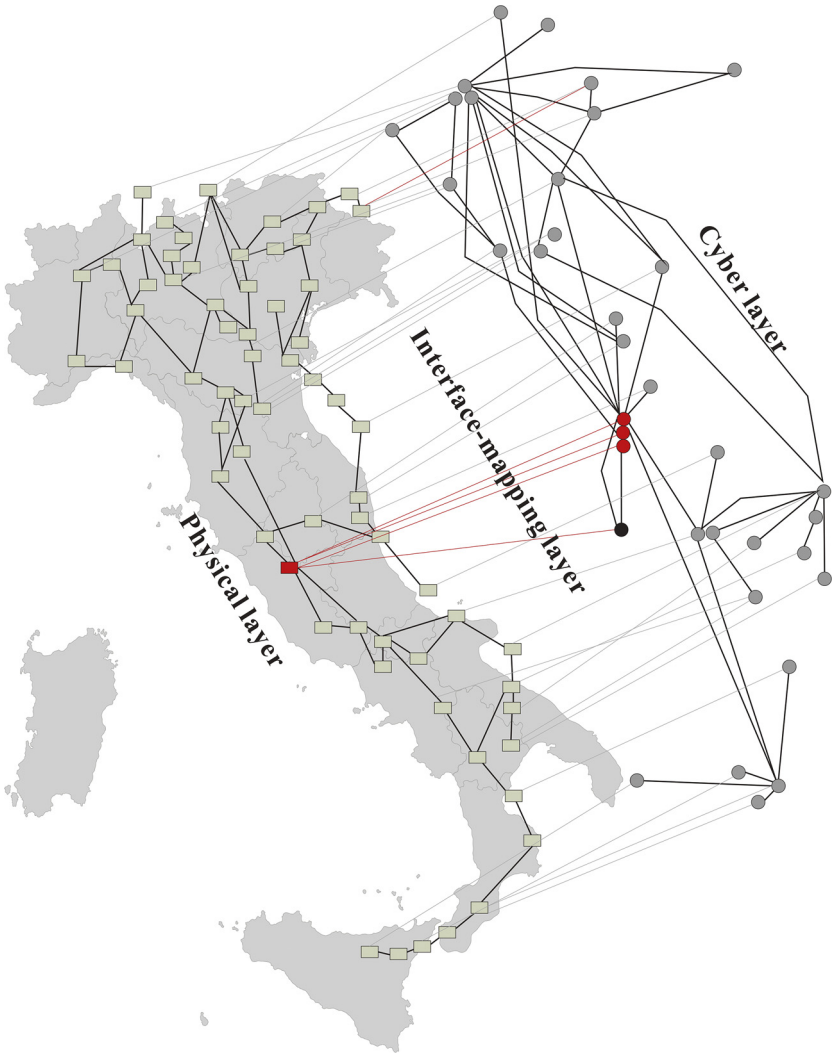

Fig. 4. The CN modeling of cascade failures of CPPS in Italy. (For interpretation of the references to color in the text, the reader is referred to the web version of this article.)

an autonomous system and each cyber node has a unique link that connects to the power node. At the same time, each power station may supply electricity for multiple autonomous systems simultaneously. This can be equivalent to a situation in which there are multiple links from the physical nodes to the cyber nodes. Accordingly, the number of cyber nodes in the formed CN is more than that in physical nodes, and the interdependency is "one-to-multiple" [44].

Fig. 4 shows the electrical blackout that occurred in Italy using the CN model [45]. The rectangles denote power stations while the circles connected to rectangles represent the Internet servers. Removing the power station marked by red color could cut power supply for cyber nodes depending on it, and as a result the additional physical nodes and cyber nodes would be removed. In this situation, a cascading failure may happen. Based on the complex characteristics of the CPPS, the CN model can combine well the microscopic mechanism of the complex system with the macroscopic practical system characteristics [45–47]. However, owing to the fairly simplified treatment of the physical characteristics of the power system, it is relatively difficult to guide the operation and control of the actual CPPS through CN models.

Both the aforementioned GT- and CN-based CPPS modeling methods treat the cyber network and power network as equivalent to nodes and branches connected by a definite topology. The difference between them is presented in Table 1.

2.1.3. Finite state machine models

In the interaction process of a CPPS, the cyber system and the physical system perform a state transition against different stages under different conditions. FSM is regarded as a type of mathematical model based on the state description of dynamic behavior, and it has the ability to express the limited state and the relationship between transitions [48,49]. FSM aims at describing the state sequence that the object experiences in its life cycle and how to respond to any events from the outside world. It is generally applied to generate the state chart diagram (SCD) as a visual representation through the method of exhaustion to implement the modeling of the system dynamic behavior. The SCD can be utilized to analyze cyber–physical interactions qualitatively and make the specific process clear and visible. In Ref. [49], the normal sequential order of two adjacent control commands is modeled as $\langle t_i, t_{i+1}\rangle$, where $\{t_1, t_2, ..., t_n\}$ is a finite set of transitions. Then the false sequential logic attack on SCADA system $\widetilde{v}_i$, which aims to modify the sequential order of two adjacent control commands, is modeled as $\widetilde{v}_i = \langle t_i', t_{i+1}'\rangle = \langle t_{i+1}, t_i\rangle$. The detailed process of how this attack affects the physical system can be obtained. Moreover, an extension of FSM can provide some advanced features including composite state, entry and exit actions, state transitions, and guard conditions. Although it is convenient to model a complicated behavior according to these advanced features, some difficulties in the process of implementation, such as poor reusability, difficult maintenance, and unsuitable quantization, still exist.

2.1.4. Petri net models

PN is a type of network that describes the relationship between events and conditions. It represents the abstraction of the system organization and the control behavior. PN is particularly suitable for describing asynchronous, concurrent, and distributed events in the CPPS. Moreover, the graphical form for system description is relatively intuitive. The interactive behavior between the discrete information of the cyber system and the continuous information of the power network can be simulated well by using this model, and the incidence matrix method [50,51] is applied for the system analysis. It should be noted that an FSM model could be converted into a PN model to infer the propagation mechanism of failure [52].

In CPPSs, cyberattacks or failures are stochastic processes rather than deterministic events. A stochastic PN (SPN) model can be formed by introducing a time parameter (a stochastic delay time between the enabling and firing of each transition) in PN. The stochastic cyber intrusion process can be modeled with the SPN model and analyzed by probabilistic analysis methods [11].

Regarding the impacts of cyberattacks, all tokens are indistinguishable from each other in the basic PN being constructed. The colored PN (CPN) appends a data value called a token color to each token, which can describe the data type and complex data operations so that different attackers can be distinguished by a separate identity in the model. By using the CPN, the structure and information flow of the intelligent meter can be modeled, and the data flow of false data injection (FDI) attacks can be analyzed to study the intrusion detection pattern [53]. Moreover, combined with CPN, an attack on the CPPS can be modeled by the stochastic colored PN (SCPN). Based on the advantages of SCPN, the threat propagation process in the CPPS can be further described quantitatively [34]. Furthermore, different types of PN models can introduce the concept of hierarchy to organize the model of the entire system from different levels, which can help experts in different domains to model and use different modules in the subsystems of the CPPS [20]. Fig. 5 depicts an example based on the blackout occurred in the United States and Canada on August 14, 2003 to model a coordinated attack. A cyberattack on unit's control system (P1) finally causes losses of Sammis-Star line and other transmission lines in northern Ohio (P6), and the detailed descriptions can be found in Ref. [20].

PN is responsible for representing the condition of the system change and the state of the system after the change; however, it is difficult to describe the specific change or operation of a data value or attribute in a system. In a large complex system model, the difficulty of PN applications is mainly caused by the complexity of the model state space. It is imperative to modify and regulate the model according to the specific application environment and restrictions as the computation time increases exponentially with increasing actual system size.

2.1.5. Network attack models

Cyber NAs have led to an increasing number of system failures. Owing to the coupling characteristics of the cyber–physical system, even a pure cyberattack can cause serious consequences. As a special case of cyber network failures, cyberattacks can be modeled as follows.

1. *Attack tree*: An attack tree is generally applied to show all attack paths through intuitive graphic description. The advantages of using

Table 1
Difference between GT-based and CN-based models.

Models	Features	Solving methods
GT-based models	Basic modeling approach pertinent to network topology; Modeling based on the actual CPPS topology; Can be combined with other modeling methods.	Matrix-based analysis methods
CN-based models	Specialize in larger-scale, complex network modeling, and the research on relationship between system topology and network evolution; Modeling mostly through algorithm to create an abstracted topology; Only suitable for a single complex network model.	CN-based analysis methods

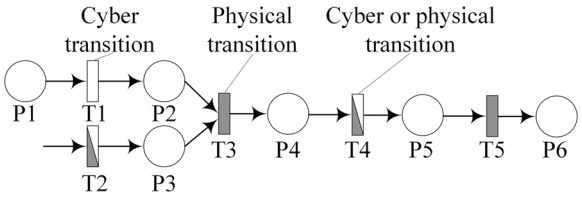

Fig. 5. PN model for hypothetical attack.

the attack tree can be summarized as follows: (i) it can facilitate the description of the multistage cyber network intrusion and (ii) it can express the characteristics of cyberattack structurally and describe the process of attack intuitively and easily. This model can be utilized to identify attack paths, conduct risk assessments or vulnerability analyses, and implement risk detections [18,54–56]. An example of this model can refer to the studies carried out in Ref. [18], in which cyber–physical threat model with respect to power system contingencies is described by attack trees. However, the modeling of an attack tree only corresponds to a limited variety of attacks, and its formation will become very complicated for some relatively complex modeling objects. Additionally, this model can only simulate attack events occurring in sequence. It cannot model attacks occurring simultaneously or behaviors of multiple attackers targeting against multiple components. In order to effectively capture the concurrent activities in the attack process, an existing attack tree analysis case is transformed into an SPN model to conduct corresponding research in Ref. [57].

2. *Attack graph*: An attack graph is used to describe the attacking behavior of an attacker and the dependency between them, which is analyzed by exhaustive methods. This model considers the network topology information and investigates the probability that an attacker might utilize the identified flaws in the network to implement penetration and transition. Moreover, this model attempts to avoid the bad complexity of the system state space. Thus, with the increase in network size and network flaws, the attack graph can apply an automatic generation method to model a complex combined network attack behavior. Practically, in Ref. [58], attack graph is used to build a security assessment model for power control systems. By improving the attack graph, it can also quantitatively analyze the harmfulness of cascading failures across spaces [59]. In addition, after considering the uncertainty of effective attacks, a Bayesian attack graph model is used to explain the attack procedures and assess the likelihood of successful cyberattacks [60].
3. *State transition diagram*: Based on this model, the attack behavior is simulated as a discrete Markov decision process (MDP) or a semi-Markov process (SMP) with consideration of the transition probability between system states under different attack behaviors, which is generally analyzed by a probability method to evaluate the system vulnerabilities [61,62]. This model can describe all types of attacks in detail to satisfactorily meet the detection requirements. In addition, it can define multiple system states according to the safety requirements of the CPPS. Furthermore, the changing trend in system states and the possible attack behavior leading to a change in state can be described exactly by using the model.

Table 2
Common AMs of system applications under cyberattacks.

Objectives	Equations	Details
Transmission line fault detection/location under time synchronization attack (TSA) [63]	$\Delta D = \left(\frac{1}{2\gamma L}\right)\ln\left(\frac{(A+B)(C+De^{j\Delta\delta})}{(C+D)(A+Be^{j\Delta\delta})}\right)$	ΔD is line fault location error due to TSA; $\Delta\theta$ is phase angle difference between the sending end and the receiving end; L is transmission line length; γ is attenuation constant; A, B, C, and D are formulas generated by voltage and current at the receiving end and the sending end.
Voltage stability monitoring under TSA [63]	$I_Z = 100\left(1 - \frac{Z_{th}}{Z_L}\right)$ $I_P = \Re\left(Z_{th}\left\|\frac{E_{th}}{2Z_{th}}\right\|^2\right) - \Re\left(Z_L\left\|\frac{E_{th}}{Z_{th}+Z_L}\right\|^2\right)$	I_Z, I_P are voltage stability margins in terms of load impedance and active power delivered to the load respectively; Z_{th}, Z_L, and E_{th} are complex impedances and voltage of the T-equivalent of transmission corridor which may be affected by TSA.
Event location under TSA [63]	$(x_i - x_e)^2 + (y_i - y_e)^2 - V_e^2(t_i - t_e)^2 = 0$	(x_i, y_i) and (x_e, y_e) are coordinates of the i-th PMU and the disturbance event respectively; V_e is event propagation speed; t_e is initial transmission time of the signal; t_i is disturbance arrival time of the i-th PMU.
AMI under FDI attack [30]	$VSI = V_S^4 - 4(P_rX - Q_rR)^2 - 4(P_rR + Q_rX)V_S^2$	VSI is voltage stability index; P_r and Q_r are total injection real and reactive powers at node r respectively; V_S is voltage magnitude at the sending end; R and X are resistance and reactance respectively.
AGC under FDI attack [64]	$ACE = (P_{tie} - P_{sch}) + \beta(f - 60)$	ACE is area control error; P_{tie} and f are tie-line power flow and system frequency that may be fabricated by attack; P_{sch} is scheduled tie-line power exchange; β_i is frequency bias.
Real-time pricing under FDI attack [65]	$\lambda_1 = \frac{\sum_{j\in M}\frac{b_j}{2a_j} + \sqrt{K}}{\sum_{j\in M}\frac{1}{a_j}}$ $K = \left(\sum_{j\in M}\frac{b_j}{2a_j}\right)^2 + 4\sum_{j\in M}\frac{1}{2a_j}\cdot\sum_{i\in N} w_{i1}$ $\lambda_2 = \frac{n}{2} + m\sqrt{\left(\frac{n}{2m}\right)^2 + \frac{2}{m}\sum_{i\in N} w_{i2}}$	λ_1 and λ_2 represent prices of renewable energy and traditional power sources; w_{i1} and w_{i2} are corresponding preference factors that may be compromised for demand-user i; m, n, a_j, and b_j are coefficients of cost function; M and N are number of supply-users and demand-users.
AC SE under FDI attack [14,25]	$\|r\| = \left\|\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} - \begin{pmatrix} h_1(x_1) \\ h_2(x_2) \end{pmatrix}\right\|$	$\|r\|$ is residuals of AC state estimates; z_2 and $h_2(\hat{x}_2)$ are measurement and state variable that are maliciously altered while z_1 and $h_1(\hat{x}_1)$ keep intact.
DC SE under FDI attack [14,69]	$\|r\| = \|z - H\hat{x}\|$	$\|r\|$ is residuals of DC state estimates; z is vector of measured values that may be tampered; x is vector of state variables; H is dependency matrix.
Kalman filtering under FDI attack [66]	$r = \left\|\frac{z_{k,i} - h\left(\hat{x}_k^-, 0\right)}{\rho_{k,i}}\right\|$	r is anomaly detection criteria; $z_{k,i}$ is malicious measurement; $h(x_k, 0)$ is predicted measurement; $\hat{x}_k^-$ is predicted state; $\rho_{k,i}$ is intermediate variable.
Topology attack of a smart grid [38]	$\bar{s} = s + b$	$s \in \{0,1\}$ corresponds to a system topology; $\bar{s}$ is modified network data; $b \in \{0,1\}$ represents the modifications.

2.2. Mechanism models

Regarding the combination of continuous and discrete events, and the mixture of static and dynamic behaviors, the interactions between cyber system and physical system can be analyzed by using mechanism models.

2.2.1. Analytical models

Because many cyber devices are now equipped with independent power supplies for reliability consideration, the more performance of the CPPS interactive behavior corresponds to the impacts of the cyber network reliability on the power system, i.e., the influence of the change of power measurement information or control information on the power system. By initiating an FDI attack, an attacker can control intelligent devices and manipulate critical information such as synchronization time information, measurement data, electricity price, and state estimation (SE) results.

System AMs generally consider cyber network failures or attacks as a type of data fluctuation pertinent to some power system function and implement a specific application analysis corresponding to the changes in measurement information. Table 2 summarizes several common AMs of system applications under cyberattacks.

Based on the transmission line fault detection module, voltage stability monitoring module, and regional disturbance event positioning module, which are all equipped with phasor measurement units (PMUs), the corresponding AMs pertinent to power system synchronization time data can be built to analyze the influence of cyberattacks on the function module [63]. A similar AM can also be built to study the impacts of tempered measure data on the AGC, power system frequency control, and voltage stability [30,64]. In addition, setting the AM with respect to the power system operator revenue and electricity price information can effectively evaluate the loss level of revenue when the information is being tampered [65].

Actual power system measurement data are first gathered into the control center. After filtering out normal disturbances by SE, the corresponding generated data then become the source that would be used by other advanced applications. Nevertheless, the conventional bad data detection and identification module from SE can only eliminate the bad data that are randomly distributed in the traditional sense. FDI can effectively bypass the monitoring and defense system and tamper the data source coming from the SE. This will threaten the safe and stable operation of subsequent functional modules based on these data sources. By establishing the AM of the CPPS SE, the impacts of cyberattacks on SE can be evaluated quantitatively [25,66], and the function module changes based on the SE results can be further quantitatively analyzed. Regarding cyberattacks, the AC power flow can be used in the SE model. However, it is time consuming and does not necessarily converge to a global optimal solution. Hence, the DC power flow model can be used for the desired solution [38,67,68]. It should be noted that compared with the DC SE model, the AC SE model can better hide from the bad data and intrusion detection system owing to the uncertainty of the DC power flow SE [14].

2.2.2. Dynamic system based models

In the stability analysis of the CPPS, the modeling of the physical system dynamics is considered first, which is usually described in the form of differential equations. Then, the impact of the cyber system on the physical system is modeled as the stimulus of the generator state (frequencies and phase angles) in the generator rotor swing equation. In Ref. [26], a stealthy attack vector is constructed to compromise the synchronous generators in cyber-controlled DER so as to perpetuate physical instability in a smart grid.

After constructing the dynamic models of the excitation system, prime mover/speed governor, synchronous generator, power system stabilizer, high-voltage direct current transmission lines, flexible AC transmission system, and wind turbine, the CPPS can be modeled as a time-delay closed-loop dynamic system. In the case of a closed-loop CPPS analysis based on a wide-area measurement PMU and damping control technology, communication delays cannot be negligible and will affect the stability of the system. In Ref. [29,70], the authors have used eigen-analysis to explore and exploit the delay-dependent stability of the system.

In addition, combined with the relevant method of GT, the CPPS is modeled as a directed graph, and each power node is closely related to the state information determined by the dynamic system equation [33]. This combined model can conveniently evaluate the state variations of the physical system under cyberattacks through numerical simulations.

2.2.3. Hybrid system (HS) models

Power systems follow a continuous dynamic law during operation. Nevertheless, the process of the system operation represents a type of evolution of discretization due to signal sampling, control sequence output, and other digitized information existing in the cyber system. Therefore, it is necessary to choose a fusion modeling method, which can comprise the continuity of the physical system and the discretization of the cyber system. Because the HS is a formal model for a mixed discrete-continuous system, the dynamic behavior of the power system and the corresponding control behavior through the cyber network can be modeled as an HS.

In Ref. [71], the authors have used HS model to analyze the stability of the power system dynamics and associated control actions through a communication network, as depicted in Fig. 6. The power system is measured as $y(t)$ and discretized by the sampling units of communication system, such as PMUs and IEDs. Then the Kalman filter and linear quadratic regulator (LQR) produce the control signals $u(k)$ according to the received data $y'(k)$. Converted from the discrete to analog, which are realized by zero order hold (ZOH) devices, control signals are sent to the corresponding actuators. Meanwhile, the communication data delivery rate is modeled as a stochastic process with an approximate Bernoulli distribution.

In Ref. [72], the transient stability of power system is quantitatively estimated as safety specifications in HS models, which are then translated into restrictions in the model's reachable sets of states. The safe initial states could also be obtained by analyzing the algorithmic reachability of HS.

2.2.4. Variable structure system (VS) models

When the switches of power systems are under attack, the topology of the studied system would continually change. The dynamics of CPPS can be modeled as a VS, which depends on the value of switching signal. VS models can identify the weaknesses that result in reconfiguration of the system through mathematical deduction [73].

In Ref. [74], the authors model the CPPS as a VS and design a state-dependent sequence for the corrupted switches by identifying insidious weaknesses stemming from cyber–physical interactions. They try to identify the sliding surface of the CPSS transient stability control by leveraging the localized state information. Then the transient instability of the target synchronous generator could be generated by destroying the stability condition of a particular sliding mode. This would further induce cascading failures.

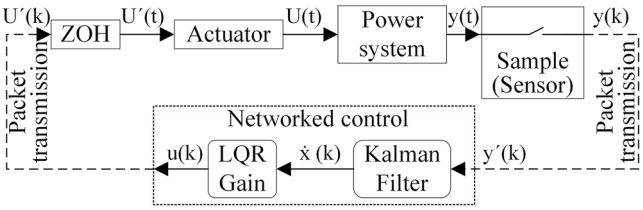

Fig. 6. A reduced HS model of the CPPS.

2.2.5. Multi-agent system models

With the integration of large-scale distributed energy resources (DERs), the distributed characteristics of power systems become increasingly obvious, the data exchange becomes increasingly frequent, and the control modes become increasingly flexible. Accordingly, with a conventional centralized control mode, it is difficult to implement a flexible and an effective control for various DERs. The MA can solve well the collaborative optimization problem of distributed systems owing to its excellent autonomy, adaptability, coordination, and social stability. In MA, each agent represents a corresponding physical entity and can communicate with other agents by exchanging system information.

A holonic MA system is investigated in Ref. [75] which enables the optimal operation scheme of a CPPS through controlling the reactive power at solar photovoltaic (PV) installations. While considering the demand and influence of the cyber system, this holonic MA system also adopts the communication network to provide required information for estimation. In Ref. [76], the authors study the cyber and physical properties, and use the agents to reinforce detection technique. Moreover, they provide situational awareness of the complete system view based on synchrophasor information, relay status logs, and network event monitor logs. This could be used to distinguish the cyberattacks and the conventional physical failures to improve the cyber security and stability. In Ref. [77], a general MA framework in CPPS is proposed. In this framework, the delay-resilient cyber–physical controller enhances the transient stability based on communication latency and state of the cyber component of the system.

Meanwhile, a distributed consensus control can be used to ensure the consistency of the communication content in the CPPS with the MA model. It should be noted that the communication protocol needs to be redesigned to address the influences of communication delay and topology change in communication links [78].

2.2.6. Other models

The authors in Ref. [27] construct a forwarding trees model to connect PMUs and phasor data concentrators (PDC) aiming to minimize the number of invalid or dropped measurements at the PDC. This model can be used to build delay-aware measurement which can enhance WAMS performance under delay attacks.

In Ref. [79], the dynamics of DERs, power plants, and power loads are analyzed through a structure-preserving model, and the cyber part is modeled as different types of measurement information and communication between them. The implementation of the CPPS global observability mainly depends on the coordination between the established model components and the exchange of mutual information, without relying on the observability of the local system components. Based on this modeling method, the measurement and control of the future energy system can be realized.

Furthermore, in Ref. [80], the dynamic behavior of a CPPS is studied via a system dynamics approach. Starting from the internal structure of the system, this approach could be used to quantitatively evaluate which control variables are critical and important to the CPPS. The system dynamics modeling method must deeply understand the relationship between the overall system and the local part, and the relationship between the internal and external systems. However, it links the behavior of the system pattern with its internal feedback loop structure.

2.3. Probabilistic models

Cyber–physical power systems are often influenced by events of a probabilistic nature. The existing situation or future progress trend cannot be described exactly. In this situation, it can be modeled by uncertainty models. Meanwhile, the process of rational participants making decisions is often under uncertain conditions. When there exist interactions between multiple decision-making participants, each one would choose such strategy that is conducive to its own benefit according to the existing information. This kind of probabilistic nature is often described by game-theoretic models.

2.3.1. Uncertainty models

The cyber–physical interactions in power systems bear uncertainty including the direct impacts of cyber system unreliability or cyberattacks on the power systems [81], as well as the indirect impacts of the damage monitoring and protection systems due to the malfunction of the cyber systems [4,82,83]. The decrease in CPPS reliability might be caused by many reasons, such as breakdown of information and communication systems, failure of power network equipment, or improper configuration of SCADA.

Based on the most recent studies, a single cyber system is modeled in three different ways, namely reliability block diagram, discrete MDP, and SMP. The reliability block diagram method is one of the most practical ways in building the reliability model of the cyber layer. In Ref. [3], this method is adopted to calculate the reliability of cyber system, and then the multi-state Markov chain is used to study the impacts of cyber system function failures on the availability of physical components. Another approach is to model the cyberattacks as a discrete MDP in order to enumerate all possible attack scenarios [61]. In this Markov process, an attacker can obtain corresponding rewards after a state transition is finished with a certain probability. Then, the current security state can be estimated using this model combined with cyber intrusion detection sensor alerts. In Ref. [62], the authors model cyberattacks on SCADA systems as an SMP. The SMP has several states that can be enumerated, and the transition probability from one state to another depends on the duration time of the process in that state. In addition, the communication delay model, including the minimum deterministic delay, Internet traffic delay with probability density function (PDF), and router processing delay with PDF, is adopted to allow a deeper insight into the communication process in Ref. [6].

As for the physical systems, regarding the topology and reliability of cyber layer as well as the protection and monitoring strategies, a multistate Markov chain model is built to describe the availability of the physical layer components in Ref. [3].

For the entire CPPS, after the reliability information of the system components is collected, the system reliability can be expressed by a probability table (P-Table) [81,82], and the state transition probability of the individual components can be modeled by a state transition diagram [4,83]. Moreover, the Bayesian structure extracted by the minimal cut set-based method can be used for the CPPS reliability assessment, which is realized by a Bayesian network probabilistic reasoning [17].

2.3.2. Game-theoretic models

In recent years, cyberattack events targeting secondary power systems are gaining increasing attention worldwide. Attackers can lead to losses of CPPSs at low cost through cyberattacks. Defenders can protect the physical components through an effective resource allocation. The process of cyber–physical interactions is generally modeled as a type of attack-mitigation GM, which can be applied for system vulnerability analysis.

As two or more participants make their rational decisions in confrontational or competitive situations, they intend to maximize their interests via allocating limited resources. This competitive relationship can be modeled as a Colonel Blotto game [62], zero-sum game [84], and stochastic game [36].

On the contrary, an attack-mitigation dynamic game can be formulated as a bi-level mathematical programming problem. This model assumes that both players fully understand the global information of the CPPS. In Ref. [85], the authors present an idea that the attacker aims to maximize the load losses caused by the attack in the upper level, and the operator tries to minimize the impact of the attack by optimizing power system operation in the lower level. Considering the

most effective cyberattack, the upper level is modeled as a topology preserving attacks on the power network, and the lower level is modeled as a load redistribution attack, which ensures that all variations in measurements are not detected in [86]. The GM can also be modeled as a three-stage defender-attacker-defender tri-level mathematical programming problem. In Refs. [87,88], the authors describe the following three steps: (i) the defender allocates the defense resources, (ii) the attacker attacks the resources, (iii) and the defender reduces the power losses.

All the GMs mentioned above presume that the statuses of the two players are equal. Hence, their actions are similar. That is, when an attacker makes a decision, the attacker is not aware of the defender's decision. Practically, however, the statuses of the players are not always equal, which further lead to the asymmetry in decision order. The attacker first determines the defender's behavior, and then decides his or her own countermeasures. This asymmetric competition can be modeled as a static infinite Stackelberg GM. In Ref. [89], this model is used to describe the interactions between different security agents in cyber system, while a different Stackelberg game is applied to model the full-information H^{∞} minimax control with package drops in physical system.

Moreover, the dynamic attack-mitigation game would not be finished at once, and the game under the same structure could always be repeated many times. In this situation, the participants' history can be observed, and hence, their decisions can be made based on the opponents' actions. Then, both sides would consider the existence of their own long-term interests. The interactions between cyberattackers and physical defenders can be modeled as an iterated game, whose results may be relatively different from a one-time game [28].

Almost all previous studies conduct the corresponding analysis from the decision-making viewpoint without considering the actual physical models and assume that all controls are optimal. When considering the dynamics of power systems, the physical systems are usually represented mathematically by a series of differential equations. In Ref. [26], the attack-mitigation game is expressed by a nonlinear differential GM with fully taking dynamic power system into consideration. This model combining the GT with DS can be applied to study the system stability under various cyberattacks and develop countermeasures.

2.4. Simulation models

In CPPSs, the discrete characteristics of cyber systems and the continuous characteristics of power systems complicate the research of CPPSs. In this situation, a type of integrated simulation platform for CPPSs can be built to conduct research by establishing corresponding numerical simulation models and integrating existing calculation methods, which aim to keep the integrity and accuracy of the entire system to the highest degree. The simulation models of power systems can be built using the following well-known software: Matlab [76,90], PSCAD [91], PowerWorld [92], Modelica [93], OpenDSS [94,95], DIgSILENT [96], EMTP-RV [97], and OPAL-RT [98]. The simulation models for cyber systems can be built under OMNet++ [94], Java [76,91], NS2 [99], RINSE [100], OPNET [90,92,95–97], and Visual Studio [101] software development environments. The simulations can realize a unified modeling of the static structure and dynamic behavior or the discrete system and the continuous system.

In order to describe the detailed information exchange and communication protocol, the communication models applied to the advanced functions in CPPSs must comply with some corresponding standards. Table 3 lists the main released international standards in several advanced functions [102].

3. Solution methods

Table 4 summarizes the features of all modeling methods and their scopes of applications described above. The details pertinent to each solution method are discussed below.

3.1. Matrix-based analysis methods

The matrix-based analysis methods lay the foundations of expression and analysis in mathematical form for GT-based models and can obtain the network topology relations easily. For GT-based models, the relation between vertices and edges can be expressed by an incidence matrix, and the relation between vertex pairs can be expressed by an adjacency matrix (collectively, "relation matrix"). Conventionally, several incidence matrices for evaluating the correlated characteristics between the cyber system and physical system in CPPSs currently exist. These incidence matrices mainly involve the power–power incidence matrix, cyber–cyber incidence matrix, and power–cyber incidence matrix. A major advantage of applying an incidence matrix is that it can reflect the influence path of the cyber system on the power system by analyzing the topological structure of the CPPS. These matrices have been widely used in the past to investigate the impacts of delays, interruptions, and error codes of communication systems on power systems [103], and the corresponding influence values depend on the CPPS vulnerability indices, which need to be created.

Based on the power–power incidence matrix, the power flow characteristics of a power system with a change in network structure caused by the cyber system can be analyzed by ignoring the line losses [2,37–40]. Interestingly, the incidence matrix can be utilized to describe the system structure modeled by PNs and to calculate the results of transitions [50]. Moreover, the CN model can also be represented by the incidence matrix [42] to implement the topological relations.

Another major analysis matrix is the cyber–physical interface matrix, which represents the mapping relationship between various cyber failure modes and physical failures. Based on this matrix, the impacts of cyber network failures on the overall reliability of the system can be analyzed [4,83].

In addition, the matrix-based analysis methods can realize a

Table 3
Main released international standards in advanced functions considering information and communication requirements.

IEC standards	AMI	DA	DER	DMS	DR	EMS	EV	SA	Storage	Smart home
IEC 61970	√	√	√	√	√	√	–	√	√	–
IEC 60870-5	–	√	–	√	–	√	–	√	–	–
IEC 60870-6	–	–	–	√	–	√	–	–	–	–
IEC 61334-4	√	–	–	–	–	–	–	–	–	–
IEC 61400-25-1	–	–	√	√	–	√	–	–	–	–
IEC 61850	√	√	√	√	–	√	√	√	√	–
IEC 61968-13	√	–	√	√	√	–	–	–	–	–
IEC 62056	√	–	√	√	√	–	√	–	–	√
IEC/TS 62351	√	√	√	√	√	√	√	√	√	√

Table 4
Characteristics, applications, and solution approaches of CPPS models.

Models	Characteristics	Applications	Solution approaches						
			3.1	3.2	3.3	3.4	3.5	3.6	3.7
GT	Network topology representation and matrix utilization to analyze power systems	Vulnerability analysis; impact analysis of cyberattacks on power systems; modeling and countermeasures against cyberattacks	√	–	–	–	√	–	√
CN	Research on the relationship between system topology and network evolution	Interactive analysis between cyber systems and power systems; propagation mechanism of cascading failures; robustness of the communication network	√	√	–	–	–	–	–
FSM	Research on the relationship between the limited state and the transition under external events	Impact of cyberattacks on power systems	–	–	√	–	–	–	–
PN	Research on the relationship between events and conditions; intuitive graphical representation with precise mathematical definition; expert in modeling discrete complex systems; powerful analysis function	Interactive analysis between cyber systems and power systems; vulnerability analysis; modeling and countermeasures against cyberattacks	√	–	√	–	–	√	–
NA	Intuitive graphical expression; the features of the cyberattacks and its attack process; detailed description of the various attacks	Attack paths identification; risk assessment; vulnerability analysis; risk detection	–	–	√	–	–	√	–
AM	Quantitative analysis; combination with the practical system functions; easy simulation	Impact of cyberattacks on power systems; vulnerability analysis; countermeasures against cyberattacks	–	–	–	√	–	–	–
DS	Expert in analyzing relationship between the dynamic mechanism of the power system and the stability analysis	Impact of cyberattacks on power systems; stability analysis; countermeasures against cyberattacks	–	–	–	–	√	–	√
HS	Simultaneous consideration of the characteristics of continuous system and discrete system; easy analysis for the stability of CPPS	Stability analysis; system dynamic performance analysis	–	–	–	–	√	–	–
VS	Expert in the stability analysis of CPPS under cyberattacks	Modeling and countermeasures against cyberattacks; stability analysis	–	–	–	–	√	–	–
MA	Easy analysis for the operation problem of CPPS with DER	System operation optimization; impact analysis of cyberattacks on power systems; design countermeasures; robustness analysis	–	–	–	√	√	–	√
UM	Consideration of the probability of system failure, successful cyberattacks, and different path of cyberattacks	System reliability analysis; impact of cyberattacks on power systems	√	–	–	–	–	√	√
GM	Analysis from attack-mitigation strategy	Vulnerability assessment; modeling and countermeasures against cyberattacks; security analysis	–	–	–	–	–	√	√

quantitative evaluation of system performance. Through matrix calculations [41], the security risks of physical systems can be evaluated based on graphical models constructed using information flow and energy flow. In Ref. [11], a state transition probability matrix is used to calculate the steady-state probability of a system based on the SPN model, and the load losses after an attack are evaluated as well.

3.2. Complex network based analysis methods

The static characteristic and vulnerability of a system network structure in CNs can be analyzed by using the statistical description of various properties of CNs [42,43,45,46]. These statistical indices reflect the degree of closeness between the cyber network and the power network, impacts of the interactions, and coverage rate of cyber equipment. Table 5 lists the common statistical indices in practical analysis.

Given that network nodes are removed from the CN when failures occur in cyber networks, this inevitably results in changes in the physical system structure, which in turn affects the cyber networks. Therefore, combined with percolation theory, the network structure characteristics can be analyzed by calculating the number of surviving nodes after failure to further investigate the propagation mechanism of cascading failures in CPPSs [44]. In an attempt to make each failure scenario as close as possible to reality, the cascading failures in CPPSs would be analyzed from both topology and power flow aspects [42]. By extending the corresponding CN betweenness, the vulnerability after cascading failures can be analyzed and the weaknesses in the system considering the topology and system characteristics can be identified. Moreover, the fault types are not limited to network nodes in CNs, but also include the network edges removed by the influences [47]. Based on these studies, the corresponding mitigation strategies of preventing cascading failures and the auxiliary decision-making schemes of protecting key components can be proposed.

3.3. Method of exhaustion

The method of exhaustion is used to test different possible situations one by one, and then to find the anticipative solution or no solution conclusion.

The state machine model is used to qualitatively describe and explain the cyber–physical interactions. In general, failures occurring on the cyber network and physical network are analyzed separately at first, and then the interaction results of both failures are considered through the method of exhaustion [52].

After the attack tree model is obtained, a feasible attack path is identified from each leaf node. Then, the difficulty of the attack and the severity of the loss to the system can be qualitatively determined [18]. After the vulnerability index of the leaf node is obtained, the overall vulnerability index of the system can be calculated by traversing the set of attack paths, which is used to improve the security performance of the system [56].

Similarly, the vulnerability index of individual states and the weights of different security indices can be quantified to evaluate the security performance of the system by traversing the attack graph model [58]. In addition, the causal relationship between attacks and possible system failures can be analyzed. The first step is to improve the conventional attack graph model by abstracting all types of security risks (cyberattacks, secondary power equipment failures, and transient stability) into the vertices of the attack graph. Following this treatment, all security risks that may lead to cascading failures are traversed to realize a quantitative assessment of various cross-space damage hazards [59].

3.4. Analytical methods

The interferences or attacks on cyber systems would essentially lead to certain state deviations related to power system functions. Analytical methods are applied to obtain the relation between state deviations and system functions (such as AGC [64], SE [14,38,66], economic dispatch [66], power flow analysis [66], voltage stability index analysis [30], and power market price [65]) by constructing the corresponding AMs. Furthermore, the effect of the deviation in the measured state data on the system functions can be verified by using a power simulation program.

3.5. Control theory-based analysis methods

Control theory-based analysis methods are particularly useful and powerful in studying the dynamic stability of CPPSs and proposing enhanced control strategies. Different methods are thus developed to deal with such significant issues according to specific model characteristics of the studied systems. In [70], the stability of a large delayed cyber–physical power system incorporating wide-area damping controllers is solved by applying a critical eigenvalue analysis. The stability of a microgrid with constant time delay and variable time delay is addressed by finding an index called the time-delay margin [29]. The closed-loop stability of a Markovian jump linear power system with an HS model is analyzed by applying a linear matrix inequalities-based method [71]. In Ref. [72], the authors proposed a novel algorithm to address the joint dynamics of physical processes and cyber elements via a dynamic hybrid model.

To realize the stability control of a system described by a structure-preserving model, a module-based interactive control is proposed [79]. Furthermore, a Lyapunov–Krasovskii function-based distributed averaging-based integral control strategy has been designed by scholars to keep the stability of multi-agent CPPSs under a communication delay and topology change [78].

In other respects, the system dynamics approach is used to analyze the impacts of cyberattacks on power system infrastructures described by dynamic models [80]. Aiming at a CPPS under a multi-agent model, a Luenberger-like nonlinear state observer agent and decoupling controller agent are designed by some scholars to analyze the potential impacts of integrity attacks [104]. Moreover, the existence of the switching vulnerability depending on the local structure of the power system is demonstrated by using the VS theory [73,74].

3.6. Probabilistic analysis methods

The reliability of CPPSs is analyzed by using probabilistic analysis methods that are carried out in several steps. To begin the process, the network method and the state space method are used to obtain the reliability indices of the cyber systems [3]. Then, the mapping relationship between the cyber network failure and the power network

Table 5
Statistical indices of CNs.

Structural parameters	Average degree [43]; Average path length [43]; Clustering coefficient [43]; Degree distribution [43,45]; Maximum degree [43]; Node centrality [46]; Edge centrality [46].
Connectivity indices	Node interdependency ratio [43]; Point-to-point pilot protection ratio [43]; Inter degree–degree correlation [43]; Average inter degree difference [43]; Nodes' contact ratio [46]; Links' contact ratio [46]; Centrality difference [46].
CPPS vulnerability indices	Ratio of edge loss [42]; Ratio of load loss [42]; Loss of extended betweenness [47].

failure is established (optional). The mapping relationship can be formed by a cyber–physical interface matrix [4,83], P-Table [81], state updating-based model [82]. In the follow-up phase of the method, taking the minimum load shedding as the goal, the Monte Carlo simulation (MCS) method is used to simulate the operations of the stochastic processes of the system. Finally, all types of reliability indices of the systems according to these operations can be calculated. As a result, the probability of CPPS failures and their effects are estimated by using such reliability indices as loss of load probability and expected energy not supplied.

The sequential Monte Carlo method [3,4,60,62,83] and non-sequential Monte Carlo method [3] can be used for the index analysis of CPPS reliability. The convergence speed of the MCS method is independent of the dimension of the problem. Therefore, it is suitable for solving multidimensional and high-dimensional problems. However, as the system size increases, the evaluation time of each state will increase significantly, and the total computation time will substantially increase as well.

In addition, the Bayesian network is used to analyze the reliability model of CPPSs [17]. After considering the uncertainty of a successful attack, a Bayesian attack graph model is proposed to explain the steps of the attack and to evaluate the likelihood of a successful attack [60].

In addition to the reliability analysis, the quantitative indices of system security can be obtained by using a cyber–physical contingency selection algorithm pertinent to the MDP model [61]. As for the SPN model, each identity of SPN is mapped into a state of Markov chain (MC) so that the parameters of the state transition probability matrix of MC can be obtained. Therefore, the steady-state probability of each state of MC can be calculated, and the vulnerability and reliability of the CPPS can be solved accordingly [11].

3.7. Optimization methods

Linear programming (LP) methods can be used to solve the problems of minimizing power loss [75,105], minimizing load shedding [37], maximizing data connection in cyber networks [81], minimizing costs [35] but maximizing profits during cyberattacks [69], and determining the effectiveness of countermeasures in response to attacks [35].

Optimization methods have been widely used to investigate game problems. The game theory analysis aims to find the optimal strategy combination for the players by solving a game model based on the confirmation of players and their strategies as well as the establishment of a profit function. In general, different types of game models correspond to different methods for the solutions of their optimal strategies.

The zero-sum game, which is the most common game model, is generally translated into an LP problem [84]. Regarding the bi-level programming model used to model a game problem, the objective function of the upper-level submodel is determined by the solution function of the lower-level submodel, which is nonlinear and non-differentiable. Even a linear bi-level programming is non-convex and non-differentiable everywhere. A two-stage algorithm can be applied to convert the original bi-level programming problem into an equivalent LP problem [86]. As for the mixed-integer nonlinear bi-level programming problem, a novel approach based on Benders decomposition within a restart framework can be used for the solution [85].

The tri-level programming model used to analyze an attack-mitigation game problem in a distribution network is extremely difficult to solve perfectly owing to the existence of mixed-integer decision variables and nonlinear power flows. For small-scale systems, it would be possible to calculate each expected power loss under attack based on the method of exhaustion; then, the defense resources can be allocated to the transmission lines of the system based on the expected calculation results [88]. For large-scale power systems, the original tri-level programming model can be approximately transformed into a bi-level programming model, which can be solved by using a greedy algorithm [87]. This tri-level programming problem can also be directly solved by using some computational intelligence methods such as genetic algorithm and particle swarm optimization [88].

Furthermore, the existing body of research has attempted to solve the game problem from various perspectives. The optimal allocation of the offensive and defensive resources in the Colonel Blotto game is obtained once the Nash equilibrium condition of the game resource allocation is satisfied [62]. In the static infinite Stackelberg game, the allocation can be obtained by satisfying the configuration strategy and control strategy of the game model [89]. Such problem based on an iterated game model can be solved by applying a zero-determinant strategy [28], and the nonlinear differential game can be solved by using a novel iterative algorithm [26].

3.8. Simulation-based methods

This study mainly introduces the simulation platform-based method to analyze and solve problems in CPPSs through the integrated simulation experiments. There are three types of simulation solutions: (i) single equivalent simulation scheme, (ii) single modeling simulation scheme, and (iii) hybrid simulation scheme.

The single equivalent simulation scheme treats the cyber information being tampered as the deviation of the analog signal (phase angle, voltage, current, and power) or digital signal (breaker state). Then, the impact of cyber information change on the physical system is analyzed by using power simulation programs [33,63,106]. In addition, the impact of communication transmission delay on the system can be simulated by setting the control command delay or measuring the data upload delay based on the power simulation software [39].

The main idea of the single modeling simulation scheme is to build a compound model of the CPPS under the power system simulation software environment. The design of an embedded communication simulator integrated with PSCAD for communication mechanisms research is discussed in Ref. [107]. It demonstrated that the communication requirements could be significantly reduced with an error-dependent strategy, allowing for more robust operation under communication capacity variation.

The hybrid simulation scheme requires that the modeling of the cyber network and physical network is performed by using their respective professional simulation software. Through a time synchronization method, the two programs can run in the same time domain. Hybrid simulation can be divided into non-real-time hybrid simulation and real-time hybrid simulation [18,108–110].

The existing non-real-time hybrid simulation schemes have been able to deal with the static problems of power system, which are affected by cyber system, such as demand response configuration and reactive power optimization. However, the biggest challenge for non-real-time hybrid simulation schemes mainly comes from the problem of time synchronization, when dealing with dynamic problems in power system, such as stability control and wide-area monitoring. Meanwhile, the lack of timely updates of power data and the processing of delays in cyber systems would seriously affect the accuracy of simulation [111]. On the other hand, the real-time simulation can avoid the problem of time synchronization through building real-time simulation units for both power and cyber parts. In addition, a high-level architecture (IEEE Std. 1516) framework can be used to build an advanced collaborative simulation CPPS experimental platform [112]. However, such integrated simulation platform-based method is still in its infancy, and most advanced function of CPPS cannot be simulated in this way. The main difficulties are addressed as follows: (i) The CPPS model needs to include physical processes, software models, computing platforms, and communication networks, and the control links involve physical process calculations, control process calculations and communication transmissions. These complex factors lead to the difficulties in data transfer, synchronization, and coordination between two platforms. (ii) Though it is desirable to describe cyber elements, continuous dynamic

events, and discrete events in detail in order to ensure simulation correctness, an overly detailed simulation model will result in a heavy computational burden, and it is not conducive to highlighting key factors such as system stability, safety, and reliability.

However, the simulation platform-based method is still one of the best ways in dealing with problems considering the detailed cyber system, such as the influence analysis of data flow rate, latency and response time on power system. In contrast, in the analysis of vulnerability, reliability, stability and attack-mitigation strategy, most research studies generally utilize the graphical, mechanism and probabilistic models without considering the detailed cyber system architecture. Furthermore, the corresponding simulations are conducted via the conventional numerical analysis method.

4. CPPS research in China

Since 2010, China has made preliminary and exploratory studies on the architecture and implementation technology of CPPSs, and relevant achievements are gaining significant attention. In recent years, the main studies in China have focused on the interaction mechanism and modeling theory of CPPSs [113,114], steady-state and dynamic characteristics of CPPSs [115], and vulnerability and mitigation strategies under attacks [88].

As an increasing number of DERs and energy storage devices are integrated into the power networks, from the control viewpoint, many Chinese scholars are researching an information-led EI system [116] to realize precise control through the fusion of cyber and energy. This EI system could make energy similar to information on the Internet by which any legal entity can freely access and share information. The ultimate goal is to achieve a two-way free flow of energy and information between the supply side and demand side. In this case, the information flow can provide support for energy scheduling, and the energy flow can guide users' decision-making. This is suitable for maximizing the utilization of renewable energy and achieving friendly interactions with energy users [117]. From the viewpoint of data integration, based on the unified information model, a unified data interaction specification is designed to realize full data access to big data platform to support decision-making.

In the aspect of CPPS modeling, China has also studied the graphical models, mechanistic models, and probabilistic models [88]. In addition, several investigations have considered the energy information fusion modeling analysis methods to achieve the modeling of massive multiple energy components, information security, and user behaviors. Based on this fusion model, additional useful information can be integrated into the power control process, and a global optimization control can be realized. For example, Ref. [118] used the FSM and the mixed logical dynamical model as the CPPS fusion model. Ref. [119] established the fusion model through one-to-one mapping between the physical model and information model. Furthermore, by analyzing the logical relation between the cyber object and the physical object, Ref. [120] implemented the CPPS interactive modeling method based on the set theory.

In the application to CPPSs, the safety and reliability evaluation technology, risk pre-warning technology, and real-time optimization control method in active distribution networks, which are novel solutions to the flexible utilization of DERs [114], are being explored by scholars in China.

5. Conclusion and future work

In recent years, the research studies on cyber–physical interactions in power systems have gained considerable attention. The corresponding models and solution methods can be categorized in such way as described in Section 2 and Section 3 in this paper. Certainly, other categorizations can also be suggested for different purposes. In this paper, the major contributions to the review of cyber–physical interactions in power systems are highlighted as follows:

1. This study mainly summarizes the CPPS models concerning impact analysis of cyberattacks on power systems, system stability control, attack identification, countermeasures against cyberattacks, system security assessment, reliability and vulnerability assessment from the viewpoints of topology, mechanism, probability and simulation.
2. The corresponding solution methods pertinent to these CPPS interactive models are also discussed elaborately.
3. The latest research progress of Chinese research on CPPS is briefly discussed.

It should be noted that only some typical research works were organized and summarized. The models and methods discussed in this study can provide a strong support for guiding the safe and stable operation of CPPSs. However, some shortcomings in these modeling and solution approaches still exist. For instance, the specific communication network topology and communication transmission mechanism are not taken into consideration in the information and communication network. The cyberattacks are generally assumed as single-source attacks, and no further intensive analysis on simultaneous attacks pertinent to multiple points and attacks against multiple targets is conducted. Moreover, it is usually presupposed that the attackers have full knowledge of all the resources of the actual CPPS, and the control results of power systems are hypothesized to be optimal. Such approximations and simplifications do not conform to actual situations.

By ignoring the behavioral characteristics of specific CPPS elements and the complex self-adaptability of systems, the current research has only a theoretical significance. Therefore, building an integrated model of CPPSs that takes the actual information and power flow into consideration is the primary problem to be solved in the near future. Based on this model, it is more appropriate to evaluate the interactions of practical CPPSs using a unified computing framework. In addition, more information and power data will be connected to systems in the future. Accordingly, proposing a better CPPS control strategy by efficiently organizing and managing power space-time big data becomes relatively crucial.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China (51777103).

References

[1] C. Dong, H. Jia, T. Jiang, L. Bai, Q. Hu, L. Wang, Y. Jiang, Effective method to determine time-delay stability margin and its application to power systems, IET Gener. Transm. Distrib. 11 (7) (2017) 1661–1670, https://doi.org/10.1049/iet-gtd.2016.0953.
[2] Y. Wang, Z. Lin, X. Liang, W. Xu, Q. Yang, G. Yan, On modeling of electrical cyber–physical systems considering cyber security, Front. Inf. Technol. Electron. Eng. 17 (5) (2016) 465–478, https://doi.org/10.1631/FITEE.1500446.
[3] Y. Han, Y. Wen, C. Guo, H. Huang, Incorporating cyber layer failures in composite power system reliability evaluations, Energies 8 (2015) 9064–9086, https://doi.org/10.3390/en8099064.
[4] H. Lei, C. Singh, A. Sprintson, Reliability modeling and analysis of IEC 61850 based substation protection systems, IEEE Trans. Smart Grid 5 (2014) 2194–2202, https://doi.org/10.1109/TSG.2014.2314616.
[5] H. Ye, Y. Liu, P. Zhang, Efficient eigen-analysis for large delayed cyber–physical power system using explicit infinitesimal generator discretization, IEEE Trans. Power Syst. 31 (2016) 2361–2370, https://doi.org/10.1109/TPWRS.2015.2463109.
[6] J. Zhang, S. Nabavi, A. Chakrabortty, Y. Xin, ADMM optimization strategies for wide-area oscillation monitoring in power systems under asynchronous communication delays, IEEE Trans. Smart Grid 7 (2016) 2123–2133, https://doi.org/10.1109/TSG.2016.2547939.
[7] D. Kushner, The real story of stuxnet, IEEE Spectr. 50 (2013) 48–53, https://doi.org/10.1109/MSPEC.2013.6471059.
[8] Symantec security response, Dragonfly: cyberespionage attacks against energy suppliers, Symantec, 2014. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.
[9] M. Assante, Confirmation of a coordinated attack on the Ukrainian power grid,

SANS Industrial Control Systems Security Blog, 2016. https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.
[10] TOI STAFF, Steinitz Israel's electric authority hit by 'severe' cyber-attack, The Times of Israel, 2016. https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/. (Accessed 28 November 2017).
[11] C.W. Ten, C.C. Liu, G. Manimaran, Vulnerability assessment of cybersecurity for SCADA systems, IEEE Trans. Power Syst. 23 (2008) 1836–1846, https://doi.org/10.1109/TPWRS.2008.2002298.
[12] E. Bompard, R. Napoli, F. Xue, Vulnerability of interconnected power systems to malicious attacks under limited information, Eur. Trans. Electr. Power 18 (2008) 820–834, https://doi.org/10.1002/etep.274.
[13] C.W. Ten, G. Manimaran, C.C. Liu, Cybersecurity for critical infrastructures: attack and defense modeling, IEEE Trans. Syst. Man Cybern. A: Syst. Hum. (2010) 853–865, https://doi.org/10.1109/TSMCA.2010.2048028.
[14] G. Hug, J.A. Giampapa, Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks, IEEE Trans. Smart Grid 3 (2012) 1362–1370, https://doi.org/10.1109/TSG.2012.2195338.
[15] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, U. Adhikari, Modeling cyber–physical vulnerability of the smart grid with incomplete information, IEEE Trans. Smart Grid 4 (2013) 235–244, https://doi.org/10.1109/TSG.2012.2232318.
[16] Y. Zhu, J. Yan, Y. Tang, Y.L. Sun, H. He, Joint substation-transmission line vulnerability assessment against the smart grid, IEEE Trans. Inf. Forensics Secur. 10 (2015) 1010–1024, https://doi.org/10.1109/TIFS.2015.2394240.
[17] M. Eliassi, A. Khoshkholgh Dashtaki, H. Seifi, M.-R. Haghifam, C. Singh, Application of Bayesian networks in composite power system reliability assessment and reliability-based analysis, IET Gener. Transm. Distrib. 9 (2015) 1755–1764, https://doi.org/10.1049/iet-gtd.2014.0660.
[18] K.R. Davis, C.M. Davis, S.A. Zonouz, R.B. Bobba, R. Berthier, L. Garcia, P.W. Sauer, A cyber–physical modeling and assessment framework for power grid infrastructures, IEEE Trans. Smart Grid 6 (2015) 2464–2475, https://doi.org/10.1109/TSG.2015.2424155.
[19] Y. Zhang, L. Wang, Y. Xiang, Power system reliability analysis with intrusion tolerance in SCADA systems, IEEE Trans. Smart Grid 7 (2016) 669–683, https://doi.org/10.1109/TSG.2015.2439693.
[20] T.M. Chen, J.C. Sanchez-Aarnoutse, J. Buford, Petri net modeling of cyber–physical attacks on smart grid, IEEE Trans. Smart Grid 2 (2011) 741–749, https://doi.org/10.1109/TSG.2011.2160000.
[21] C. Lo, N. Ansari, CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid, IEEE Trans. Emerg. Top. Comput. 1 (1) (2013) 33–44, https://doi.org/10.1109/TETC.2013.2274043.
[22] F. Pasqualetti, F. Dorfler, F. Bullo, Attack detection and identification in cyber–-physical systems, IEEE Trans. Autom. Control 58 (2013) 2715–2729, https://doi.org/10.1109/TAC.2013.2266831.
[23] S. Backhaus, R. Bent, J. Bono, R. Lee, B. Tracey, D. Wolpert, D. Xie, Y. Yildiz, Cyber–physical security: a game theory model of humans interacting over control systems, IEEE Trans. Smart Grid 4 (2013) 2320–2327, https://doi.org/10.1109/TSG.2013.2270291.
[24] T. Liu, Y. Sun, Y. Liu, Y. Gui, Y. Zhao, D. Wang, C. Shen, Abnormal traffic-indexed state estimation: a cyber–physical fusion approach for Smart Grid attack detection, Future Gener. Comput. Syst. 49 (2015) 94–103, https://doi.org/10.1016/j.future.2014.10.002.
[25] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, W. Zhao, On false data-injection attacks against power system state estimation: modeling and countermeasures, IEEE Trans. Parallel Distrib. Syst. 25 (2014) 717–729, https://doi.org/10.1109/TPDS.2013.92.
[26] P. Srikantha, D. Kundur, A DER attack-mitigation differential game for smart grid security analysis, IEEE Trans. Smart Grid 7 (2016) 1476–1485, https://doi.org/10.1109/TSG.2015.2466611.
[27] R. Kateb, P. Akaber, M. Tushar, A. AL-Barakati, M. Debbabi, C. Assi, Enhancing WAMS communication network against delay attacks, IEEE Trans. Smart Grid 3053 (2018) 1, https://doi.org/10.1109/TSG.2018.2809958.
[28] A. Farraj, E. Hammad, A. Al Daoud, D. Kundur, A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems, IEEE Trans. Smart Grid 7 (2016) 1846–1855, https://doi.org/10.1109/TSG.2015.2440095.
[29] T.J. Mary, P. Rangarajan, Delay-dependent stability analysis of microgrid with constant and time-varying communication delays, Electr. Power Compon. Syst. 44 (2016) 1441–1452, https://doi.org/10.1080/15325008.2016.1170078.
[30] A. Anwar, A.N. Mahmood, Z. Tari, Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid, Inf. Syst. 53 (2015) 201–212, https://doi.org/10.1016/j.is.2014.12.001.
[31] A. Roy, D.S. Kim, K.S. Trivedi, Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees, Secur. Commun. Netw. 5 (2012) 929–943, https://doi.org/10.1002/sec.299.
[32] G. Wen, W. Yu, X. Yu, J. Lü, Complex cyber–physical networks: from cybersecurity to security control, J. Syst. Sci. Complex. 30 (2017) 46–67, https://doi.org/10.1007/s11424-017-6181-x.
[33] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, K.L.B. Purry, Towards modelling the impact of cyber attacks on a smart grid, Int. J. Secur. Netw. 6 (2011) 2, https://doi.org/10.1504/IJSN.2011.039629.
[34] X.X. Liu, J.X. Zhang, P.D. Zhu, Modeling cyber–physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory, Int. J. Crit. Infrastruct. Prot. 16 (2017) 13–25, https://doi.org/10.1016/j.ijcip.2016.11.002.
[35] O. Vuković, K.C. Sou, G. Dán, H. Sandberg, Network-aware mitigation of data integrity attacks on power system state estimation, IEEE J. Sel. Areas Commun. 30 (2012) 1108–1118, https://doi.org/10.1109/JSAC.2012.120709.
[36] L. Wei, A.I. Sarwat, W. Saad, S. Biswas, Stochastic games for power grid protection against coordinated cyber–physical attacks, IEEE Trans. Smart Grid 9 (2) (2018) 684–694, https://doi.org/10.1109/TSG.2016.2561266.
[37] M. Parandehgheibi, E. Modiano, D. Hay, Mitigating cascading failures in interdependent power grids and communication networks, 2014 IEEE International Conference on Smart Grid Communications (2015) 242–247, https://doi.org/10.1109/SmartGridComm.2014.7007653.
[38] J. Kim, L. Tong, On topology attack of a smart grid: undetectable attacks and countermeasures, IEEE J. Sel. Areas Commun. 31 (7) (2013) 1294–1305, https://doi.org/10.1109/JSAC.2013.130712.
[39] X. Lou, D.K.Y. Yau, H.H. Nguyen, B. Chen, Profit-optimal and stability-aware load curtailment in smart grids, IEEE Trans. Smart Grid 4 (2013) 1411–1420, https://doi.org/10.1109/TSG.2013.2249672.
[40] S. Soltan, M. Yannakakis, G. Zussman, Power grid state estimation following a joint cyber and physical attack, IEEE Trans. Control Netw. Syst. 5 (1) (2018) 499–512, https://doi.org/10.1109/TCNS.2016.2620807.
[41] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, C. Chen, Cyber–physical modeling and cyber-contingency assessment of hierarchical control systems, IEEE Trans. Smart Grid 6 (2015) 2375–2385, https://doi.org/10.1109/TSG.2014.2387381.
[42] J. Guo, Y.Q. Han, C.X. Guo, F.D. Lou, Y.B. Wang, Modeling and vulnerability analysis of cyber–physical power systems considering network topology and power flow properties, Energies 10 (2017).
[43] X.P. Ji, B. Wang, D.C. Liu, Z.Y. Dong, G. Chen, Z.S. Zhu, X.D. Zhu, X.T. Wang, Will electrical cyber–physical interdependent networks undergo first-order transition under random attacks? Phys. A: Stat. Mech. Appl. 460 (2016) 235–245, https://doi.org/10.1016/j.physa.2016.05.017.
[44] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, A. Nayak, Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory, IEEE 8th Conference on Industrial Electronics and Applications (ICIEA) (2013), https://doi.org/10.1109/ICIEA.2013.6566517.
[45] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028, https://doi.org/10.1038/nature08932.
[46] J.Q. Hu, J. Yu, J. De Cao, M. Ni, W.J. Yu, Topological interactive analysis of power system and its communication module: a complex network approach, Phys. A: Stat. Mech. Appl. 416 (2014) 99–111, https://doi.org/10.1016/j.physa.2014.08.015.
[47] J. Yan, H. He, Y. Sun, Integrated security analysis on cascading failure in complex networks, IEEE Trans. Inf. Forensics Secur. 9 (2014) 451–463, https://doi.org/10.1109/TIFS.2014.2299404.
[48] E.A. Lee, S.A. Seshia, Introduction to Embedded Systems: A Cyber–Physical Systems Approach, MIT Press, 2017.
[49] W.Z. Li, L. Xie, Z.L. Deng, Z.L. Wang, False sequential logic attack on SCADA system and its physical impact analysis, Comput. Secur. 58 (2016) 149–159, https://doi.org/10.1016/j.cose.2016.01.001.
[50] K. Schneider, C.C. Liu, J.P. Paul, Assessment of interactions between power and telecommunications infrastructures, IEEE Trans. Power Syst. 21 (2006) 1123–1130, https://doi.org/10.1109/TPWRS.2006.876692.
[51] O. Gursesli, A.A. Desrochers, Modeling infrastructure interdependencies using Petri nets, IEEE International Conference On Systems, Man And Cybernetics, IEEE (2003) 1506–1512, https://doi.org/10.1109/ICSMC.2003.1244625.
[52] J.-C. Laprie, K. Kanoun, M. Kaâniche, Modelling interdependencies between the electricity and information infrastructures, International Conference on Computer Safety, Reliability, and Security (2007), https://doi.org/10.1007/978-3-540-75101-4_5.
[53] X.X. Liu, P.D. Zhu, Y. Zhang, K. Chen, A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure, IEEE Trans. Smart Grid 6 (2015) 2435–2443, https://doi.org/10.1109/TSG.2015.2418280.
[54] P.A. Khand, System level security modeling using attack trees, 2009 2nd International Conference on Computer, Control and Communication IC4 2009 (2009), https://doi.org/10.1109/IC4.2009.4909245.
[55] P.A.S. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks, ISA Trans. 46 (2007) 583–594, https://doi.org/10.1016/j.isatra.2007.04.003.
[56] C.W. Ten, C.C. Liu, M. Govindarasu, Vulnerability assessment of cybersecurity for SCADA systems using attack trees, 2007 IEEE Power Engineering Society General Meeting PES (2007), https://doi.org/10.1109/PES.2007.385876.
[57] G.C. Dalton, R.F. Mills, J.M. Colombi, R.A. Raines, Analyzing attack trees using generalized stochastic Petri nets, 2006 IEEE Information Assurance Workshop (2006) 116–123, https://doi.org/10.1109/IAW.2006.1652085.
[58] N. Liu, J.H. Zhang, H. Zhang, W.X. Liu, Security assessment for communication networks of power control systems using attack graph and MCDM, IEEE Trans. Power Deliv. 25 (2010) 1492–1500, https://doi.org/10.1109/TPWRD.2009.2033930.
[59] Y.F. Wang, K.L. Gao, T. Zhao, J. Qiu, Assessing the harmfulness of cascading failures across space in electric cyber–physical system based on improved attack graph, Proc. CSEE 36 (2016) 1490–1499, https://doi.org/10.13334/j.0258-8013.pcsee.2016.06.004.
[60] Y. Zhang, L. Wang, Y. Xiang, C.W. Ten, Power system reliability evaluation with SCADA cybersecurity considerations, IEEE Trans. Smart Grid 6 (2015) 1707–1721, https://doi.org/10.1109/TSG.2015.2396994.
[61] S. Zonouz, C.M. Davis, K.R. Davis, R. Berthier, R.B. Bobba, W.H. Sanders, SOCCA: a security-oriented cyber–physical contingency analysis in power infrastructures, IEEE Trans. Smart Grid 5 (2014) 3–13, https://doi.org/10.1109/TSG.2013.2280399.
[62] Y.C. Zhang, L.F. Wang, Y.M. Xiang, C.W. Ten, Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation, IEEE Trans. Power Syst. 31 (2016) 4379–4394, https://doi.org/10.1109/TPWRS.2015.2510626.
[63] Z.H. Zhang, S.P. Gong, A.D. Dimitrovski, H.S. Li, Time synchronization attack in smart grid: impact and analysis, IEEE Trans. Smart Grid 4 (2013) 87–98, https://doi.org/10.1109/TSG.2012.2227342.
[64] S. Sridhar, M. Govindarasu, Model-based attack detection and mitigation for

automatic generation control, IEEE Trans. Smart Grid 5 (2014) 580–591, https://doi.org/10.1109/TSG.2014.2298195.
[65] X.L. Zhang, X.Y. Yang, J. Lin, G. Bin Xu, W. Yu, On data integrity attacks against real-time pricing in energy-based cyber–physical systems, IEEE Trans. Parallel Distrib. Syst. 28 (2017) 170–187, https://doi.org/10.1109/TPDS.2016.2546259.
[66] Q. Yang, L. Chang, W. Yu, On false data injection attacks against Kalman filtering in power system dynamic state estimation, Secur. Commun. Netw. 9 (2016) 833–849, https://doi.org/10.1002/sec.835.
[67] J. Yan, H. He, X. Zhong, Y. Tang, Q-learning-based vulnerability analysis of smart grid against sequential topology attacks, IEEE Trans. Inf. Forensics Secur. 12 (2017) 200–210, https://doi.org/10.1109/TIFS.2016.2607701.
[68] J. Bae, S. Lee, Y.-W. Kim, J.-H. Kim, Protection strategies against false data injection attacks with uncertain information on electric power grids, J. Electr. Eng. Technol. 12 (2017) 19–28, https://doi.org/10.5370/JEET.2017.12.1.019.
[69] K. Khanna, B.K. Panigrahi, A. Joshi, Data integrity attack in smart grid: optimised attack to gain momentary economic profit, IET Gener. Transm. Distrib. 10 (2016) 4032–4039, https://doi.org/10.1049/iet-gtd.2016.0350.
[70] H. Ye, W. Gao, Q. Mou, Y. Liu, Iterative infinitesimal generator discretization-based method for eigen-analysis of large delayed cyber–physical power system, Electr. Power Syst. Res. 143 (2017) 389–399, https://doi.org/10.1016/j.epsr.2016.10.016.
[71] A.K. Singh, R. Singh, B.C. Pal, Stability analysis of networked control in smart grids, IEEE Trans. Smart Grid 6 (2015) 381–390, https://doi.org/10.1109/TSG.2014.2314494.
[72] Y. Susuki, T.J. Koo, H. Ebina, T. Yamazaki, T. Ochi, T. Uemura, T. Hikihara, A hybrid system approach to the analysis and design of power grid dynamic performance, Proc. IEEE 100 (2012) 225–239, https://doi.org/10.1109/JPROC.2011.2165329.
[73] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, K. Butler-Purry, A framework for modeling cyber–physical switching attacks in smart grid, IEEE Trans. Emerg. Top. Comput. 1 (2013) 273–285, https://doi.org/10.1109/TETC.2013.2296440.
[74] S. Liu, B. Chen, T. Zourntos, D. Kundur, K. Butler-Purry, A coordinated multi-switch attack for cascading failures in smart grid, IEEE Trans. Smart Grid 5 (2014) 1183–1195, https://doi.org/10.1109/TSG.2014.2302476.
[75] A. Pahwa, S.A. DeLoach, B. Natarajan, S. Das, A.R. Malekpour, S.M. Shafiul Alam, D.M. Case, Goal-based holonic multiagent system for operation of power distribution systems, IEEE Trans. Smart Grid 6 (2015) 2510–2518, https://doi.org/10.1109/TSG.2015.2404334.
[76] M.S. Rahman, M.A. Mahmud, A.M.T. Oo, H.R. Pota, Multi-agent approach for enhancing security of protection schemes in cyber–physical energy systems, IEEE Trans. Ind. Inf. 13 (2017) 436–447, https://doi.org/10.1109/TII.;2016.2612645.
[77] A. Farraj, E. Hammad, D. Kundur, A cyber–physical control framework for transient stability in smart grids, IEEE Trans. Smart Grid 9 (2) (2018) 1205–1215, https://doi.org/10.1109/TSG.2016.2581588.
[78] J. Schiffer, F. Dörfler, E. Fridman, Robustness of distributed averaging control in power systems: time delays & dynamic communication topology, Automatica 80 (2017) 261–271, https://doi.org/10.1016/j.automatica.2017.02.040.
[79] M.D. Ilic, L. Xie, U.A. Khan, J.M.F. Moura, Modeling of future cyber–physical energy systems for distributed sensing and control, IEEE Trans. Syst. Man Cybern. A: Syst. Hum. 40 (2010) 825–838, https://doi.org/10.1109/TSMCA.2010.2048026.
[80] B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, Int. J. Crit. Infrastruct. Prot. 10 (2015) 3–17, https://doi.org/10.1016/j.ijcip.2015.04.001.
[81] B. Falahati, Y. Fu, L. Wu, Reliability assessment of smart grid considering direct cyber-power interdependencies, IEEE Trans. Smart Grid 3 (2012) 1515–1524, https://doi.org/10.1109/TSG.2012.2194520.
[82] B. Falahati, Y. Fu, Reliability assessment of smart grids considering indirect cyber-power interdependencies, IEEE Trans. Smart Grid 5 (2014) 1677–1685, https://doi.org/10.1109/TSG.2014.2310742.
[83] H. Lei, C. Singh, Power system reliability evaluation considering cyber-malfunctions in substations, Electr. Power Syst. Res. 129 (2015) 160–169, https://doi.org/10.1016/j.epsr.2015.08.010.
[84] M. Esmalifalak, G. Shi, Z. Han, L.Y. Song, Bad data injection attack and defense in electricity market using game theory study, IEEE Trans. Smart Grid 4 (2013) 160–169, https://doi.org/10.1109/TSG.2012.2224391.
[85] A. Delgadillo, J.M. Arroyo, N. Alguacil, Analysis of electric grid interdiction with line switching, IEEE Trans. Power Syst. 25 (2010) 633–641, https://doi.org/10.1109/TPWRS.2009.2032232.
[86] Z.Y. Li, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, Bilevel model for analyzing coordinated cyber–physical attacks on power systems, IEEE Trans. Smart Grid 7 (5) (2016) 2260–2272, https://doi.org/10.1109/TSG.2015.2456107.
[87] D. Shelar, S. Amin, Security assessment of electricity distribution networks under DER node compromises, IEEE Trans. Control Netw. Syst. 4 (2017) 23–36, https://doi.org/10.1109/TCNS.2016.2598427.
[88] L.B. Shi, Z. Jian, Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model, Autom. Electr. Power Syst. 40 (2016) 99–105, https://doi.org/10.7500/AEPS20160510002.
[89] Y. Yuan, F.C. Sun, H.P. Liu, Resilient control of cyber–physical systems against intelligent attacker: a hierarchal stackelberg game approach, Int. J. Syst. Sci. 47 (2016) 2067–2077, https://doi.org/10.1080/00207721.2014.973467.
[90] K. Zhu, M. Chenine, L. Nordstrom, ICT architecture impact on wide area monitoring and control systems' reliability, IEEE Trans. Power Deliv. 26 (2011) 2801–2808, https://doi.org/10.1109/TPWRD.2011.2160879.
[91] M. Baran, R. Sreenath, N.R. Mahajan, Extending EMTDC/PSCAD for simulating agent-based distributed applications, IEEE Power Eng. Rev. 22 (2002) 52–54, https://doi.org/10.1109/MPER.2002.4311887.
[92] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, S. Hariri, A testbed for analyzing security of SCADA control systems (TASSCS), IEEE PES Innovative Smart Grid Technologies Conference Europe (2011), https://doi.org/10.1109/ISGT.2011.5759169.
[93] V. Liberatore, A. Al-Hammouri, Smart grid communication and co-simulation, IEEE 2011 EnergyTech (2011), https://doi.org/10.1109/EnergyTech.2011.5948542.
[94] M. Lévesque, D.Q. Xu, G. Joós, M. Maier, Communications and power distribution network co-simulation for multidisciplinary smart grid experimentations, SCS/ACM Spring Simulation Multi-conference (2012) 1–7.
[95] X.W. Sun, Y. Chen, J.T. Liu, S.W. Huang, A co-simulation platform for smart grid considering interaction between information and power systems, 2014 IEEE PES Innovative Smart Grid Technologies Conference (2014), https://doi.org/10.1109/ISGT.2014.6816423.
[96] H. Georg, S.C. Müller, N. Dorsch, C. Rehtanz, C. Wietfeld, INSPIRE: integrated co-simulation of power and ICT systems for real-time evaluation, 2013 IEEE International Conference on Smart Grid Communications (2013) 576–581, https://doi.org/10.1109/SmartGridComm.2013.6688020.
[97] R. Bottura, A. Borghetti, F. Napolitano, C.A. Nucci, ICT-power co-simulation platform for the analysis of communication-based volt/var optimization in distribution feeders, 2014 IEEE PES Innovative Smart Grid Technologies Conference (2014), https://doi.org/10.1109/ISGT.2014.6816425.
[98] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, Y. Wu, Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance, IEEE Power and Energy Society General Meeting (2015), https://doi.org/10.1109/PESGM.2015.7286238.
[99] J. Nutaro, P.T. Kuruganti, L. Miller, S. Mullen, M. Shankar, Integrated hybrid-simulation of electric power and communications systems, 2007 IEEE Power Engineering Society General Meeting (2007), https://doi.org/10.1109/PES.2007.386202.
[100] C.M. Davis, J.E. Tate, H. Okhravi, C. Grier, T.J. Overbye, D. Nicol, SCADA cyber security testbed development, 2006 38th Annual North American Power Symposium (2006) 483–488, https://doi.org/10.1109/NAPS.2006.359615.
[101] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour, S. Shi, A simplified co-simulation model to investigate impacts of cyber-contingency on power system, IEEE Trans. Smart Grid 1 (2017), https://doi.org/10.1109/TSG.2017.2675362.
[102] Core IEC Standards, Int. Electrotech. Comm. http://www.iec.ch/smartgrid/standards/. (Accessed 29 May 2018).
[103] Y. Tang, X. Han, Y.J. Wu, Y. Ju, X. Zhou, M. Ni, Electric power system vulnerability assessment considering the influence of communication system, Proc. CSEE 35 (2015) 6066–6074, https://doi.org/10.13334/j.0258-8013.pcsee.2015.23.013.
[104] M.S. Rahman, H.R. Pota, M.A. Mahmud, M.J. Hossain, T.F. Orchi, Distributed multi-agent scheme to enhance cyber security of smart power grids, IEEE Power and Energy Society General Meeting (2015), https://doi.org/10.1109/PESGM.2015.7286316.
[105] M.X. Cheng, M. Crow, Q. Ye, A game theory approach to vulnerability analysis: integrating power flows with topological analysis, Int. J. Electr. Power Energy Syst. 82 (2016) 29–36, https://doi.org/10.1016/j.ijepes.2016.02.045.
[106] J. Yan, C.C. Liu, M. Govindarasu, Cyber intrusion of wind farm SCADA system and its impact analysis, 2011 IEEE/PES Power Systems Conference and Exposition (2011), https://doi.org/10.1109/PSCE.2011.5772593.
[107] E. Moradi-Pari, N. Nasiriani, Y.P. Fallah, P. Famouri, S. Bossart, K. Dodrill, Design, modeling, and simulation of on-demand communication mechanisms for cyber–physical energy systems, IEEE Trans. Ind. Inf. 10 (4) (2014) 2330–2339, https://doi.org/10.1109/TII.2014.2326080.
[108] G. Celli, P.A. Pegoraro, F. Pilo, G. Pisano, S. Sulis, DMS cyber–physical simulation for assessing the impact of state estimation and communication media in smart grid operation, IEEE Trans. Power Syst. 29 (2014) 2436–2446, https://doi.org/10.1109/TPWRS.2014.2301639.
[109] R. Liu, C. Vellaithurai, S.S. Biswas, T.T. Gamage, A.K. Srivastava, Analyzing the cyber–physical impact of cyber events on the power grid, IEEE Trans. Smart Grid 6 (2015) 2444–2453, https://doi.org/10.1109/TSG.2015.2432013.
[110] A. Stefanov, C.C. Liu, M. Govindarasu, S.S. Wu, SCADA modeling for performance and vulnerability assessment of integrated cyber–physical systems, Int. Trans. Electr. Energy Syst. 25 (2015) 498–519, https://doi.org/10.1002/etep.1862.
[111] T. Yi, L. Feng, W. Qi, C. Bin, N. Ming, Overview of the co-simulation methods for power and communication system, 2016 IEEE International Conference on Real-Time Computing and Robotics (RCAR) (2016), https://doi.org/10.1109/RCAR.2016.7784007.
[112] H. Georg, S.C. Müller, C. Rehtanz, C. Wietfeld, Analyzing cyber–physical energy systems: the INSPIRE cosimulation of power and ICT systems using HLA, IEEE Trans. Ind. Inf. 10 (2014) 2364–2373, https://doi.org/10.1109/TII.2014.2332097.
[113] X. Wang, G. Zhu, R. He, M. Tian, Z. Dong, D. Dai, J. Long, L. Zhao, Q. Zhang, Survey of cascading failures in cyber physical power system based on complex network theory, Power Syst. Technol. 41 (2017) 2947–2956, https://doi.org/10.13335/j.1000-3673.pst.2017.0044.
[114] D. Liu, W.X. Sheng, Y. Wang, Y.M. Lu, C. Sun, Key technologies and trends of cyber physical system for power grid, Proc. CSEE 35 (2015) 3522–3531, https://doi.org/10.13334/j.0258-8013.pcsee.2015.14.006.
[115] J.H. Zhao, F.S. Wen, Y.S. Xue, Z.Y. Dong, Modeling analysis and control research framework of cyber physical power systems, Autom. Electr. Power Syst. 35

(2011) 1–8.
[116] Z.X. Chen, Y.J. Zhang, Z.X. Cai, L.C. Li, P. Liu, Characteristics and technical challenges in energy Internet cyber–physical system, IEEE PES Innovative Smart Grid Technologies Conference Europer (2017), https://doi.org/10.1109/ISGTEurope.2016.7856183.
[117] T.J. Pu, K.W. Liu, N.S. Chen, X.J. Ge, J.C. Yu, D. Wang, W. Wang, Design of ADN based urban energy internet architecture and its technological issues, Proc. CSEE 35 (2015) 3511–3521, https://doi.org/10.13334/j.0258-8013.pcsee.2015.14.005.
[118] Y. Wang, D. Liu, Y. Lu, Research on hybrid system modeling method of cyber physical system for power grid, Proc. CSEE 36 (2016) 1464–1470, https://doi.org/10.13334/j.0258-8013.pcsee.2016.06.001.
[119] Z.Y. Zeng, D. Liu, Study on cyber–physical system modeling on coordinated control of photovoltaic generation and battery energy storage system, Power Syst. Technol. 37 (2013) 1506–1513, https://doi.org/10.13335/j.1000-3673.pst.2013.06.015.
[120] S. Ma, Z. Xu, L.M. Wang, Set theory based modeling method of cyber physical system for power grid, Autom. Electr. Power Syst. 41 (2017), https://doi.org/10.7500/AEPS20160804007.