frontiers in Energy Research

REVIEW
published: 03 May 2021
doi: 10.3389/fenrg.2021.642997

Review of Modeling and Simulation Methods for Cyber Physical Power System

Hong Fan[1,2], Hongxiang Wang[2], Shiwei Xia[1], Xuan Li[3], Pengfei Xu[4] and Yuhan Gao[5]*

[1] State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Beijing, China, [2] Department of Electrical Engineering, Shanghai University of Electric Power, Shanghai, China, [3] State Grid Economic and Technological Research Institute Co., Ltd., Beijing, China, [4] Shanghai Sermatec Energy Technology Co., Ltd., Shanghai, China, [5] College of Energy and Materials Engineering, Taiyuan University of Science and Technology, Jincheng, China

With the development of informatization and intellectualization technology, the power system has become the cyber-physical power system (CPPS) with deep integration of the cyber side and the physical side. As the support system of smart grids with new forms and features, the CPPS considers the coupling relationship between the communication network and the physical power grid, and is a research hotspot in the field of smart grids. This paper provides an overview of the CPPS framework and describes the interaction between the communication network and the physical power grid. Then the mainstream modeling and simulation methods of CPPS are summarized, and the advantages and disadvantages of each method are pointed out. In the end, the paper looks forward to the possible research directions of CPPS in the future. The article provides researchers with different perspectives on the dynamic model and simulation methods of CPPS.

Keywords: cyber physical power system, CPPS framework, interaction, communication network, modeling and simulation methods

OPEN ACCESS

Edited by:
Yang Li,
Northeast Electric Power University, China

Reviewed by:
Jia Cui,
Shenyang University of Technology, China
Lei Wang,
Northeast Electric Power University, China

***Correspondence:**
Shiwei Xia
s.w.xia@ncepu.edu.cn

Specialty section:
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

Received: *17 December 2020*
Accepted: *06 April 2021*
Published: *03 May 2021*

Citation:
Fan H, Wang H, Xia S, Li X, Xu P and Gao Y (2021) Review of Modeling and Simulation Methods for Cyber Physical Power System. Front. Energy Res. 9:642997. doi: 10.3389/fenrg.2021.642997

INTRODUCTION

With the continuous integration of computing, communication and control technologies in smart grids, the composition of power system is becoming increasingly complex, which makes the power system become the cyber-physical power system (CPPS) with deep integration of information and physics (Su et al., 2017). It includes not only the traditional physical grid but also the power communication network formed by the information acquisition units, the control decision-making units, etc. The arrival of the 5G era will inevitably make the power communication network more complex and play a more important role in the power system. At the same time, the impact of communication system faults on the physical power grid will be more serious (Yu and Xue, 2016; Xia et al., 2018; Tao et al., 2020; Zerihun et al., 2020; Lu et al., 2021). The communication network and the physical power grid have formed a strong coupling closed-loop system. The events that affect the performance of the communication network, such as data loss, transmission delay (Pall et al., 2016; Xia et al., 2019a,b), channel interruption, and physical faults of communication equipment (Li et al., 2019), will directly or indirectly affect the situation awareness (Xi et al., 2019; Xia et al., 2019c; Xiao et al., 2019) and control command's execution of the physical power grid, resulting in protection's malfunction, and in serious cases, it will cause cascading failures, such as the blackout

in the United States and Canada in 2003 and the blackout in Ukraine in 2015. Consequently, more attention is paid to the interaction between the physical power grid and the power communication network in the research of CPPS. However, CPPS is a multi-source heterogeneous system composed of continuous and discrete processes, which makes it difficult to analyze the interactive processes quantitatively. Therefore, how to realize the quantitative analysis of CPPS is the key challenge to CPPS research, which has attracted some scholars to make some new attempts.

Since the concept of cyber physical system was proposed by the National Science Foundation in 2006, with the in-depth study of smart grids, scholars at home and abroad have gradually linked the power grid with cyber physical system. At first, in order to realize the collaborative analysis of physical power grid and power communication network, Dr. Kenneth Hopkinson built EPOCHS in 2006, a cyber physical co-simulation platform, using the existing commercial simulation software. This is an attempt by researchers to conduct joint research on physical power grid and communication network from the perspective of co-simulation when the relevant theories of CPPS have not been established. In 2010, the research team led by Academician Yusheng Xue of the Chinese Academy of Engineering proposed the architecture, key technologies, and challenges of CPPS. After that, Chinese scholars began to study the related theories of CPPS. Academician Yusheng Xue and Associate Professor Qinglai Guo of Tsinghua University proposed the different modeling methods of CPPS, which promoted the theoretical development of CPPS. Applying CPPS modeling theories for quantitative analysis of network risk is a hot research topic. The dynamic model of CPPS network risk propagation was established based on the percolation theory in Qu et al. (2018), and the survival function was used to quantify the risk propagation threshold and predict the critical point of risk outbreak. The CPPS risk area prediction model was proposed by using the dependent markov chain to predict the probability of the risk occurrence (Qu et al., 2020). At present, the research related to CPPS mainly focuses on the following directions: (1) research on the fusion modeling methods of communication network and physical power grid; (2) research on the hybrid simulation methods. (3) Research on the network security issues; this paper reviews the related research of CPPS and summarizes the existing problems in the current research from the perspective of modeling and simulation.

The paper is organized as follows: the framework of CPPS and the interaction between the communication network and the physical power grid are introduced in section "Framework of CPPS," while the modeling and simulation methods of CPPS are respectively summarized in section "Modeling Methods of CPPS" and "CPPS Simulation Methods." Section "Conclusion" concludes the paper with the future research suggested in the "Future Work" section.

FRAMEWORK OF CPPS

On the whole, the CPPS is mainly composed of two parts: physical power grid and power communication network. In the physical layer, electrical quantities are converted into virtual signals through the data acquisition, and then this data is transmitted to the information layer through wired or wireless networks. In the information layer, the control instructions are output through the data analysis and decision-making processes of control units, so as to control the equipment of the physical layer. Then, the state of the physical layer changes and the new state information is transmitted to the information layer, thus forming a complex closed-loop system of perception – analysis – decision-making – execution. In these processes, the interaction between energy flow and information flow is realized. In essence, the energy flow is driven by the information flow to realize the optimal configuration of electric energy. The abnormal operation of any of the four processes will affect the performance of the whole closed-loop system. Only when the interaction between physical power grid and power communication network is fully considered and the interaction mechanism is studied, can the CPPS be correctly modeled and the dynamic characteristics of CPPS be correctly simulated (Liu et al., 2015; Guo J. et al., 2016; Farraj et al., 2018; Rana and Bo, 2020). The general framework of CPPS is illustrated in **Figure 1**. The two subsystems, i.e., the power communication network and physical power grid, are described in detail in sections "Power Communication Network" and "Physical Power Grid," respectively.

Power Communication Network

The power communication network is mainly composed of terminal equipment, switching equipment and transmission link. In the research of CPPS, the data communication process of the power communication network is mainly concerned. **Figure 2** illustrates the data communication process. A simplex communication process is as follows: sending – source coding – channel coding – modulation – channel transmitting – demodulation – channel decoding – source decoding – receiving. In the actual power communication network, the full duplex communication and half-duplex communication are often carried out (Tang and Wang, 2015), and the channels include the power line carrier channels, optical fiber channels and other wired channels, as well as microwave communication, mobile communication, satellite communication and other wireless channels, which makes the actual power communication network more complex.

The main function of data communication is to realize the measurement of the power system's operating state parameters and the control of operation equipment on the support of supervisory control and data Acquisition (SCADA) system. The SCADA relies on telecontrol technology to complete telemetering, teleindication, telecommand, and teleadjusting of power system. The telecontrol system is composed of remote terminal unit (RTU) at the slave station (power station and substation), front-end processor at the master station (control center) and telecontrol channel (Liu and Liu, 2016). In the telecontrol system, the power flow information, the opening and closing state information of circuit breakers and disconnectors, and the control instructions information of corresponding operating equipment is mainly concerned. As shown in **Figure 2**, the RTU collects the real-time operation information of the

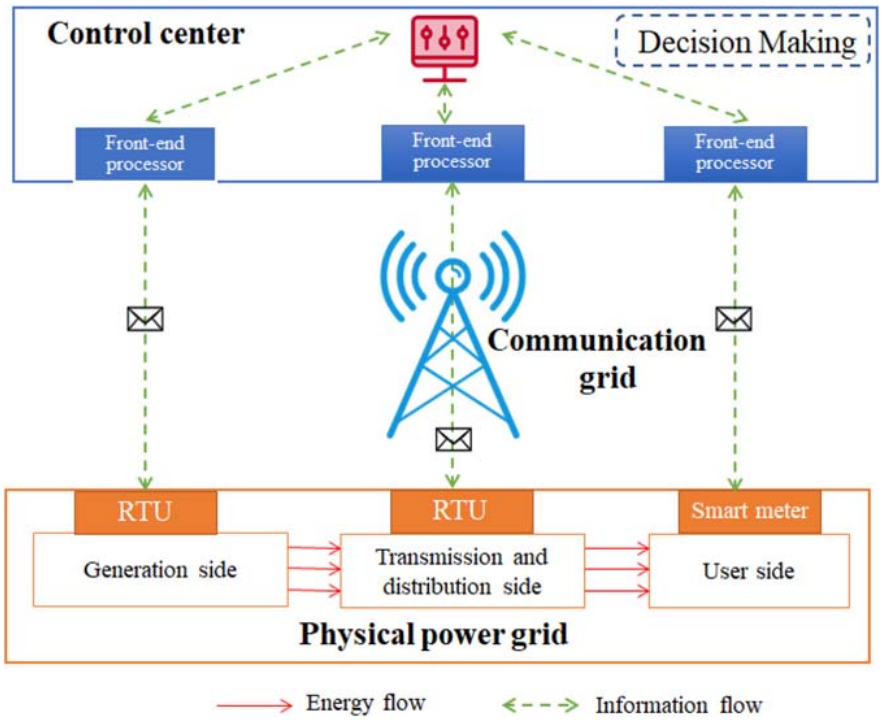

FIGURE 1 | Framework of CPPS.

power grid required by the dispatching center from the slave station, and sends it to the front-end processor of the dispatching center. The front-end processor forward the real-time operation information to the control center, and the control center sends remote control or remote regulation instructions to RTU through the front-end processor after making control decisions. It is difficult to fully consider the whole data communication process in the research of CPPS, so it can be simplified reasonably according to the above processes, ignoring the specific and complex information transformation process, such as coding and modulation, and only considering the data content, transmission direction and channels from a macro perspective. The front-end processor can be regarded as the communication sub-station node, and then the whole power communication network can be abstracted into three parts, i.e., communication sub-station node, uplink channel and downlink channel, in which the RTU and front-end processor adopt point-to-point configuration (Wang C. et al., 2020). Therefore, the data communication process can be described by matrix, which greatly simplifies the communication process, and provides an idea for introducing the communication process into power system modeling.

Physical Power Grid

The physical power grid is mainly composed of five parts: power generation, transmission, transformation, distribution, and utilization. It can be abstracted as a large grid structure composed of nodes and branches, in which the energy flow flows between nodes and branches. In the CPPS research, the power flow information and line opening and closing information that characterizes the energy flow are needed. In addition, temperature, humidity, wind speed, light intensity and other non-electrical information that may affect the operation of equipment is also needed. This information will be uploaded to the control center through the power communication network, and then the grid status will be updated according to the control center's instructions.

The modeling, simulation, and analysis methods of the physical power grid have been quite mature, but these methods are no longer applicable when considering the information flow driven by discrete events. The main content of CPPS research is to study the interaction between the physical power grid and the power communication network, including the impact of the physical power grid on the communication network and the impact of the communication network on the physical power grid. Due to the limitation of interdisciplinary, the current research focuses on the latter. Network security is a research hotspot in the field, for example, the false data injection attack (FDIA) (Kang et al., 2018). The FDIA modifies the real-time operation data of power grid by injecting false data into measuring equipment and cheating bad data monitoring, which leads to control center to make wrong control instructions based on the false measurement data. The current research is devoted to the risk assessment of network attacks and minimizes the impact of network attacks on the physical power grid (Srivastava et al., 2018). The genes extraction model was proposed in Qu et al. (2021) to extract the key characteristics of FDIA and accurately identify FDIA through the uniqueness of the FDIA genes. In addition to network attacks, self-failure of communication

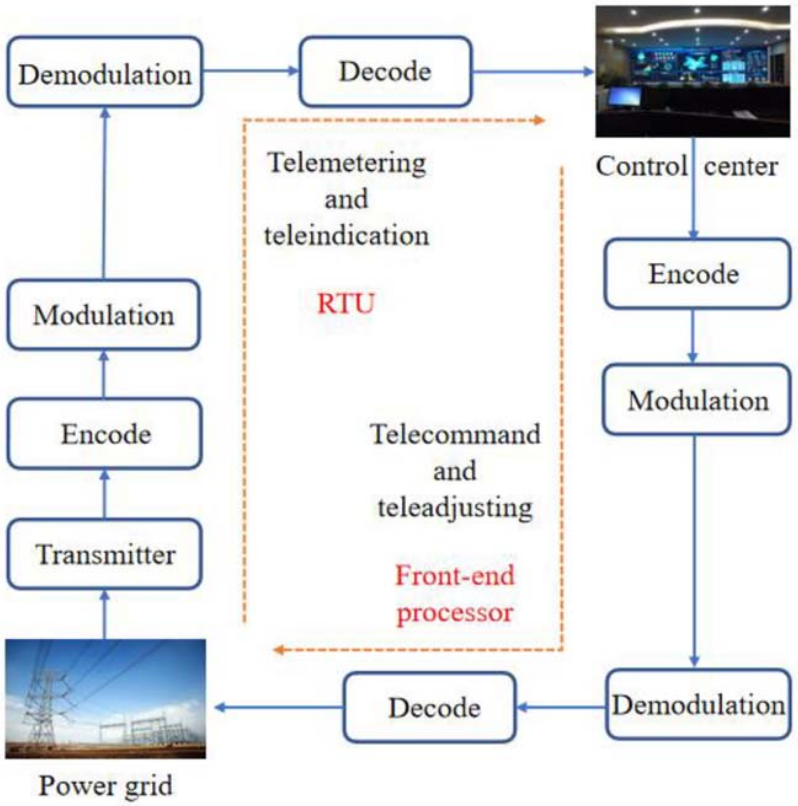

FIGURE 2 | Data communication process.

network or other outside interference may also lead to data transmission error, transmission delay, transmission interruption or transmission dislocation. These failures may lead to cascading failures of the power system and worsen the operation of the power system, which needs to be evaluated in detail (Calvo et al., 2018). To study the impact of these problems on the physical grid, the quantitative analysis should be carried out through CPPS modeling.

MODELING METHODS OF CPPS

In CPPS, the physical system is a continuous system driven by time, while the information system is a discrete system driven by events, which makes the CPPS a heterogeneous system with continuous and discrete coexistence. In CPPS modeling, the coupling relationship between the information system and the physical system should be considered, and the continuous and discrete processes should be unified. As the existing modeling methods of the physical power grid are very mature, and for power system researchers, the modeling of power communication part belongs to an interdisciplinary problem, which brings some research challenges. Therefore, more attention is paid to the research of the communication system modeling methods and cyber physical fusion modeling methods in the research of CPPS modeling methods. Three mainstream modeling methods of CPPS are summarized: i.e., modeling based on incidence characteristic matrix, information flow-energy flow hybrid model and modeling based on theories of hybrid system.

Modeling Based on Incidence Characteristic Matrix

The power communication network can be represented by a digraph composed of data nodes and directed branches (Xin et al., 2015; Guo Q. et al., 2016). The data nodes represent the data sets of input and output information of various modules in the power system, and the directed branches represent the process of information processing and transmitting. Among them, the information processing and transmitting process can be modeled according to the mapping relationship between input and output, and the topological relationship between nodes and branches can be reflected by the node branch incidence matrix, thus establishing a simplified model of the entire communication network. By modifying the elements of the node branch incidence matrix, the corresponding communication fault can be created, such as channel interruption, data loss, etc. The incidence characteristic matrix can also be extended to establish a complete CPPS model. The connection among the power grid nodes, secondary equipment nodes and communication nodes in CPPS can be established by using the incidence characteristic matrix, which built a bridge between the physical layer and information

layer of CPPS (Li M. et al., 2020). The elements in the matrix are represented by a multivariate array, which can include the relationship between nodes and branches, communication delay and so on, and the interaction between information and physics can be quantitatively described by the multivariate array. The topological relationship of the communication network or the coupling relationship between information and physical system can be expressed by the matrix, which is convenient for mathematical analysis and has high calculation efficiency by power flow calculation. If the CPPS is divided into physical layer, secondary device layer and information layer, and consists of n power system nodes, k secondary device nodes and m information nodes, respectively, the general model of CPPS based on incidence characteristic matrix can be mathematically expressed as follows:

(a) **Communication network model $\mathbf{C_{m \times m}}$:** The diagonal element C_{ii} represents the communication node, the non-diagonal element C_{ij} represents the communication branch, and the element $C_{ij} = \left[T_{ij}\ P_{B,ij}\ P_{M,ij} \cdots \right]$ represents the communication performance such as the communication delay, communication interruption probability and communication error probability between i and j.

(b) **Secondary device-communication node model $\mathbf{(S-C)_{k \times m}}$/Communication node-secondary device model $\mathbf{(C-S)_{m \times k}}$:** $(S-C)_{k \times m}$ indicates the process of uploading information and $(C-S)_{m \times k}$ indicates the process of downloading instructions. The element $(S-C)_{ij} = \left[(S-C)_{TP,ij}\ (S-C)_{T,ij}\ (S-C)_{PB,ij} \cdots \right]$ indicates whether there is communication, communication delay, communication interruption probability and other communication performance between the communication j node and the secondary device node i. $(C-S)_{ij}$ is similar to $(S-C)_{ij}$.

(c) **Secondary device node model $\mathbf{(S_{ii})_{k \times k}}$:** $(S_{ii})_{k \times k}$ describes the information processing performance of the secondary equipment node with the multivariate array $S_{ii} = \left[F_{ii}\left(a_{input}\right)\ T_{ii}\left(F_{ii}\right)\ P_{ii}\left(F_{ii}\right) \cdots \right]$. Among them, $F_{ii}\left(a_{input}\right)$ is the information processing algorithm, $T_{ii}\left(F_{ii}\right)$ and $P_{ii}\left(F_{ii}\right)$ are the information processing delay and information processing error probability determined by the performance of the information processing algorithm, respectively.

(d) **Secondary device network model $\mathbf{S_{k \times k}}$:** The diagonal element of $S_{k \times k}$ is S_{ii}, and the non-diagonal element is the performance of the communication channel between the secondary device nodes. When two nodes can communicate, the communication performance is calculated by the hybrid algorithm of $(S_{ii})_{k \times k}$, $(S-C)_{k \times m}/(C-S)_{m \times k}$, and $C_{m \times m}$. When there is no communication between two nodes, the corresponding element is $\left[0\ 0\ 0 \cdots \right]$.

(e) **Physical-secondary device model $\mathbf{(P-S)_{n \times k}}$/ Secondary device-physical model $\mathbf{(S-P)_{k \times n}}$:** $(P-S)_{n \times k}$ and $(S-P)_{k \times n}$, respectively represent the relationship between power system nodes and secondary device nodes in the data acquisition process and the instruction issuance process. The elements of $(P-S)_{n \times k}$ and $(S-P)_{k \times n}$ are similar to $(S-C)_{ij}$ and $(C-S)_{ij}$. The multivariate array of diagonal elements is $\left[1\ 1\ 1 \cdots \right]$.

(f) **Secondary device-information node model $\mathbf{(S-I)_{k \times l}}$/information node-secondary device model $\mathbf{(I-S)_{l \times k}}$:** $(S-I)_{k \times l}$ and $(I-S)_{l \times k}$, respectively represent the relationship between secondary device nodes and information nodes in the data acquisition process and the instruction issuance process. The elements of $(S-I)_{k \times l}$ and $(I-S)_{l \times k}$ are similar to $(P-S)_{n \times k}$ and $(S-P)_{k \times n}$.

(g) **Physical-information node coupling model $\mathbf{(P-I)_{n \times l}}$/information-physical node coupling model $\mathbf{(I-P)_{l \times n}}$:** $(P-I)_{n \times l}$ and $(I-P)_{l \times n}$ reflect the coupling relationship between power system nodes and information nodes, which can be obtained through the hybrid algorithm of $S_{k \times k}$, $(P-S)_{n \times k}/(S-P)_{k \times n}$ and $(S-I)_{k \times l}/(I-S)_{l \times k}$.

However, the information that the matrixes can reflect is limited, so it is not able to conduct detailed quantitative analysis on CPPS and only the influence of simple communication failures on the power system can be studied. In order to study the interaction between communication network and physical power grid in detail, the most accurate method is to establish a detailed information flow – energy flow hybrid model.

Information Flow – Energy Flow Hybrid Model

The information flow – energy flow hybrid model of the whole CPPS is an extension of the power flow equation, including the following four parts (Guo Q. et al., 2016; Wang et al., 2019; Xu et al., 2019), i.e., the energy flow calculation model expressed by power flow equation, the energy flow to information flow calculation model that describes the measurement process, the information flow calculation model that describes the information-processing process (Wang T. et al., 2020) and the information flow to energy flow calculation model that describes the control process (Xin et al., 2017). The equations in the above four models can be combined to form a complete information flow – energy flow hybrid model of CPPS based on the power flow equation, which includes the mapping between physical quantities and information quantities. The contribution of information flow to the operation of the physical power grid and the impact of information failure on energy flow can be calculated quantitatively by information-physical coupling sensitivity formed by the hybrid model. The general information flow – energy flow hybrid model of CPPS can be mathematically expressed as follows:

(a) **Energy flow model:** the energy flow model represents the power flow of power system in a control cycle N to combine

the following discrete information flow model, that is,

$$\mathrm{f}\left(x\left(N+1\right),u\left(N\right),D\left(N+1\right),p,A\right)=0 \quad (1)$$

where x is the state variable, u is the control variable, D is the disturbance variables, p is the network element parameters and A is the node-branch incidence matrix.

(b) **Energy flow to information flow model:** this model corresponds to the telemetering and teleindication process from the physical state to the virtual signal, that is,

$$x\left(N\right)\rightarrow z\left(N\right)=\Phi\cdot x\left(N\right)=\Phi\cdot\left[U,\theta,P,Q,\pi\right]^{T} \quad (2)$$

where $z(N)$ is the measurement column vector, Φ is the measurement mapping matrix, $[U, \theta, P, Q, \pi]$, respectively represent voltage amplitude, phase angle, active power, reactive power, and switch status.

(c) **Information flow model:** this model corresponds to the optimization decision-making process of the information layer. After the control center receives the measured variable$z(N)$, it generates the control command $\mathrm{y}(N)$ according to the optimization function, that is,

$$\mathrm{y}\left(N\right)=F\left(z\left(N\right)\right)=\arg min\left\{f\left(y,z\right)|g\left(y,z\right)\leq h\left(y,z\right)\right\} \quad (3)$$

where $F=\arg min\left\{f\left(y,z\right)|g\left(y,z\right)\leq h\left(y,z\right)\right\}$ is the general form of the decision-making function of the control center.

(d) **Information flow to energy flow calculation model:** this model represents the telecommand and teleadjusting process, transforming control commands $\mathrm{y}(N)$ into actual physical control quantities $u(N)$ through the control mapping matrix C, that is,

$$\mathrm{y}\left(N\right)\rightarrow u\left(N\right)=C\cdot\mathrm{y}\left(N\right) \quad (4)$$

(e) **Information flow – energy flow hybrid model:** this model can be obtained by combining the above 4 models, that is,

$$\mathrm{f}\left(x\left(N\,1\right),C\cdot F\left(\Phi\cdot x\left(N\right)\right),D\left(N\,1\right),p,A\right)=0 \quad (5)$$

Compared to the method in section "Modeling Based on Incidence Characteristic Matrix," the hybrid model is more detailed and the whole closed-loop process of CPPS can be reflected theoretically. However, because the composite function contains both linear and nonlinear parts, the information flow with nonlinear problem needs to be carried out a partition and equivalence in the solution, and the timing characteristics of the model need to be considered, which makes the solution process complicated. Therefore, it has a strong research significance and prospect to study the corresponding cyber physical hybrid calculation method.

Modeling Based on Theories of Hybrid System

Apart from the above two modeling methods, some researchers proposed to apply the theories of hybrid system in control field to CPPS fusion modeling. Among them, due to the simple logic of the finite state machine (FSM) modeling method, it is more suitable for preliminary application in the CPPS fusion modeling. The FSM can be used to simulate the conversion of discrete processes in a communication network, and realize the combination of the states of the power system and information system in CPPS. The general FSM model can be represented by a multi-group $\mathrm{H}=\{X, Q, G, E, I\}$, where X represents the set of continuous dynamic parts, Q represents the set of discrete dynamic parts, G is the switching logic set of discrete events, E is the state transition function, and I is the initial state set. For each discrete process, its dynamic model can be established by the differential equation, that is,

$$\dot{x\left(t\right)}=\begin{cases}A_1x\left(t\right)+B_1u\left(t\right)\ if\ L_1\\ A_2x\left(t\right)+B_2u\left(t\right)\ if\ L_2\\ \quad\vdots\\ A_nx\left(t\right)+B_nu\left(t\right)\ if\ L_n\end{cases} \quad (6)$$

where $x(t)$ is the system status, $u(t)$ is the control input, A is the system matrix, B is the output matrix, and L is the switching logic between discrete states.

Since the transitions of event-driven continuous dynamic processes often exist in CPPS, which conforms to the application scenario of FSM. In Chen et al. (2019), the physical process and information process of frequency modulation system are divided into several different states which are related to each other. Different states correspond to different control strategies. The transition between different state depends on whether the system frequency exceeds the limit and whether the frequency collection time-out. By modeling the continuous process of each state and event-driven, the quantitative analysis of the cyber physical interaction of frequency modulation system can be realized. This method that combines the physical state and information state of power system by state transitions is simple in logic and easy to implement. It is suitable for analyzing small systems with multiple working states. Zhao et al. (2011) established a steady-state model of information system including the balance equation of information flow and the maximum information flow constraint of nodes and lines, and established the dynamic model of information system represented by differential equation by using the theory of FSM. Since the information system is established based on algebraic and differential equations, the information system and physical system model can be solved simultaneously. Since the FSM model cannot reflect the optimal decision-making function in CPPS, it can be combined with mixed logic dynamic (MLD) theory to transform the FSM model into inequality constraints through logical variables, so as to realize the optimal decision-making function in CPPS. The general expression of the MLD model can be expressed as follows.

$$\begin{cases}x\left(t+1\right)=Ax\left(t\right)+B_1u\left(t\right)+B_2\delta\left(t\right)+B_3z\left(t\right)\\ y\left(t\right)=Cx\left(t\right)+D_1u\left(t\right)+D_2\delta\left(t\right)+D_3z\left(t\right)\\ E_2\delta\left(t\right)+E_3z\left(t\right)\leq E_1u\left(t\right)+E_4x\left(t\right)+E_s\end{cases} \quad (7)$$

where $\delta(t)$ is the auxiliary logic variable, $z(t)$ is the auxiliary continuous variable, $y(t)$ is the output vector, and E is the matrix corresponding to the constraints.

With the MLD theory, a control analysis model of CPPS was established in Wang et al. (2016) based on the FSM and MLD model. The FSM was used to establish the operation strategy model under each state in the form of piecewise continuous equation, and then the FSM model was transformed into the MLD description model described by logical variables, which realized the transformation from continuous process to discrete process, thus realizing the integration of primary power system and information control system. This fusion modeling method can use the mathematical method of traditional control theory to solve the optimal control problem of CPPS. As the communication system involves a variety of communication strategies and modes, it is difficult to model in detail by using these theories of hybrid system in the control field and these ideas are not universal in CPPS modeling (Guo et al., 2019). In **Table 1**, the three modeling methods are compared.

CYBER-PHYSICAL POWER SYSTEM SIMULATION METHODS

Although the fusion model of CPPS can be established now, the heterogeneous nature of CPPS makes it difficult to develop a corresponding solution algorithm. Therefore, at present, simulation is the main method of CPPS quantitative analysis. The core of CPPS simulation is to simulate correctly the interaction between the actual physical power grid and communication network. It is necessary to provide a simulation platform for the dynamic study of the impact of physical power grid fault on the communication network and the impact of communication system fault on the power system. According to the different simulation schemes (Hopkinson et al., 2006; Hua et al., 2011, 2012; Celli et al., 2014; Lai et al., 2014; Tang et al., 2016; Sun et al., 2019; Attarzadeh-Niaki and Sander, 2020), the CPPS simulation methods can be divided into three categories, i.e., cyber physical co-simulation, semi-physical simulation, embedded simulation.

Cyber Physical Co-simulation

Cyber physical co-simulation is to build a collaborative simulation platform by using mature power system simulation software and communication system simulation software, respectively, and realizes information interaction under the condition of independent simulation. Cyber physical co-simulation method is the research hotspot of CPPS simulation at present, because it is difficult to develop CPPS integrated simulation platform that will take a long time and the final simulation effect is not easy to guarantee. On the basis of the existing simulation software, it is simple to carry out physical power grid simulation and communication network simulation separately, and the simulation accuracy of the existing simulation platform can be guaranteed after years of development and wide application. Researchers can mainly solve data exchange problem and time synchronization problem of different simulation software. According to whether real-time simulation can be realized, co-simulation is divided into non-real-time co-simulation and real-time co-simulation.

Non-real-Time Co-simulation

In the initial research stage of CPPS simulation method, a research group developed an agent interface of PSCAD/EMTDC, which achieved the data communication between PSCAD/EMTDC and agent-based distributed application, thus realizing the basic loop network simulation and opening the prelude of cyber physical co-simulation. Hopkinson et al. (2006) developed a collaborative simulation platform EPOCHS, which combines PSCAD/ EMTDC, PSLF and NS2 (a communication network simulation software). RTI is used as the interface between simulation software to allow periodic data exchange, so as to ensure time synchronization and routing communication. However, RTI in EPOCHS, as a synchronization intermediary, makes the process cumbersome, and the simulation process does not match the dynamic characteristics and actual interaction of CPPS. Hua et al. (2011, 2012) used PSLF and NS2, and designed interface models on both sides to realize collaborative simulation, in which the two interface models are used for acquisition, transmission, storage and interpretation of data between two simulation software, and the simulation process can also be controlled by the interface model on the PSLF side. The co-simulation method simplifies EPOCHS and improves simulation accuracy. In Celli et al. (2014), a cyber physical simulation package for distribution management system was developed, in which OpenDSS is used for power system simulation and NS2 is used for communication simulation. Both communicate with MATLAB through different interfaces, and MATLAB conducts event coordination. As NS2 can calculate the information transmission delay caused by weather and DERs location, the impact of communication delay on the distribution management system can be studied in the simulation scenario. Non-real-time co-simulation can make full use of mature simulation software to simulate two systems in detail, but physical simulator and communication simulator have different time management methods, so it is necessary to design a time synchronization method between the two simulators to realize collaborative simulation. At the beginning of the study, three main time synchronization methods were formed, i.e., alternate simulation method (Chen et al., 2013), time stepping method (Li et al., 2012; Tang et al., 2015) and global event driven method (Al-Hammouri and Ahmad, 2012; Dong et al., 2018).

In the alternate simulation method, physical simulator and communication simulator simulate alternately, and one of them dominates the simulation time. This method is simple to implement, and the simulation strictly follows the simulation process established in advance. The two simulators cannot simulate at the same time, so the simulation efficiency is low. In the time stepping method, the synchronization time is fixed to an integer multiple of the periodic sampling time of the physical simulator. The two simulators are synchronized periodically and only exchange data at a fixed synchronization time. The synchronization time is fixed and the logic is simple, but there is a high interaction delay and the simulation error is large. Based on the time stepping method, the synchronization time is

TABLE 1 | Comparison of CPPS modeling methods.

Modeling methods	References	Pros and cons	Range of application
Modeling based on incidence characteristic matrix	Xin et al., 2015; Guo Q. et al., 2016; Li M. et al., 2020	Pros: simplified description of CPPS complex interaction mechanism; high calculation efficiency. Cons: a complete CPPS model includes multiple sub-models, and the model can only reflect limited information	Analysis of data loss, channel interrupt and other simple communication fault; Safety assessment of FDI attack
Information flow-energy flow hybrid model	Guo Q. et al., 2016; Wang et al., 2019; Xu et al., 2019; Wang T. et al., 2020; Xin et al., 2017	Pros: detailed description of CPPS complex interaction mechanism; the hybrid model can be expressed by a composite function. Cons: the model is difficult to solve	Situations where the interaction between the energy flow and the information flow needs to be considered in detail; Comprehensive safety assessment of CPPS
Modeling based on theories of hybrid system	Chen et al., 2019; Zhao et al., 2011; Wang et al., 2016; Guo et al., 2019	Pros: mature modeling method; it is easy to solve; complex control models can be established. Cons: different theories are suitable for different scenes, and the model is not universal	Research on the control strategy of CPPS

determined by the event in global event driven method. When a communication event occurs, both simulators synchronize and exchange data at the next periodic sampling time. Compared with the time stepping method, this method can select the synchronization time more flexibly and the simulation efficiency is improved. The above three traditional synchronization methods are difficult to simulate the actual dynamic process of CPPS accurately and cannot meet the requirements of CPPS simulation (Li et al., 2014; Broderick et al., 2017; Gomes et al., 2017; Huang et al., 2017). Some researchers have improved the traditional time synchronization methods. In Zhou et al. (2017), the synchronization points were divided into periodic time synchronization points and event synchronization points. The two simulators can run alternately between these synchronization points, and time windows were designed near the event points that need to be synchronized in order to reduce the number of events. This method greatly improves the simulation accuracy on the basis of the traditional synchronization method. A variable step size method was mentioned in Suzuki et al. (2018). At the beginning of the simulation, the physical simulator commands the communication simulator to advance to a cycle sampling time. If there is no communication event during the period, the communication simulator advances to a cycle sampling time. If a communication event occurs during the period, the communication simulator advances to the event time and notifies the physical simulator to advance to the event time and updates the information. In this method, the physical side or the information side can respond to the received information immediately, which reduces the unnecessary delay and improves the simulation accuracy.

Since non-real-time co-simulation with a good time synchronization method can realize the collaborative analysis of physical power grid and communication network, it can be widely used in the fields of measurement, protection and control of smart grid. However, in CPPS research, more attention is paid to the real-time data communication and real-time co-simulation is required in some research scenarios such as network attacks.

Real-Time Co-simulation

Real-time co-simulation requires that the simulation software can run in real time and the model can be divided into several sub-models for parallel computation. This requires hardware-based real-time power system simulation platforms, such as RTDS and OPAL-RT. Therefore, real-time co-simulation is expensive and difficult, mainly used for the test and exercise of smart grid projects, and it is still in the initial stage. At present, some researchers have built a real-time co-simulation platform by using OPAL-RT and the commercial communication simulator OPNET, in which physical time synchronization is achieved by setting the time factor of both simulators to 1 (Armendariz et al., 2014; Bian et al., 2015). The structure of real-time co-simulation using RT-LAB and OPNET is shown in **Figure 3**. The TCP/IP data interaction interface in RT-LAB and the SITL data interaction interface in OPNET use the TCP/IP protocol to exchange the power grid status information and the control command information in the form of sockets through Ethernet. Since not all grid state information is required by OPNET simulation, the grid state information will be filtered, detected and converted in the SITL module. This real-time collaborative simulation platform truly reflects the real-time operating status of the power system and the communication network environment, and is suitable for studying the impact of cyber-attacks on the power system, the control of wide-area intelligent load, the control of microgrid or distributed generation, and the verification of HVDC security defense. However, due to the characteristics of data transmission and network hardware, this simulation platform still has an inevitable inherent delay. Shanghai KeLiang Company uses OPAL-RT's core software RT-LAB and OPNET to build a real-time co-simulation platform that includes 12 large-scale wind farms, a MMC-HVDC, a secondary system, a set of wind farm monitoring systems and a SCADA monitoring system for attack and defense of power system, which provides a very realistic training scenario for network security of power system. The simulation platform can not only simulate various accidental power failures in the links of power generation,

transmission, transformation and distribution, but also simulate various network attacks at the same time, such as distributed denial of service (DDOS) attacks, FDI attacks, and network virus infections. In addition, it can also realize the intrusion monitoring, detection, alarm and defense. Due to a large number of mature power system and communication system simulation software, cyber physical co-simulation has a variety of selectivity (Jung et al., 2018; Sun et al., 2019; Thule et al., 2019; Jahromi et al., 2020; Li B. et al., 2020), and there is no direct research to show which combined scheme has better simulation effect, so co-simulation platform is worthy of further study.

Semi-Physical Simulation

Semi-physical simulation means that the primary system in CPPS is simulated by power system simulation software and the secondary equipment in CPPS is replaced by a real object according to the different research objects, or vice versa. Semi-physical simulation introduces the real object into the simulation,

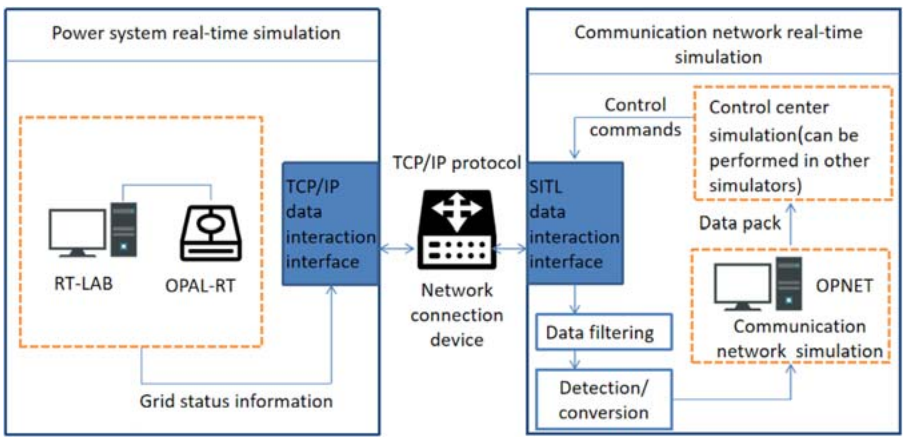

FIGURE 3 | Structure of real-time co-simulation using RT-LAB and OPNET.

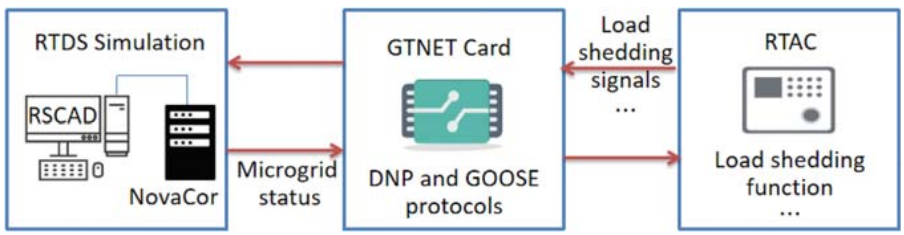

FIGURE 4 | Microgrid semi-physical simulation scheme.

TABLE 2 | Comparison of CPPS simulation methods.

Simulation methods	References	Pros and cons	Range of application
Cyber physical co-simulation	Hopkinson et al., 2006; Hua et al., 2011; Hua et al., 2012; Celli et al., 2014; Zhou et al., 2017; Suzuki et al., 2018	Pros: power grid and communication network can be simulated in detail; a variety of simulation software is available; good simulation effect, especially real-time co-simulation. Cons: complex data interaction process; data conversion is required between different simulators	Measurement, protection and control of smart grid; network attacks
Semi-physical simulation	Weng et al., 2018; Fu et al., 2019	Pros: simple data interaction process; reliable simulation results. Cons: high cost; limited simulation capabilities; the communication protocol depends on the built-in modules of the simulation hardware	Test and verification of engineering projects
Embedded simulation	Moradi-Pari et al., 2014; Rasmussen et al., 2018	Pros: there is no time synchronization problem. Cons: rough simulation; the other side is difficult to model	Suitable for scenarios that do not require high simulation accuracy on one side

which increases the authenticity of the simulation, realizes the direct interaction between the cyber part and physical part in CPPS, and improves the simulation accuracy. In Weng et al. (2018), the primary system of the active distribution network was built in DIGSILENT to realize the digital simulation. Then the simulation results were sent to the actual secondary equipment through the real-time interface, and the action status of the actual secondary equipment was transmitted back to the simulation software, thus forming a closed-loop cyber physical simulation. The action of the actual physical device after the fault can reflect the real control effect of the control strategy and verify the effectiveness of the control strategy, so as to realize the fault analysis of the active distribution network. The semi-physical simulation method of active distribution network was also utilized in Moradi-Pari et al. (2014). The physical power grid was built by RT-LAB, the communication system was simulated by OPNET, and the data monitoring controller and system control units were real physical devices. The control device can obtain the simulation system data and make control decisions, and then transmits them to the power system simulation platform through wireless transmission to realize the control of distributed generation. The difference from Weng et al. (2018) is that communication system simulation software is added in Fu et al. (2019), which can study the influence of communication network faults such as communication congestion and data loss on power system. In order to simulate and test the load shedding function of the microgrid, RTDS Company proposed a microgrid semi-physical simulation scheme using real-time automation controllers (RTAC), as shown in **Figure 4**. The microgrid model was built in RSCAD software and the physical side of the microgrid was simulated with the support of NovaCor hardware. RTAC and NovaCor exchange data through GTNET card with the DNP and GOOSE protocols. The active power, reactive power, frequency, power setting value, switch and load status of the microgrid simulation model are sent to RTAC through the GTNET card. RTAC generates a load shedding signal according to its load shedding function, and then sends it to the microgrid simulation model through the GTNET card. This simulation scheme can be extended to simulate various control functions of the microgrid in grid-connected and island operation, but the realization of its control functions is limited by the performance of the physical controller. Although the semi-physical simulation has high simulation accuracy, it needs the participation of real physical devices, which is expensive. It is suitable for the test and research of engineering projects, so, its application range is narrow.

Embedded Simulation

Because cyber physical co-simulation needs to use a variety of simulation software and consider the time synchronization between different software, the process is cumbersome, and the cost of semi-physical simulation is high, so some researches designed communication modules in the power system simulation software to simulate communication strategies. This method is called the embedded simulation. In Moradi-Pari et al. (2014), a communication module is embedded in PSCAD and the discrete event simulation of the communication module is synchronized by using the existing time steps in PSCAD, thereby realizing the simulation of discrete events in PSCAD. Rasmussen et al. (2018) designed a perception control module in PSCAD, in which the sending and receiving of information are realized through a communication module to complete the perception, control and communication of power system, thus realizing the joint simulation of communication strategy and power system. The difficulty of embedded simulation lies in the design of communication module in power system simulation software. On the one hand, power system simulation is based on continuous events, while communication process is based on discrete events; on the other hand, it is difficult to simulate accurate communication process in power system simulation software, only rough simulation can be carried out, which limits the application field of embedded simulation. In **Table 2**, the three simulation methods are compared.

CONCLUSION

Due to the different characteristics of information systems and physical systems, the modeling and simulation methods of CPPS are significantly different from those of traditional power systems, which brings difficulties to the further quantitative analysis of CPPS. This paper reviews the quantitative analysis methods of CPPS from two aspects of modeling and simulation. Three kinds of CPPS modeling methods are summarized: modeling based on incidence characteristic matrix, a hybrid model of information flow and energy flow, and modeling based on theories of hybrid model in the control field. The CPPS simulation methods are divided into three categories: cyber physical co-simulation, semi-physical simulation and embedded simulation, in which the most commonly used is the cyber physical co-simulation. These CPPS modeling and simulation methods can be widely applied to situational awareness, risk assessment, reliability analysis and other aspects of smart grids. However, at present, there is no general CPPS modeling method and mature CPPS simulation method, and most of these methods focus on the normal operating state of a kind of energy without paying attention to the multiple operating states of multiple energy.

FUTURE WORK

According to the existing problems in the CPPS research, the following research directions of CPPS can be explored in future work.

(1) In the CPPS modeling methods, the communication network has been greatly simplified, which causes these methods unable to fully reflect the characteristics of the communication network. Therefore, a more detailed model of the communication network should be established in future research, considering the influence of different communication manners and information processing processes. Besides, how to simplify the communication network properly remains to be studied.

Although some researchers have established the hybrid model of information flow and energy flow, the hybrid calculation method of solving the fusion model is still a big challenge. The corresponding algorithm should consider how to unify the discrete and continuous quantities in the processes of data interaction.

(2) In the CPPS simulation methods, the simulation effect of different non-real-time co-simulation schemes is different, which mainly depends on the time synchronization method. Therefore, it is worthwhile to further study the synchronization strategies between different simulators to improve the simulation accuracy. At present, physical power grid simulation and communication network simulation are in a state of separation, and more attention has been paid to how to establish the relationship between the two simulations, so, it is necessary to develop an integrated real-time simulation platform to improve the simulation efficiency and meet the requirements of real-time simulation. From the perspective of simulation, how to apply the fusion model to simulation is also a problem that needs to be solved urgently.

(3) In the analysis of the traditional power system, researchers usually only focus on the optimal operation of the power system, but the optimal operation of the power communication network in CPPS should also be concerned. Due to the different importance of the information flow, the data transmission path of power communication network should be optimized according to the importance of the information flow, that is, route optimization, to ensure the efficient and safe transmission of the important information. Besides, as a large-scale cyber physical system, smart grid also includes lots of distributed generations. In the future CPPS research, distributed energy such as photovoltaic and wind power should also be considered, and cyber physical system with various energy forms should be discussed.

(4) Digital twin technology is the key to achieve equivalent mapping of physical entities in virtual space. Proposing an accurate equivalent method for physical entities will become an opportunity for the rapid development of CPPS modeling and simulation methods, which will promote power system operation status prediction and CPPS Network risk prediction.

(5) The further development of CPPS needs to process and analyze the massive data in CPPS. The data-driven CPPS model can make full use of massive data and provide data feedback to improve the robustness of state perception, risk prediction, reliability assessment and CPSS models. This is also one of the most challenging directions in future work.

AUTHOR CONTRIBUTIONS

HF: conceptualization, methodology, and investigation. HW: validation, and writing – original draft preparation. SX: methodology, investigation, and software. XL: validation, and writing – review. PX: editing, methodology, and software. YG: validation and project administration. All authors contributed to the article and approved the submitted version.

FUNDING

This work was supported partially by the National Natural Science Foundation of China (52077075), the Jiangsu Basic Research Project (BK20180284), and the Fundamental Research Funds for the Central Universities (2019MS007).

ACKNOWLEDGMENTS

The authors would like to thank the editor and reviewers for their valuable comments.

REFERENCES

Al-Hammouri, A., and Ahmad, T. (2012). A comprehensive co-simulation platform for cyber-physical systems. *Comput. Commun.* 36, 8–19. doi: 10.1016/j.comcom.2012.01.003

Armendariz, M., Chenine, M., Nordström, L., and Al-Hammouri, A. (2014). "A co-simulation platform for medium/low voltage monitoring and control applications," in *Proceedings of the 2014 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, (Washington, DC: ISGT). doi: 10.1109/ISGT.2014.6816369

Attarzadeh-Niaki, S. H., and Sander, I. (2020). Heterogeneous co-simulation for embedded and cyber-physical systems design. *Simul-T Soc. Mod Sim.* 96, 753–765. doi: 10.1177/0037549720921945

Bian, D., Kuzlu, M., Pipattanasomporn, M., Rahman, S., and Wu, Y. (2015). "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in *Proceedings of the IEEE Power & Energy Society General Meeting*, (Denve, CO: IEEE). doi: 10.1109/PESGM.2015.7286238

Broderick, S., Cruden, A., Sharkh, S., and Bessant, N. (2017). Technique to interconnect and control co-simulation systems. *IET Gener. Trans. Distrib.* 11, 3115–3124. doi: 10.1049/iet-gtd.2016.1569

Calvo, J. L., Tindemans, S. H., and Strbac, G. (2018). Risk-based method to secure power systems against cyber-physical faults with cascading impacts: a system protection scheme application. *J. Modern Power Syst. Clean Energy* 6, 930–943. doi: 10.1007/s40565-018-0447-8

Celli, G., Pegoraro, P. A., Pilo, F., Pisano, G., and Sulis, S. (2014). DMS Cyber-Physical simulation for assessing the impact of state estimation and communication media in smart grid operation. *IEEE Trans. Power Syst.* 29, 2436–2446. doi: 10.1109/TPWRS.2014.2301639

Chen, G., Liu, D., and Weng, J. (2019). Cyber physical modeling of power frequency control system and its application in fault-tolerant control. *Power Syst. Technol.* 43, 2376–2383. doi: 10.13335/j.1000-3673.pst.2018.1481

Chen, Y., Song, Y., and Fei, M. (2013). Design and development of cosimulation platform for NCS based on simulink and OPNET. *J. Syst. Simul.* 25, 1518–1523. doi: 10.16182/j.cnki.joss.2013.07.041

Dong, W., Liu, K., and Hu, L. (2018). "CPS event driving method based on micro PMU of distribution network," in *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, (Zhengzhou: IEEE). doi: 10.1109/CyberC.2018.00076

Farraj, A., Hammad, E., and Kundur, D. (2018). A cyber-physical control framework for transient stability in smart grids. *IEEE Trans. Smart Grid* 9, 1205–1215. doi: 10.1109/TSG.2016.2581588

Fu, C., Wang, L., Qi, D., and Zhang, J. (2019). Design and experiments of active distribution network CPS simulation platform. *Proc. CSEE* 39, 7118–7125+7485. doi: 10.13334/j.0258-8013.pcsee

Gomes, C., Thule, C., Broman, D., Larsen, P. G., and Vangheluwe, H. (2017). *Co-Simulation: State of the Art*. New York, NY: Cornell University.

Guo, J., Han, Y, Guo, C., Li, D., and Sun, J. (2016). Reliability assessment of cyber physical power system considering monitoring function and control function. *Proc. CSEE* 36, 2123–2130. doi: 10.13334/j.0258-8013.pcsee.2016.08.011

Guo, J., Liu, W., Zhang, J., and Ma, T. (2019). A survey of reliability modeling and evaluation methods for active distribution cyber-physics systems. *Power Syst. Technol.* 43, 2403–2412. doi: 10.13335/j.1000-3673.pst.2019.0073

Guo, Q., Xin, S., Sun, H., and Wang, J. (2016). Power system cyber-physical modelling and security assessment: motivation and ideas. *Proc. CSEE* 36, 1481–1489. doi: 10.13334/j.0258-8013.pcsee.2016.06.003

Hopkinson, K., Wang, X., Giovanini, R., Thorp, J., Birman, K., and Coury, D. (2006). EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Trans. Power Syst.* 21, 548–558. doi: 10.1109/TPWRS.2006.873129

Hua, L., Sambamoorthy, S., Shukla, S., Thorp, J., and Mili, L. (2011). "Power system and communication network co-simulation for smart grid applications," in *Proceedings of the Innovative Smart Grid Technologies (ISGT)*, (Anaheim, CA: IEEE PESISGT). doi: 10.1109/ISGT.2011.5759166

Hua, L., Santhosh, S. V., Sandeep, S. S., Lamine, M., and James, T. (2012). GECO: global event-driven co-simulation framework for interconnected power system and communication network. *IEEE Trans. Smart Grid* 3, 1444–1456. doi: 10.1109/TSG.2012.2191805

Huang, R., Fan, R., Daily, J., Fisher, A., and Fuller, J. (2017). Open-source framework for power system transmission and distribution dynamics co-simulation. *IET Gener. Trans. Distrib.* 11, 3152–3162. doi: 10.1049/iet-gtd.2016.1556

Jahromi, A. A., Kemmeugne, A., Kundur, D., and Haddadi, A. (2020). Cyber-physical attacks targeting communication-assisted protection schemes. *IEEE Trans. Power Syst.* 35, 440–450. doi: 10.1109/TPWRS.2019.2924441

Jung, T., Shah, P., and Weyrich, M. (2018). Dynamic co-simulation of internet-of-things-components using a multi-agent-system. *Proc. CIRP* 72, 874–879. doi: 10.1016/j.procir.2018.03.084

Kang, J., Joo, I., and Choi, D. (2018). False data injection attacks on contingency analysis: attack strategies and impact assessment. *IEEE Access* 6, 8841–8851. doi: 10.1109/ACCESS.2018.2801861

Lai, L. L., Shum, C., Wang, L., Lau, W. H., Tse, N., Chung, H., et al. (2014). "Design a co-simulation platform for power system and communication network," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, (San Diego, CA; IEEE). doi: 10.1109/SMC.2014.6974392

Li, B., Zhao, H., Diao, J., and Han, Z. (2020). Design of real-time co-simulation platform for wind energy conversion system. *Energy Rep.* 6, 403–409. doi: 10.1016/j.egyr.2019.11.094

Li, J., Liu, Y., Xie, J., Li, M., Sun, M., Liu, Z., et al. (2019). A remote monitoring and diagnosis method based on four-layer iot frame perception. *IEEE Access* 7, 144324–144338. doi: 10.1109/ACCESS.2019.2945076

Li, M., Xue, Y., Ni, M., and Li, X. (2020). Modeling and hybrid calculation architecture for cyber physical power systems. *IEEE Access* 8, 138251–138263. doi: 10.1109/ACCESS.2020.3011213

Li, W., Zhang, X., and Dong, Y. (2012). Study of co-simulation methods applied in power systems (Part I): VPNET. *Proc. CSEE* 32, 95–102+196. doi: 10.13334/j.0258-8013.pcsee.2012.13.015

Li, W., Zhang, X., and Li, H. (2014). Co-simulation platforms for co-design of networked control systems: an overview. *Control Eng. Pract.* 23, 44–56. doi: 10.1016/j.conengprac.2013.10.010

Liu, D., Sheng, W., Wang, Y., Lu, Y., and Sun, C. (2015). Key technologies and trends of cyber physical system for power grid. *Proc. CSEE* 35, 3522–3531. doi: 10.13334/j.0258-8013.pcsee.2015.14.006

Liu, Y., and Liu, X. (2016). *Telecontrol of Power System*. Beijing: China Electric Power Press.

Lu, X., Xia, S., Sun, G., Hu, J., Zou, W., Zhou, Q., et al. (2021). Hierarchical distributed control approach for multiple on-site DERs coordinated operation in microgrid. *Int. J. Electr. Power Energy Syst.* 129:106864. doi: 10.1016/j.ijepes.2021.106864

Moradi-Pari, E., Nasiriani, N., Fallah, Y. P., Famouri, P., Bossart, S., and Dodrill, K. (2014). Design, modeling, and simulation of on-demand communication mechanisms for cyber-physical energy systems. *IEEE Trans. Industr. Inform.* 10, 2330–2339. doi: 10.1109/TII.2014.2326080

Pall, G. K., Bridge, A. J., Skitmore, M., and Gray, J. (2016). Comprehensive review of delays in power transmission projects. *IET Gener. Trans. Distrib.* 10, 3393–3404. doi: 10.1049/iet-gtd.2016.0376

Qu, Z., Dong, Y., Qu, N., Li, H., Cui, M., Bo, X., et al. (2021). False data injection attack detection in power systems based on cyber-physical attack genes. *Front. Energy Res.* 9:57. doi: 10.3389/fenrg.2021.644489

Qu, Z., Xie, Q., Liu, Y., Li, Y., Wang, L., Xu, P., et al. (2020). Power cyber-physical system risk area prediction using dependent markov chain and improved grey wolf optimization. *IEEE Access* 8, 82844–82854. doi: 10.1109/ACCESS.2020.2991075

Qu, Z., Zhang, Y., Qu, N., Wang, L., Li, Y., and Dong, Y. (2018). Method for quantitative estimation of the risk propagation threshold in electric power CPS based on seepage probability. *IEEE Access* 6, 68813–68823. doi: 10.1109/ACCESS.2018.2879488

Rana, M. M., and Bo, R. (2020).). IoT-based cyber-physical communication architecture: challenges and research directions. *IET Cyber Phys. Syst. Theory Appl.* 5, 25–30. doi: 10.1049/iet-cps.2019.0028

Rasmussen, T. B., Yang, G., Nielsen, A. H., and Dong, Z. (2018). Effects of centralized and local PV plant control for voltage regulation in LV feeder based on cyber-physical simulations. *J. Modern Power Syst. Clean Energy* 6, 979–991. doi: 10.1007/s40565-018-0445-x

Srivastava, A. K., Ernster, T. A., Liu, R., and Krishnan, V. G. (2018). Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information. *J. Modern Power Syst. Clean Energy* 6, 887–899. doi: 10.1007/s40565-018-0448-7

Su, Z., Xu, L., Xin, S., Li, W., Shi, Z., and Guo, Q. (2017). "A future outlook for cyber-physical power system," in *Proceedings of the IEEE Conference on Energy Internet and Energy System Integration (EI2)*, (Beijing: IEEE). doi: 10.1109/EI2.2017.8245733

Sun, C., Cheng, S., Yuan, K., Sun, J., Song, Y., Wu, Z., et al. (2019). Real time simulation platform of power cyber-physical system based on node mapping model. *Power Syst. Technol.* 43, 2368–2377. doi: 10.13335/j.1000-3673.pst.2018.1143

Suzuki, A., Masutomi, K., Ono, I., Ishii, H., and Onoda, T. (2018). CPS-Sim: co-simulation for cyber-physical systems with accurate time synchronization. *IFAC Papers OnLine* 51, 70–75. doi: 10.1016/j.ifacol.2018.12.013

Tang, A., and Wang, X. (2015). A-duplex: medium access control for efficient coexistence between full-duplex and half-duplex communications. *IEEE Trans. Wirel. Commun.* 14, 5871–5885. doi: 10.1109/TWC.2015.2443792

Tang, Y., Wang, Q., Ni, M., and Xue, Y. (2015). Review on the hybrid simulation methods for power and communication system. *Autom. Electr. Power Syst.* 39, 33–42. doi: 10.7500/AEPS20150331035

Tang, Y., Wang, Q., Tai, W., and Ning, M. (2016). Real-time simulation of cyber-physical power system based on OPAL-RT and OPNET. *Autom. Electr. Power Syst.* 40, 15–21. doi: 10.7500/AEPS20160515020

Tao, J., Umair, M., Ali, M., and Zhou, J. (2020). The impact of internet of things supported by emerging 5G in power systems: a review. *CSEE J. Power Energy Syst.* 6, 344–352. doi: 10.17775/CSEEJPES.2019.01850

Thule, C., Lausdahl, K., Gomes, C., Meisl, G., and Larsen, P. G. (2019). Maestro: the INTO-CPS co-simulation framework. *Simul. Model. Pract. Theory* 92, 45–61. doi: 10.1016/j.simpat.2018.12.005

Wang, C., Dong, X., Sun, H., Wang, C., Wang, Y., and Wang, Y. (2020). Modeling method of power cyber-physical system considering multi-layer coupling characteristics. *Autom. Electr. Power Syst.* 45, 83–91. doi: 10.7500/AEPS20200109004

Wang, T., Long, Q., Gu, X., and Chai, W. (2020). Information flow modeling and performance evaluation of communication networks serving power grids. *IEEE Access* 8, 13735–13747. doi: 10.1109/ACCESS.2020.2966489

Wang, Y., Liu, D., and Lu, Y. (2016). Research on hybrid system modeling method of cyber physical system for power grid. *Proc. CSEE* 36, 1464–1470. doi: 10.13334/j.0258-8013.pcsee.2016.06.001

Wang, Z., Chen, Y., Zeng, J., Chen, J., and Liu, J. (2019). Modeling and reliability assessment of completely distributed microgrid cyber physical system. *Power Syst. Technol.* 43, 2413–2421. doi: 10.13335/j.1000-3673.pst.2018.2910

Weng, J., Liu, D., Wang, Y., Zhang, M., and Ji, W. (2018). Research on fault simulation of active distribution network based on cyber physical combination. *Proc. CSEE* 38, 497–504+680. doi: 10.13334/j.0258-8013.pcsee.162537

Xi, R., Yun, X., and Hao, Z. (2019). Framework for risk assessment in cyber situational awareness. *IET Inform. Secur.* 13, 149–156. doi: 10.1049/iet-ifs.2018.5189

Xia, S., Bu, S., Hu, J., Hong, B., Guo, Z., and Zhang, D. (2019a). Efficient transient stability analysis of electrical power system based on a spatially paralleled hybrid approach. *IEEE Trans. Industr. Inform.* 3, 1460–1473. doi: 10.1109/TII.2018.2844298

Xia, S., Bu, S., Luo, X., Chan, K., and Lu, X. (2018). An autonomous real time charging strategy for plug-in electric vehicles to regulate frequency of distribution system with fluctuating wind generation. *IEEE Trans. Sustain. Energy* 2, 511–524.

Xia, S., Bu, S., Wan, C., Lu, X., Chan, K., and Zhou, B. (2019b). A fully distributed hierarchical control framework for coordinated operation of DERs in active distribution power networks. *IEEE Trans. Power Syst.* 6, 5184–5197. doi: 10.1109/TPWRS.2018.2870153

Xia, S., Zhang, Q., Jing, J., Ding, Z., Yu, J., Chen, B., et al. (2019c). Distributed state estimation of multi-region power system based on consensus theory. *Energies* 5:900. doi: 10.3390/en12050900

Xiao, J., Zhang, B., and Luo, F. (2019). Distribution network security situation awareness method based on security distance. *IEEE Access* 7, 37855–37864. doi: 10.1109/ACCESS.2019.2906779

Xin, S., Guo, Q., Sun, H., Chen, C., Wang, J., and Zhang, B. (2017). Information-energy flow computation and cyber-physical sensitivity analysis for power systems. *IEEE J. Emerg. Sel. Top. Circuits Syst.* 7, 329–341. doi: 10.1109/JETCAS.2017.2700618

Xin, S., Guo, Q., Sun, H., Zhang, B., Wang, J., and Chen, C. (2015). Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. *IEEE Trans. Smart Grid* 6, 2375–2385. doi: 10.1109/TSG.2014.2387381

Xu, L., Guo, Q., Yang, T., and Sun, H. (2019). Robust routing optimization for smart grids considering cyber-physical interdependence. *IEEE Trans. Smart Grid* 10, 5620–5629. doi: 10.1109/TSG.2018.2888629

Yu, X., and Xue, Y. (2016). Smart grids: a cyber-physical systems perspective. *Proc. IEEE* 104, 1058–1070. doi: 10.1109/JPROC.2015.2503119

Zerihun, T. A., Garau, M., and Helvik, B. E. (2020). Effect of communication failures on state estimation of 5G-enabled smart grid. *IEEE Access* 8, 112642–112658. doi: 10.1109/ACCESS.2020.3002981

Zhao, J., Wen, F., Xue, Y., and Dong, C. (2011). Modeling analysis and control research framework of cyber physical power systems. *Autom. Electr. Power Syst.* 35, 1–8.

Zhou, L., Wu, Z., Sun, J., Su, C., Gu, W., and Shi, Y. (2017). Realization of master-slave mode co-simulation in cyber physical system based on hybrid time synchronization strategy. *Autom. Electr. Power Syst.* 41, 9–15. doi: 10.7500/AEPS20160923005

Conflict of Interest: XL was employed by the company State Grid Economic and Technological Research Institute Co., Ltd., Beijing, China. PX was employed by Shanghai Sermatec Energy Technology Co., Ltd., Shanghai, China.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.