Received July 7, 2020, accepted July 17, 2020, date of publication July 22, 2020, date of current version August 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3011213

Modeling and Hybrid Calculation Architecture for Cyber Physical Power Systems

MANLI LI, YUSHENG XUE, (Life Member, IEEE), MING NI, (Senior Member, IEEE), AND XIAO LI

NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China
NARI Technology Company Ltd., Nanjing 211106, China
State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China

Corresponding author: Ming Ni (ni-ming@sgepri.sgcc.com.cn)

This work was supported in part by the National Key Research and Development Program of China (Basic Research Class) under Grant 2017YFB0903000, and in part by the Science and Technology Project of the State Grid Corporation of China (Basic Theory and Methodology for Analysis and Control of Grid Cyber Physical Systems).

ABSTRACT Traditional isolated modeling and calculation methods for cyber systems and power systems cannot satisfy the requirements for the analysis and control of cyber physical power systems (CPPSs). In this paper, a matrix-based modeling method for the coupled behavior of a CPPS is presented to describe the complex interactions of the information and energy flows. A hybrid calculation architecture is proposed for the reliability and security analysis of CPPSs. On that basis, the CPPS security defense system is established. Case studies verify the effectiveness of this CPPS modeling approach and hybrid calculation architecture.

INDEX TERMS Cyber physical power system (CPPS), cyber physical system (CPS), modeling, calculation, architecture.

I. INTRODUCTION

The widespread application of information communication technology (ICT) has transformed traditional power systems into cyber physical power systems (CPPSs). As the coupling between the cyber and physical sides becomes stronger, cyberattacks can have increasingly significant impacts on the safe operation of physical power systems, as illustrated by the effects of the Stuxnet virus in 2010 and the Ukrainian blackout in 2015 [1]. In a CPPS, the mechanisms of CPPS faults and their propagation between the cyber and physical systems are also fundamentally different from those in a traditional power system [2]. Malicious attacks based on the coordinated relationship among information applications have become an important driver of fault propagation and evolution because of the closer coupling between the cyber and physical sides.

In recent years, a great deal of research has been conducted on the critical issues related to CPPSs, especially the impact of cyberattacks on CPPSs; the related topics include the network infrastructure and the power system control applications that may be attacked in CPPSs [3], the patterns of malicious attacks and methods of attack identification [4]–[6], malicious attack modeling [7], fault set analysis [8], and security assessment [9], [10]. However, due to the lack of a complete and unified modeling and analysis theory, most existing studies are based on simplified and isolated power or cyber models, which lack adaptability and flexibility. Therefore, it is of great significance to research a general methodology of CPPS modeling, calculation, analysis and control from the perspective of the entire cyber physical system. To do so, the following four key issues must be resolved: 1) The cyber physical coupling mechanisms. The coupling mechanism is the mutual relationship between cyber and physical sides, such as how cyber and physical sides affect each other, which cyber nodes and physical nodes will affect one another, and what are the key factors that affect one another. The cyber physical coupling mechanisms are the basis of modeling and analysis. The mechanisms must be described in a general form. 2) The mismatch between the traditional cyber model and the power system model. The influence of the cyber side on the power system is mainly manifested in communication delay, bit error, interruption and data correction, etc. Power system analysis needs a cyber model for these characteristics, but the traditional cyber model focuses on describing the mechanisms of data transmission and processing. Therefore,

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

there is mismatch between the cyber model and the power system model. 3) Hybrid calculation based on the CPPS model. The cyber and physical sides each have their own algorithms, such as the power flow calculation on the physical side and the latency calculation on the cyber side. The question of how to coordinate these different algorithms, in combination with the coupling mechanisms between the two sides, to realize hybrid calculations for a CPPS is a critical issue to be resolved. 4) Model simplification and equivalence. To achieve effective calculations and analyses of CPPSs in different scenarios, it is necessary to simplify complex CPPS models to obtain equivalent models that retain only the key features required for studying the topic of interest.

For CPPS modeling, the studies reported in [11]–[14] consider cyber factors in the modeling of physical components or agents. By incorporating the input/output signals of both the physical and cyber systems, the relevant information functionalities are embodied in the internal dynamic characteristics, local sensing and execution behavior of each cyber physical module. This kind of research is relatively preliminary and addresses the key issue of the mismatch between the cyber and physical models. For CPPS security assessment, papers [15], [16] establish a static model of a CPPS by abstracting the CPPS as a directional topological graph, abstracting the state variables in the physical and cyber systems as "data nodes" and abstracting information processing and information transmission as "informational branches." On that basis, methods of hybrid calculation and sensitivity analysis are proposed, and the automatic voltage control (AVC) task is considered to validate the model. This research explores the four key issues mentioned above. However, the cyber system model considered in this approach is a logical model of information flow, which lacks the details of specific cyber devices, especially communication devices. Therefore, this kind of model can only reflect the coupling mechanism from the logical level. Both the cyber model and the coupling mechanisms between the cyber and physical sides are simplified, and consequently, the model cannot meet the requirements for CPPS investigations in many cases. With the goal of load optimization control, papers [17]–[21] propose an event-driven dynamic CPPS model based on hybrid system theory. This model is oriented toward optimal control and provides solutions for the issues of model mismatch and hybrid calculation.

At present, most CPPS models reveal the coupling mechanism from the logical level and cannot reflect the interaction between the cyber and physical sides from the device level. Therefore, the data required by the model are not easy to obtain directly, so it is difficult to directly apply to actual systems at the current stage. In addition, current studies on CPPS modeling and calculation are mainly undertaken from the perspective of a specific task rather than from the perspective of general CPPSs. Therefore, their fields of application are limited.

Papers [22]–[24], written by the authors of the current work, note that communication delay, interruption and so on have an impact on the control effect of power grid security and stability control systems and put forward the method of modeling the communication network with the matrix. On this basis, this paper focuses on how to describe the topological and business coupling relationship between cyber and physical sides using the method of the correlation characteristic matrix, realizes hybrid calculation and model simplification, and takes the security control business as an example to illustrate the practical application process of the CPPS model. The CPPS modeling method proposed in this paper reveals the coupling mechanism from the device level. The data required by the model can be obtained directly from the existing system and the model has better practicability.

In this paper, section II focuses on the cyber physical coupling mechanisms and proposes a general CPPS framework, including a decision-making layer, a cyber physical coupling layer and a physical layer, which reflects the tight coupling of the cyber and physical systems through the closed-loop processes of data collection, data processing, decision-making, and execution. In section III, the characteristics of the cyber system that directly impact the physical power system, such as communication delay, bit error, interruption, and failure probability, are described in multivariate group form to solve the problem of model mismatch. Topological and interlayer coupling relationship models are established by using the matrix method to describe the cyber physical coupling mechanisms. On this basis, a general framework for CPPS hybrid calculation is proposed in section IV. Based on the CPPS model and hybrid calculation architecture, the CPPS security defense system is established in section V. Case studies are presented in section VI to demonstrate the effectiveness of the proposed CPPS model and the hybrid calculation method. Section VII offers conclusions.

II. HIERARCHICAL STRUCTURE OF A CPPS

In a CPPS, the interactions between the cyber system and the physical power system are complex. For such an enormous system, containing massive numbers of physical, information and communication components and complex communication protocols, the foundation of CPPS modeling is to sort out the logical association relations and interactive influences to reveal the cyber physical coupling mechanisms.

At present, three different classes of cyber physical coupling mechanisms are understood to exist: coupling mechanisms based on cyber physical topological dependence [25]; coupling mechanisms based on communication, calculation, and control (3C) strategies for cyber and physical energy supply [26]; and coupling mechanisms based on closed-loop cyber physical control processes [15]. Since the operating characteristics of the CPPS itself cannot be considered, the first two types of coupling mechanisms are mostly applied to analyze the vulnerability of network topologies. Research on CPPS analysis and control normally considers coupling mechanisms based on closed-loop cyber physical control processes.

Consider the example of a power grid security and stability control system (SSCS). A slave station (a secondary device) collects real-time data on the physical power system and performs preliminary calculations (e.g., calculating the power, frequency, and voltage angle and judging fault types). The slave station then transmits the real-time analysis results through 2M cables and synchronous digital hierarchy (SDH) equipment (the communication network) to the main station (also a secondary device, the decision-making unit), which makes decisions and issues control commands in accordance with the information received. The control commands are transmitted through the communication network back to the slave station, which is responsible for actuation. The realization of such control is a typical CPPS function. In this process, the cyber physical coupling mechanism is as follows: energy flows in physical entities are transformed into information flows through data collection devices, and then, through processing by secondary devices and transmission by the communication network, these information flows becomes the input signals to decision-making units. The control commands generated by the decision-making units are sent to actuators, which operate the primary physical equipment to control the energy flows.

The cyber physical coupling mechanism is a closed-loop process involving data acquisition, data processing and transmission, decision-making and control command execution. To facilitate the description of this closed-loop process, the CPPS can be abstracted as a physical layer, a cyber physical coupling layer and a decision-making layer, which correspond to the physical network (primary equipment), the communication/secondary device network and the decision-making functions, as shown in Figure 1.

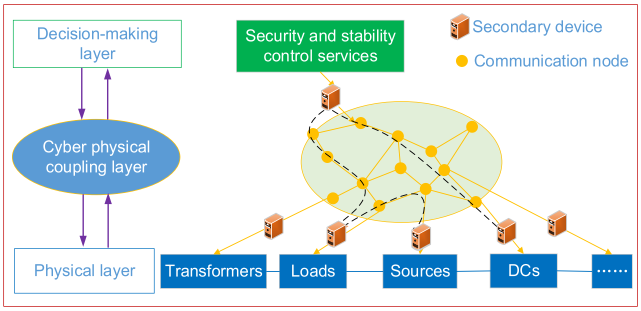


FIGURE 1. Architecture of a CPPS.

The physical layer and the cyber physical coupling layer closely interact through the data acquisition and control command execution processes. The decision-making layer is a virtual network that is abstracted from the decision-making units for different applications. Each decision-making unit takes information from the secondary device network as an input and produces control commands accordingly. Thus, the decision-making layer and the cyber physical coupling layer are tightly coupled.

III. CPPS MODELING

Based on the CPPS architecture presented above, this section introduces the CPPS modeling method. The main tasks in CPPS modeling are to model the cyber physical coupling layer and the relationship among the three layers. CPPS modeling mainly includes the modeling of the topology relationship (as shown in the matrix in Figure 2 (a)) and business relationship (as shown by "⊗" in Figure 2 (a)). This section mainly introduces the modeling of the topology relationship. Topology relationship modeling mainly includes the topology and node modeling of communication and secondary equipment networks. In terms of topology modeling, a correlation matrix is used to model the topology of the communication, secondary equipment network and topological connection among three layers. In terms of node modeling, the multivariate groups are used to describe the external characteristics of the secondary devices and communication components that affect power system operation, such as latency, interruption probability, and data error, to solve the problem of mismatch between the cyber model and power model.

Figure 2 briefly introduces the CPPS modeling method based on correlation characteristic matrices. For the detailed modeling method, please refer to paper [24].

As shown in Figure 2(a), the first step is to construct the communication network matrix $\boldsymbol{C}$, in which multivariate groups are used to model the node and branch characteristics (such as delay and interruption), and matrices are used to model the network topology.

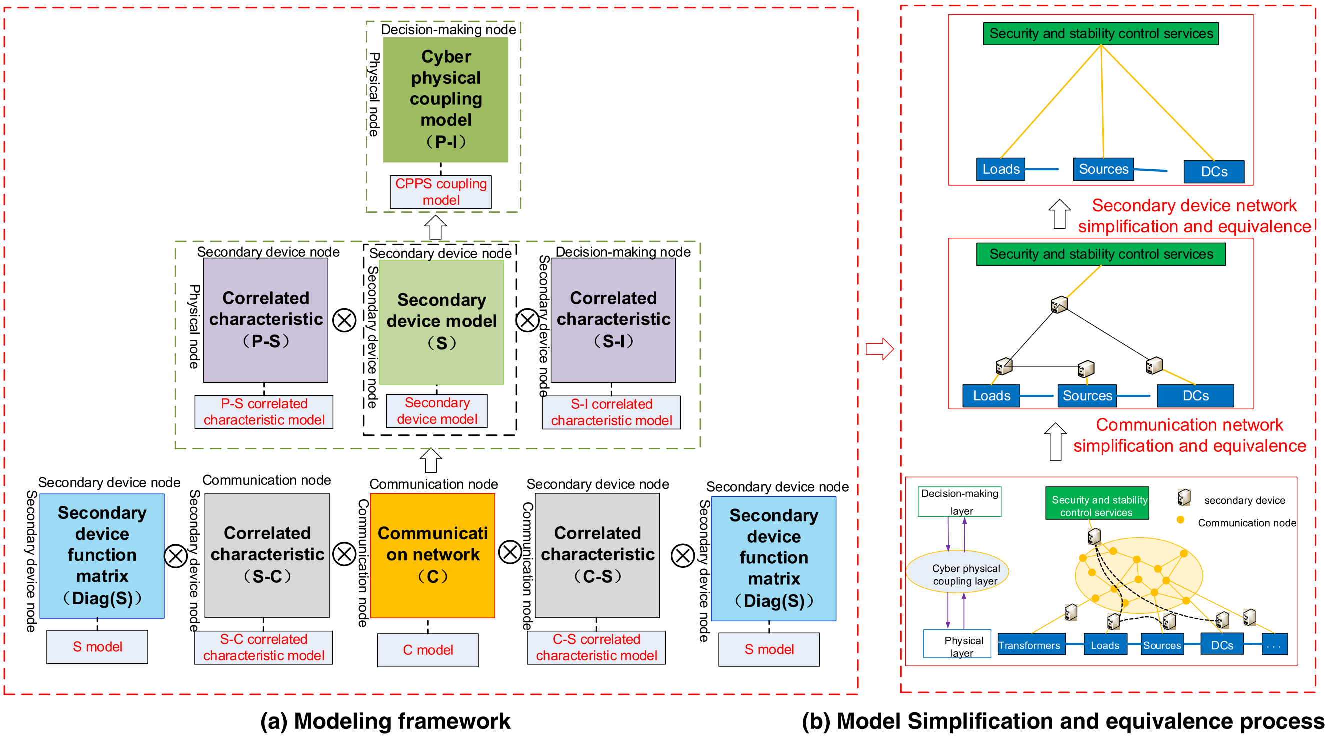
For a communication network with m nodes, $\boldsymbol{C}$ is an $m \times m$ matrix, as shown in (1):

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

$$\mathbf{C}_{ij} = \left(T_{ij}, P_{Bij}, P_{Mij}\right), \begin{cases} i=j, & \text{communication nodes} \\ i \neq j, & \text{communication branches} \end{cases} \tag{1}$$

where C_{ij} represents the communication performance on a branch that directly connects nodes i and j; if there is no direct connection, a value of "0" or "∞"will be assigned to C_{ij}. T_{ij}, P_{Bij} and P_{Mij} represent the communication latency, interruption probability and bit error probability, respectively, between nodes i and j, and this multivariate group can be modified or expanded according to the CPPS's application requirements.

The next step is to construct the secondary device network matrix $\boldsymbol{S}$, in which multivariate groups are used to model the node characteristics (such as delay and information processing), whereas the branch characteristics are derived through hybrid calculation (as introduced in the next section) based on matrix $\boldsymbol{C}$ and the correlation characteristic matrices


Decision-making node
Physical node
Cyber physical coupling model （P-I）
CPPS coupling model
Secondary device node
Physical node
Correlated characteristic （P-S）
P-S correlated characteristic model
Secondary device node
Secondary device node
Secondary device model （S）
Secondary device model
Decision-making node
Secondary device node
Correlated characteristic （S-I）
S-I correlated characteristic model
Secondary device node
Secondary device node
Secondary device function matrix （Diag(S)）
S model
Communication node
Secondary device node
Correlated characteristic （S-C）
S-C correlated characteristic model
Communication node
Communication node
Communication network （C）
C model
Secondary device node
Communication node
Correlated characteristic （C-S）
C-S correlated characteristic model
Secondary device node
Secondary device node
Secondary device function matrix （Diag(S)）
S model
Security and stability control services
Loads
Sources
DCs
Secondary device network simplification and equivalence
Security and stability control services
Loads
Sources
DCs
Communication network simplification and equivalence
Decision-making layer
Security and stability control services
secondary device
Communication node
Cyber physical coupling layer
Physical layer
Transformers
Loads
Sources
DCs
. . .

(a) Modeling framework

(b) Model Simplification and equivalence process

FIGURE 2. Modeling framework and calculation/analysis procedure for a CPPS.

S-C and ***C-S*** of the secondary device and communication networks, and the matrices are used to model the topology of the secondary device network.

The main difference between a communication node and a secondary device node is that the latter is capable of information processing; i.e., the input and output information can be different. Therefore, the diagonal elements of matrix ***S*** must reflect not only the processing time, interruption and processing error characteristics, as in matrix ***C***, but also the logical correspondence between the input and output (i.e., information processing). The multivariate group used to describe the functional characteristics of a secondary device node is shown in (2):

$$\mathbf{S}_{ii} = \left(F_{ii}\left(a_{input}\right), T_{ii}\left(F_{ii}\right), P_{ii}\left(F_{ii}\right) \ldots\ldots\right) \tag{2}$$

where $F_{ii}\left(a_{input}\right)$ is an information processing algorithm, which may have several components, such as an I/O processing algorithm $F1$, a host computer processing algorithm $F2$, and a communication algorithm $F3$. In this case, $F = F1 \cdot F2 \cdot F3$, where "·" represents a certain logical relationship. $T_{ii}\left(F_{ii}\right)$ and $P_{ii}\left(F_{ii}\right)$ represent the latency and error probability, respectively, of information processing.

Correlation characteristic matrices are then used to model the correlations between the physical layer and the secondary device network (***P-S***/***S-P***) and between the secondary device network and the decision-making layer (***S-I***/***I-S***). These matrices reflect not only the topological relationships among the physical-layer equipment, the secondary devices and the decision-making units but also other characteristics, such as information transmission delay and error.

Based on the CPPS model, the principles of the CPPS calculation and analysis process are shown in Figure 2(b). This process is achieved through the simplification and elimination of the communication and secondary device network models such that the equivalent effects of these networks are reflected in the final correlation characteristic matrix between the physical layer and the decision-making layer (***P-I***). "⊗" in Figure 2 represents the CPPS hybrid calculation algorithms, which will be introduced in the following section.

IV. HYBRID CALCULATION ARCHITECTURE

Section III introduces how to model the topology relationship in CPPS. The hybrid calculation architecture proposed in this section ("⊗"in Figure 2(a)) models the business relationship, such as the transmission path of the power system control signal in the communication network. The hybrid calculation architecture realizes the search of related devices and the calculation of key performance parameters between different layers according to the business relationship to support the simplified hybrid calculation of CPPS modeling as shown in Figure 2(b), thus supporting fast and accurate analysis for complex CPPSs.

A. HYBRID COMPUTING STRUCTURE

The three-layer hybrid calculation architecture is shown in Figure 3. It contains three subarchitectures: a communication network calculation subarchitecture, a secondary device network calculation subarchitecture, and a physical/decision-making layer calculation subarchitecture. The main functions of each subarchitecture include forming its model using real-time or historical data from the corresponding network/layer, performing calculations, analysis and optimization within that layer and providing services for other subarchitectures through data exchange interfaces.

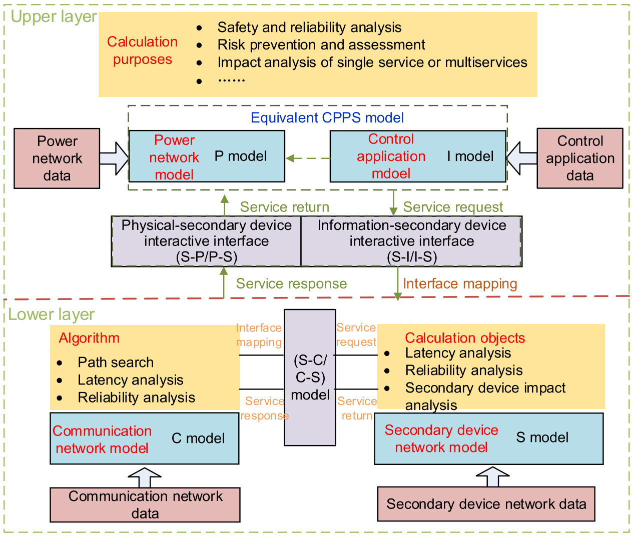


FIGURE 3. Hybrid calculation architecture.

The communication network calculation subarchitecture analyzes the communication performance, supports the optimization of the communication network, and provides calculation services for other networks/layers. It has three main functions: 1) Communication network model construction. Using real-time/historical/simulated data from the communication network, the communication network matrix $\boldsymbol{C}$ is formed, reflecting the communication characteristics, such as the real-time latency, the average latency, and the reliability. 2) Hybrid calculation algorithms for the communication network. Their main function is to simplify the communication network model, and they can be classified into three main types: ① core communication element filtering algorithms for specific power tasks, such as path search algorithms; ② calculation algorithms for key parameters, such as communication latency and interruption probability; and ③ communication network analysis and optimization algorithms, such as topological optimization algorithms. 3) Data exchange modules. These modules support data exchange with other subarchitectures.

Similar to the communication network calculation subarchitecture, the secondary device network calculation subarchitecture mainly calculates matrix S, simplifies the secondary device network model, and provides data to other subarchitectures. As shown in Figure 3, it also consists of three components: secondary device network model construction, hybrid calculation algorithms and data exchange modules.

The model simplification and equivalence procedures and the calculation of key parameters for the secondary device and communication networks are implemented in the corresponding calculation subarchitectures. The physical/decision-making layer calculation subarchitecture mainly focuses on the construction and calculation of the physical power system model ($\boldsymbol{P}$, either a steady-state or a dynamic model of the power system) and the decision-making model ($\boldsymbol{I}$, representing various analysis/control functions in the power system, such as stability control and AVC) based on the final physical/decision-making layer correlation characteristic matrix ($\boldsymbol{P}$-$\boldsymbol{I}$) obtained from the other subarchitectures. It also includes data exchange modules to support data exchange with other subarchitectures.

B. HYBRID CALCULATION PROCESS

The hybrid calculation process is shown in Figure 4. In accordance with the requirements for CPPS analysis and optimal control, from top to bottom, the calculation subarchitectures for the physical/decision-making layers, the secondary device network and the communication network are executed interactively.

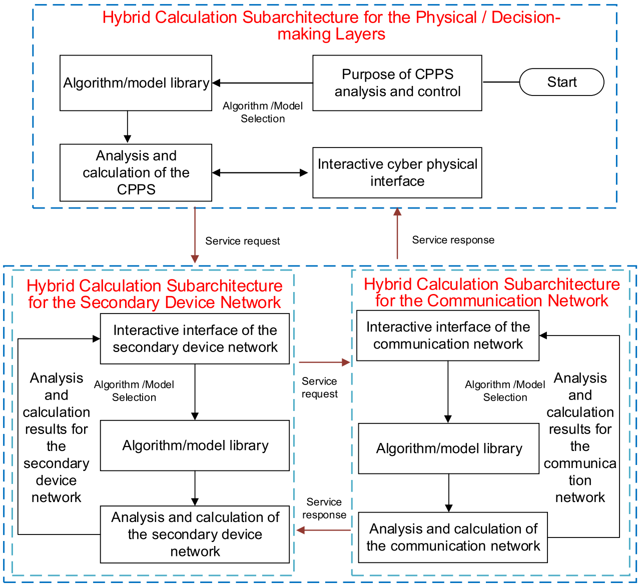

Hybrid Calculation Subarchitecture for the Physical / Decision-making Layers
Algorithm/model library
Purpose of CPPS analysis and control
Start
Algorithm /Model Selection
Analysis and calculation of the CPPS
Interactive cyber physical interface
Service request
Service response
Hybrid Calculation Subarchitecture for the Secondary Device Network
Interactive interface of the secondary device network
Analysis and calculation results for the secondary device network
Algorithm /Model Selection
Algorithm/model library
Analysis and calculation of the secondary device network
Service request
Service response
Hybrid Calculation Subarchitecture for the Communication Network
Interactive interface of the communication network
Algorithm /Model Selection
Analysis and calculation results for the communica tion network
Algorithm/model library
Analysis and calculation of the communication network

FIGURE 4. Hybrid calculation process.

Based on the analysis and control objectives, the hybrid calculation subarchitecture for each network/layer selects the appropriate hybrid calculation model and algorithm and performs the hybrid calculation. During the hybrid calculation process, data support from other networks/layers may be needed. This is implemented through the publication/response services provided by the architecture; i.e., data requests are first published to the other subarchitectures, and the other subarchitectures then respond, calculate the required data and send them back to the requester. For example, if the secondary device network must calculate the time delay for control command execution between a master station and a slave station, the communication channel latency is needed. Thus, the secondary device network calculation subarchitecture will publish a request for the communication channel latency, and the communication network calculation subarchitecture will respond by calculating and returning the required data.

C. HYBRID CALCULATION EXAMPLE

In the CPPS hybrid calculation architecture, a series of algorithms are coordinated to complete the requested analysis and calculation functions. Different analysis and calculation scenarios will require different calculation algorithms. In this section, a simple SSCS is chosen to illustrate the use of the calculation subarchitectures for the communication network and the secondary device network to calculate the control failure probability between two control stations (secondary devices).

This simple SSCS (with one slave station (SS), S1, and one execution station (ES), S2) and its associated communication network are shown in Figure 5. The calculation flow for calculating the control failure probability for S1→S2 using the proposed architecture is as follows:

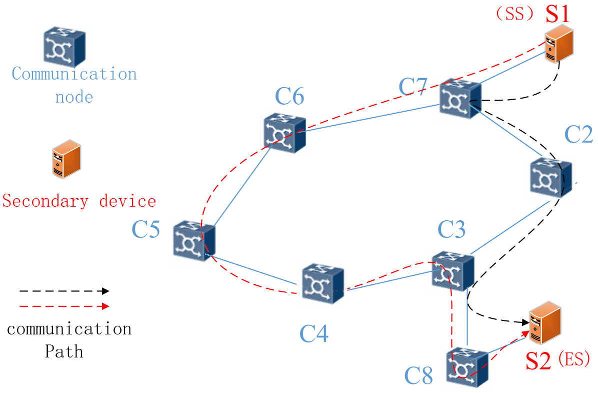


FIGURE 5. Topology of the SSCS.

(1) The secondary device network calculation subarchitecture:

1) In accordance with the requirements for the S1→S2 failure probability analysis, the failure probability model for the secondary devices of interest is selected, as shown in (3):

$$S = \begin{array}{c c} & \begin{array}{cc} S1 & S2 \end{array} \\ \begin{array}{c} S1 \\ S2 \end{array} & \begin{bmatrix} 0.01\% & P_{S1-S2} \\ P_{S2-S1} & 0.02\% \end{bmatrix} \end{array} \tag{3}$$

where the numbers in the matrix are the failure probabilities of S1 and S2 themselves and the failure probabilities between stations.

2) The failure probability calculation algorithm, defined as shown in (4), is used to calculate the control failure probability between the secondary devices:

$$P_{S1-S2} = 1 - (1 - P_C) \times (1 - P_{S1}) \times (1 - P_{S2}) \tag{4}$$

where P_{S1-S2} is the control failure probability between the slave station, S1, and the execution station, S2. P_{S1}, $P_{S2}P_{S2}$ and P_C are the failure probabilities of node S1, node S2 and the communication channel, respectively.

(2) Data exchange between the secondary device network and communication network calculation subarchitectures:

1) The secondary device network calculation subarchitecture publishes a data request (P_C) to the communication network calculation subarchitecture.

2) S1 and S2 are connected to C7 and C8, respectively; therefore, the correlation characteristic matrix ***S-C*** is defined as shown in (5):

$$S - C = \begin{array}{c c} & \begin{array}{cc} S1 & S2 \end{array} \\ \begin{array}{c} C7 \\ C8 \end{array} & \begin{bmatrix} 0.01\% & 0 \\ 0 & 0.02\% \end{bmatrix} \end{array} \tag{5}$$

where the numbers in the matrix are the failure probabilities of the interaction interfaces.

(3) The communication network calculation subarchitecture:

1) The communication network reliability matrix in equation (6), as shown at the bottom of the page, is constructed based on historical data. The communication path search algorithm is then applied to find the available C7→C8 communication paths, as shown in Figure 5: the main path is C7→C2→C3→C8, and the backup path is C7→C6→C5→C4→C3→C8.

2) As shown in (7), the communication failure probability calculation algorithm is used to calculate the failure probability for C7→C8:

$$\begin{aligned} P_m &= 1 - P_{7-2} \times P_2 \times P_{2-3} \\ P_b &= 1 - P_{7-6} \times P_6 \times P_{6-5} \times P_5 \times P_{5-4} \times P_4 \times P_{4-3} \\ P_{vp} &= P_m \times P_b \\ P_{vc} &= 1 - P_7 \times P_3 \times P_{3-8} \times P_8 \\ P_C^{'} &= P_{vc} + P_{vp} - P_{vc} \times P_{vp} = 0.2355\% \end{aligned} \tag{7}$$

$$\mathbf{C} = \begin{array}{c c} & \begin{array}{ccccccc} C2 & C3 & C4 & C5 & C6 & C7 & C8 \end{array} \\ \begin{array}{c} C2 \\ C3 \\ C4 \\ C5 \\ C6 \\ C7 \\ C8 \end{array} & \begin{bmatrix} 99.9\% & 99.0\% & 0 & 0 & 0 & 99.8\% & 0 \\ 99.0\% & 99.9\% & 99.5\% & 0 & 0 & 0 & 99.9\% \\ 0 & 99.5\% & 99.9\% & 99.7\% & 0 & 0 & 0 \\ 0 & 0 & 99.7\% & 99.9\% & 98.9\% & 0 & 0 \\ 0 & 0 & 0 & 98.9\% & 99.9\% & 99.9\% & 0 \\ 99.8\% & 0 & 0 & 0 & 99.9\% & 99.9\% & 0 \\ 0 & 99.9\% & 0 & 0 & 0 & 0 & 99.9\% \end{bmatrix} \end{array} \tag{6}$$

where $P^{'}_{C}$ is the C7→C8 communication channel failure probability.

(4) Data exchange between the communication network and the secondary device network calculation subarchitectures:

1) The communication network calculation subarchitecture returns the C7→C8 communication failure probability (P'_C) to the secondary device network calculation subarchitecture.

(5) The secondary device network calculation subarchitecture:

1) Based on the returned failure probability for C7→C8 and matrix ***S-C***, the communication channel failure probability, denoted by P_C, considering the interaction interface characteristics, is calculated as follows:

$$P_C = 1-(1-P^{'}_{C}) \times (1 - P_{S1-C7}) \times (1 - P_{S2-C8}) = 0.27\% \tag{8}$$

2) The failure probability calculation algorithm for secondary devices is used to calculate the S1→S2 failure probability, as shown in (9).

$$P_{S1-S2} = 1-(1-P_C) \times (1 - P_{S1}) \times (1-P_{S2}) = 0.30\% \tag{9}$$

Thus, the full matrix S is expressed as follows:

$$S = \begin{array}{c c} & \begin{array}{cc} S1 & S2 \end{array} \\ \begin{array}{c} S1 \\ S2 \end{array} & \begin{bmatrix} 0.01\% & 0.3\% \\ 0.3\% & 0.02\% \end{bmatrix} \end{array} \tag{10}$$

V. CPPS SECURITY DEFENSE SYSTEM

According to the proposed CPPS modeling and hybrid calculation architecture, this work develops the CPPS security defense system based on the traditional Wide Area Monitoring Analysis Protection-control (WARMAP).

A. STRUCTURE OF CPPS SECURITY DEFENSE SYSTEM

The overall structure of the CPPS security defense system is shown in Figure 6, which mainly includes the data interaction platform and the WARMAP control logic upgrade. The interaction platform realizes the data interaction between the WARMAP and the security and stability control equipment centralized monitoring and decision support application (SCMS), the telecommunication management system (TMS) and the energy management system (EMS) through the CPPS model and the hybrid calculation architecture to realize the access of the key parameters of the communication system to the WARMAP system. In the WARMAP control logic upgrade, the traditional control algorithm of WARMAP is modified, and the influence of the communication system is considered in the WARMAP to improve the defense ability for communication failure and realize the comprehensive defense of CPPS.

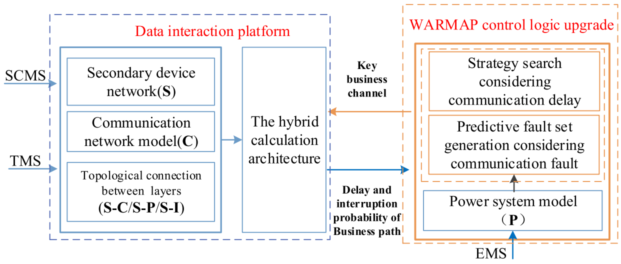

Data interaction platform
SCMS
TMS
Secondary device network(S)
Communication network model(C)
Topological connection between layers (S-C/S-P/S-I)
The hybrid calculation architecture
Key business channel
Delay and interruption probability of Business path
WARMAP control logic upgrade
Strategy search considering communication delay
Predictive fault set generation considering communication fault
Power system model (P)
EMS

FIGURE 6. Structure of CPPS security defense system.

WARMAP is used to address the impact of primary system faults on power grid security and stability. SCMS is used to monitor and analyze the SSCS. TMS is used for operation, monitoring and management of the power communication system. EMS is used for automatic monitoring, analysis and control of the power system.

B. DATA INTERACTION IMPLEMENTATION PROCESS

The data interaction implementation process is shown in Figure 7, mainly including three parts. In the first part, the core communication element filtering algorithm realizes the retrieval of the core components according to the security and stability control business path and clarifies the connection between these core components to retain the key components and key performance parameters and realize the simplification of the CPPS model. In the second part, the key parameter calculation algorithms work with the key components and performance parameters to realize the calculation of control delay and control reliability for the security and stability control business. The third part realizes the data interaction with WARMAP through the data interaction management module.

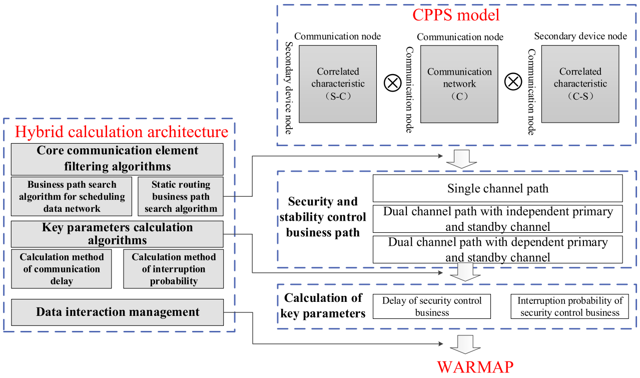

CPPS model
Communication node
Communication node
Secondary device node
Secondary device node
Correlated characteristic (S-C)
Communication node
Communication network (C)
Communication node
Correlated characteristic (C-S)
Hybrid calculation architecture
Core communication element filtering algorithms
Business path search algorithm for scheduling data network
Static routing business path search algorithm
Key parameters calculation algorithms
Calculation method of communication delay
Calculation method of interruption probability
Data interaction management
Security and stability control business path
Single channel path
Dual channel path with independent primary and standby channel
Dual channel path with dependent primary and standby channel
Calculation of key parameters
Delay of security control business
Interruption probability of security control business
WARMAP

FIGURE 7. Data interaction implementation process.

Based on the traditional WARMAP, the system architecture of CPPS security defense is designed according to the proposed CPPS model. Through the establishment of the data interaction platform, the data interaction between the communication system and the WARMAP is realized, and through the control logic upgrade, the cyber physical fusion analysis and CPPS security defense are realized. The development of the CPPS security defense needs only the further development based on the existing systems, which shows that the

CPPS model proposed in this paper has good practicability and compatibility.

VI. CASE STUDIES

To verify the validity and explain the application scenarios of the CPPS model and hybrid calculation architecture, based on the CPPS security defense system in section V, an ultrahigh-voltage (UHV) AC/DC hybrid power system is studied.

Figure 8 shows the structure of the SSCS, which contains one master station (MS), five slave stations (SS1-SS5), and 11 execution stations (ES1-ES11). The topologies of the secondary device network and the corresponding simplified communication network are shown in Figure 9, where the dotted lines are examples of upstream and downstream information paths.

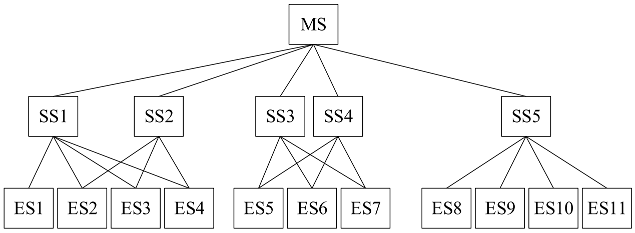


FIGURE 8. Structure of the SSCS.

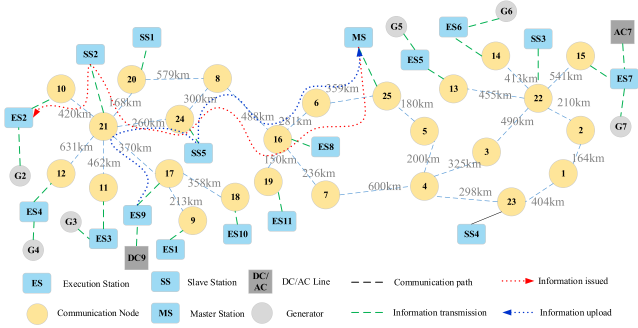


FIGURE 9. Topologies of the SSCS (secondary device network) and associated communication network.

When the UHVAC line AC7 fault and UHVDC line DC9 single-pole blocking failure occur simultaneously, the system will lose stability. Therefore, the SSCS will take action to keep the system in a secure and stable state. The procedure is as follows:

1) The detected AC7 line failure information is sent from ES7 to SS4 and then to MS.

2) The detected DC9 failure information is sent from ES9 to SS5 and then to MS.

3) MS identifies these two failures and determines the appropriate control strategy. The decision-making process is as follows: ① Find the control strategy matching the identified failures in the offline control strategy set (The security stability control system adopt the mode of ''off-line making, on-line matching'', that is, the control strategy are made in advance through off-line simulation, and when the fault occurs, the measures are matched according to off-line making). The offline control strategy for this N-2 contingency is to shut off one generation unit in each of G3, G5 and G6 and two units in G2. ② Calculate the real-time transient stability margin of the system after strategy execution (the default time required to shut down G3/G5/G6 is 300 ms).

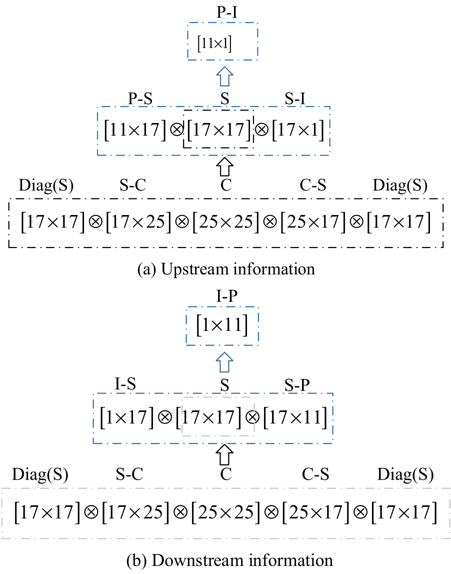
4) MS sends control commands to the related slave stations and execution stations.

A. STABILITY MARGIN ANALYSIS CONSIDERING REAL-TIME COMMUNICATION DELAY

To illustrate the effectiveness of the CPPS model and hybrid calculation architecture, based on the CPPS security defense system in Section V, the first scenario analyzes the stability margin considering real-time communication delay. By comparing the analysis results of traditional WARMAP, the effectiveness of the method proposed in this paper is illustrated.

1) CPPS MODELING AND HYBRID CALCULATION

MS simultaneously serves the functions of both a secondary device and a decision-making unit. In this case study, for the functions of data collection and transfer, MS is modeled as a secondary device node (S) in the cyber physical coupling layer, whereas its decision-making function is extracted and modeled as a decision-making node in the decision-making layer (I). Because the time delay is the characteristic considered in this example, for both the upstream and downstream information processes, only the associated time delay characteristics are included in the multivariate groups in all matrices. The framework of the matrix-based model is shown in Figure 10. The communication latency on an optical fiber line is assumed to be 5 μs/km.



(a) Upstream information

(b) Downstream information

FIGURE 10. Diagram of the matrix-based model framework considering time delay characteristics.

The modeling and analysis process is as follows:

① Set up matrices $\boldsymbol{C}$, $\boldsymbol{S}_{\mathrm{ES}}$, $\boldsymbol{S}_{\mathrm{SS}}$, $\boldsymbol{S}_{\mathrm{MS}}$, and $\boldsymbol{P}$-$\boldsymbol{S}$/$\boldsymbol{S}$-$\boldsymbol{P}$ based on real-time or historical data. The total time delay includes the action delays for primary equipment, such as circuit breakers. In this paper, to avoid formulating a separate matrix ***P*** to represent these action delays, they are included in matrix ***S-P***. Because of the simplicity of this example, matrices ***S-I*** and ***I-S*** are also not constructed, and the processing time of the decision-making node is simply included in matrix $\boldsymbol{S}_{\mathrm{MS}}$.

② Based on matrices ***C***, $\boldsymbol{S}_{\mathrm{ES}}$, $\boldsymbol{S}_{\mathrm{SS}}$, and $\boldsymbol{S}_{\mathrm{MS}}$, the hybrid calculation method for latency is used to retrieve the signal transmission path, calculate the information transmission delay considering the impact of the communication bit error on the secondary device network, and construct the full matrix ***S***.

③ Based on ***S*** and ***P-S/S-P***, matrices ***P-I*** and ***I-P*** are formed using the hybrid calculation method. These matrices will then be used as the inputs for the P-side calculation (the electromechanical simulation) and the I-side calculation (the decision-making function of MS, as mentioned above).

For ease of expression, ***S*** is expressed in block matrix form as shown in (11). $\boldsymbol{S}_{\mathrm{ES}}$, $\boldsymbol{S}_{\mathrm{SS}}$, and $\boldsymbol{S}_{\mathrm{MS}}$ represent the execution station, slave station and main station nodes, respectively. $\boldsymbol{S}_{\mathrm{ES}}$-$\boldsymbol{S}_{\mathrm{SS}}$, $\boldsymbol{S}_{\mathrm{ES}}$-$\boldsymbol{S}_{\mathrm{MS}}$, and $\boldsymbol{S}_{\mathrm{SS}}$-$\boldsymbol{S}_{\mathrm{MS}}$ represent the interaction characteristic matrices among these nodes.

$$\mathbf{S}=\left[\begin{array}{c:c:c}\mathbf{S}_{ES} & \mathbf{S}_{ES}-\mathbf{S}_{SS} & \mathbf{S}_{ES}-\mathbf{S}_{MS}\\ \hdashline (\mathbf{S}_{ES}-\mathbf{S}_{SS})^{\mathrm{T}} & \mathbf{S}_{SS} & \mathbf{S}_{SS}-\mathbf{S}_{MS}\\ \hdashline (\mathbf{S}_{ES}-\mathbf{S}_{MS})^{\mathrm{T}} & (\mathbf{S}_{SS}-\mathbf{S}_{MS})^{\mathrm{T}} & \mathbf{S}_{MS}\end{array}\right] \tag{11}$$

The elements of the diagonal matrix Diag(***S***) represent the information processing delay of each station. Diag(***S***) is also expressed in block matrix form, as follows:

$$\mathrm{Diag}(\mathbf{S})=\left[\begin{array}{c:c:c}\mathbf{S}_{ES} & 0 & 0\\ \hdashline 0 & \mathbf{S}_{SS} & 0\\ \hdashline 0 & 0 & \mathbf{S}_{MS}\end{array}\right] \tag{12}$$

The interaction delays and topology relationships between the secondary devices and the communication components are modeled by matrices S-C and C-S.

For the contingency considered in this case, the candidate control measures are to shut off generators G2-G7. The upstream information paths are DC9-ES9-SS5-MS and AC7-ES7-SS4-MS. The downstream information paths are MS-SS2-ES2-G2, MS-SS2-ES3-G3, MS-SS2-ES4-G4, MS-SS3-ES5-G5, MS-SS3-ES6-G6, and MS-SS3-ES7-G7.

Based on the established CPPS model, the CPPS hybrid calculation process is as follows: ① Run the initial P-side calculation (electromechanical simulation) using the Fast Analysis of STability using the Extended equal area criterion and Simulation Technologies (FASTEST) software to obtain the prefailure status of the physical system. ② Based on the status and failures on both the cyber and physical sides, calculate the cyber physical coupling relationship (i.e., construct matrix P-I or I-P). ③ Run the I-side calculation to determine the control strategy. ④ Based on the control strategy and P-I/I-P, run the P-side electromechanical simulation again to determine the impacts of cyber factors on the system stability margin.

Matrices ***P-I*** and ***I-P*** represent the delays of the upstream measurement information and the downstream control information, respectively. By combining these two delays, the action delay of each generator can be obtained. The action delays of G2, G3, G4, G5, G6 and G7 are 196.673ms, 196.837ms, 198.449ms, 194.281ms, 194.055ms and 194.682ms, respectively. The control strategy is to shut off one unit each in G3, G5 and G6 and two units in G2. Through the analysis of the CPPS security defense system, the resulting transient stability margin of the system is 48.56.

2) COMPARISON WITH THE RESULTS OF TRADITIONAL WARMAP

The traditional WARMAP does not consider the real-time status of the communication system, and the default time required to shut down the generators is 300ms. Through traditional WARMAP analysis, the resulting transient stability margin of the system is 23.71.

By comparison, the traditional WARMAP calculation results are more conservative, which may cause uneconomical control and other problems. In addition, in the case of communication interruption, it may lead to the failure of the security control strategy, thus jeopardizing the security and stability of the power grid.

Based on the CPPS model and the hybrid calculation architecture proposed in this paper, by connecting the communication system data to the WARMAP, the fusion analysis and defense of CPPS can be realized. The results show that the proposed method is reasonable and effective.

B. APPLICATION IN CYBER PHYSICAL FUSION ANALYSIS AND KEY COMMUNICATION LINK IDENTIFICATION

To show that the proposed method has good application prospects, in this part, an example is given to illustrate the application of the proposed method in two aspects: the impact analysis of communication bit error and the identification of key communication links.

(1) Impact analysis of communication bit errors on power system

Suppose that 1-bit error occurs on a communication link (C4→C23) during control command transmission from MS.

This bit error information will be reflected in the multivariate group corresponding to C_{4-23} in matrix ***C*** and will influence the corresponding $\mathrm{S}_{\mathrm{ES5}}$-$\mathrm{S}_{\mathrm{SS4}}$ and $\mathrm{S}_{\mathrm{ES6}}$-$\mathrm{S}_{\mathrm{SS4}}$ elements in matrix $\boldsymbol{S}_{\mathrm{ES}}$-$\boldsymbol{S}_{\mathrm{SS}}$. When the information processing functions $F(a_{\mathrm{input}})$ in the multivariate groups corresponding to $\mathrm{S}_{\mathrm{ES5}}$ and $\mathrm{S}_{\mathrm{ES6}}$ in $\boldsymbol{S}_{\mathrm{ES}}$ receive the error information, the information processing delay is found to be $\Delta\mathrm{T(F)} = 5\mathrm{ms}$ according to the communication processing mechanism (see section III) for secondary devices. At the end of the hybrid calculation process, PI_5 and PI_6 in ***P-I*** are each increased by ΔT(F) based on the original time delay.

As shown in Table 1, the FASTEST simulation indicates that a communication bit error on the C4→C23 link causes the system's stability margin to decrease from 48.56 to 41.77.

TABLE 1. **Total action times for generator shutoff and stability margins in various scenarios.**

Bit error link	T_{G2}	T_{G3}	T_{G5}	T_{G6}	Stability margin
no bit error	196.673	196.837	194.281	194.055	48.56
C4→C23	196.673	196.837	199.281	199.055	41.77
C21→C24	201.673	201.837	194.281	194.055	48.47

The result shows that the communication bit errors can significantly reduce the stability of the CPPS.

(2) Key communication link identification based on cyber physical fusion analysis

Suppose that 1-bit error occurs on a communication link (C21→C24) during control command transmission from MS. Similarly, the system's stability margin decreases from 48.56 to 48.47 due to this communication bit error on the C21→C24 link.

The results for scenarios with/without communication bit error are summarized in Table 1. Compared with a bit error on the C21→C24 link, a bit error on the C4→C23 link shows a greater impact on the CPPS, which means the C4→C23 link is the key communication link.

Aiming at the CPPS security defense system, the influence of communication bit errors and the identification of key communication links are studied, which shows the application scenario of the method proposed in this paper. Similarly, this method can be applied to other power services to improve the adaptability of traditional power services to cyber failures. In addition, with the development of SDN technology, the proposed method can be used in the scheduling and control of the communication system.

VII. CONCLUSION

This paper proposes a matrix-based CPPS modeling method that can effectively describe the complex coupling relationships within a CPPS. Based on this model, a hybrid calculation architecture is introduced that explains the complex interaction mechanisms between the cyber and physical systems and can be used to analyze the reliability and security of a CPPS. Based on the CPPS model and hybrid calculation architecture, the CPPS security defense system is established. The impact analysis of communication delay/bit errors and the identification of key communication links are analyzed for the actual UHV system, which shows the effectiveness of the model and proves that the proposed method has good practicability and rich application scenarios.

The proposed method provides ideas for the cyber physical hybrid calculation and analysis from the macroscopic aspect. Based on the existing systems, it can support the data interaction between different systems and realize the cyber physical hybrid calculation and analysis, which has good compatibility and practicability. However, how to solve the integration calculation of the discrete cyber model and the continuous power system model to comprehensively analyze and optimize specific applications is a problem that needs in-depth study.

APPENDIX

See below equations.

$$
\mathrm{C}=\begin{bmatrix}
0 & 0.82 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.02 & 0 & 0\\
0.82 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.05 & 0 & 0 & 0\\
0 & 0 & 0 & 1.625 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.45 & 0 & 0 & 0\\
0 & 0 & 1.625 & 0 & 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.49 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.405 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.795\\
0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.44 & 0 & 0 & 0 & 2.895 & 0 & 0 & 0 & 1.5 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.065 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.31 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3.155 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.275 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.065 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.705 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1.405 & 1.18 & 2.44 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.75 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.065 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.79 & 0 & 0 & 1.85 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.79 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.75 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.895 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.84 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.1 & 2.31 & 3.155 & 0 & 0 & 0 & 0 & 1.85 & 0 & 0 & 0.84 & 0 & 0 & 0 & 1.3 & 0\\
0 & 1.05 & 2.45 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.275 & 2.065 & 2.705 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2.02 & 0 & 0 & 1.49 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.3 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0.9 & 1.795 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

Communication network latency

$$
\mathbf{S}-\mathbf{C}=\left[\begin{array}{c|c|c|c}
11\times 8 & 11\times 11 & 11\times 5 & 11\times 1\\
\hline
5\times 8 & 5\times 11 & 5\times 5 & 5\times 1\\
\hline
1\times 8 & 1\times 11 & 1\times 5 & 1\times 1
\end{array}\right]=\left[\begin{array}{ccc|ccc|ccc|c}
0 & \cdots & 0 & 1 & \cdots & 0 & 0 & \cdots & 0 & 0\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots\\
0 & \cdots & 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 0\\
\hline
0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 & 0\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots\\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & 0\\
\hline
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1
\end{array}\right]
$$

$$
\mathbf{C}-\mathbf{S}=\mathbf{S}-\mathbf{C}^{\mathrm{T}}
$$

Correlation between communication network and the secondary devices network

$$\mathbf{S}_{\mathrm{ES}} = \begin{bmatrix} 3.001 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3.277 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3.148 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3.014 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4.354 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4.351 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4.006 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3.012 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3.003 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3.001 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3.007 \end{bmatrix}$$

$$\mathbf{S}_{\mathrm{SS}} = \begin{bmatrix} 3.001 & 0 & 0 & 0 & 0 \\ 0 & 3.002 & 0 & 0 & 0 \\ 0 & 0 & 3.001 & 0 & 0 \\ 0 & 0 & 0 & 3.003 & 0 \\ 0 & 0 & 0 & 0 & 3.001 \end{bmatrix}$$

$$\mathbf{S}_{\mathrm{MS}} = [9]$$

Information Processing Delay of ES, SS, MS

$$\mathbf{S}_{\mathrm{ES}} - \mathbf{S}_{\mathrm{SS}} = \begin{bmatrix} 3.76 & 0 & 0 & 0 & 0 \\ 2.94 & 2.11 & 0 & 0 & 0 \\ 3.16 & 2.32 & 0 & 0 & 0 \\ 4.10 & 3.26 & 0 & 0 & 0 \\ 0 & 0 & 2.28 & 6.17 & 0 \\ 0 & 0 & 2.07 & 5.96 & 0 \\ 0 & 0 & 2.71 & 6.61 & 0 \\ 0 & 0 & 0 & 0 & 3.96 \\ 0 & 0 & 0 & 0 & 3.16 \\ 0 & 0 & 0 & 0 & 4.94 \\ 0 & 0 & 0 & 0 & 4.70 \end{bmatrix}$$

$$(\mathbf{S}_{\mathrm{SS}} - \mathbf{S}_{\mathrm{MS}})^{\mathrm{T}} = \begin{bmatrix} 8.537 & 8.445 & 5.976 & 3.394 & 7.143 \end{bmatrix}$$

$$(\mathbf{S}_{\mathrm{ES}} - \mathbf{S}_{\mathrm{MS}})^{\mathrm{T}} = \begin{bmatrix} 12.30 & 10.56 & 10.77 & 11.71 & 8.26 & 8.05 & 8.69 & 11.10 & 10.30 & 12.08 & 11.84 \end{bmatrix}$$

Communication channel latency between ES, SS, MS (from calculation)

$$\mathbf{P} - \mathbf{S} = \begin{bmatrix} 20.83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 20.83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 21.50 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 20.63 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 20.61 & 0 & 0 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 0 & 20.64 & 0 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 20.95 & 0 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 20.87 & 0 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 21.20 & 0 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 21.13 & 0 & 000000 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 21.42 & 000000 \end{bmatrix}$$

Data collection delay (from calculation)

$$\mathbf{S}-\mathbf{P}=\begin{bmatrix}
140.83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000\\
0 & 140.83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000\\
0 & 0 & 141.50 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000\\
0 & 0 & 0 & 140.63 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 000000\\
0 & 0 & 0 & 0 & 140.61 & 0 & 0 & 0 & 0 & 0 & 0 & 000000\\
0 & 0 & 0 & 0 & 0 & 140.64 & 0 & 0 & 0 & 0 & 0 & 000000\\
0 & 0 & 0 & 0 & 0 & 0 & 140.95 & 0 & 0 & 0 & 0 & 000000\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 140.87 & 0 & 0 & 0 & 000000\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 141.20 & 0 & 0 & 000000\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 141.13 & 0 & 000000\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 141.42 & 000000
\end{bmatrix}$$

Command execution delay (from calculation)

$$\mathbf{P}-\mathbf{I}^T=\begin{bmatrix}39.801 & 38.34 & 38.42 & 39.22 & 37.14 & 37.03 & 37.34 & 38.61 & 37.80 & 39.58 & 39.35\end{bmatrix}$$

Upstream information transmission delay (from calculation)

$$\mathbf{I}-\mathbf{P}=\begin{bmatrix}159.801 & 158.34 & 158.42 & 159.22 & 157.14 & 157.03 & 157.34 & 158.61 & 157.80 & 159.58 & 159.35\end{bmatrix}$$

Downstream information transmission delay (from calculation)

REFERENCES

[1] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[2] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

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

[4] Y. Mo, T. Hyun-Jin Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[5] A. A. Cárdenas and R. Moreno, "Cyber-physical systems security for the smart grid," *Cybersecur. Cyber-Phys. Syst. Workshop*, 2012, pp. 1–6.

[6] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[7] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

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

[9] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.

[10] K. R. Davis, C. M. Davis, S. A. Zonouz, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 1–10, Sep. 2015.

[11] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber–physical energy systems for distributed sensing and control," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[12] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling future cyber-physical energy systems," in *Proc. Power Energy Soc. Gen. Meeting-Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–9.

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

[14] R. Olfati-Saber, "Flocking for multi-agent dynamic systems: Algorithms and theory," *IEEE Trans. Autom. Control*, vol. 51, no. 3, pp. 401–420, Mar. 2006.

[15] Q. Guo, S. Xin, H. Sun, and H. Wang, "Power system cyber-physical modelling and security assessment: Motivation and ideas," *Proc. CSEE*, vol. 36, no. 6, pp. 1481–1489, Aug. 2016.

[16] S. Xin, Q. Guo, H. Sun, C. Chen, J. Wang, and B. Zhang, "Information-energy flow computation and cyber-physical sensitivity analysis for power systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 329–341, Jun. 2017.

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

[18] Y. Susuki, T. J. Koo, H. Ebina, T. Yamazaki, T. Ochi, T. Uemura, and T. Hikihara, "A hybrid system approach to the analysis and design of power grid dynamic performance," *Proc. IEEE*, vol. 100, no. 1, pp. 225–239, Jan. 2012.

[19] G. K. Fourlas, K. J. Kyriakopoulos, and C. D. Vournas, "Hybrid systems modeling for power systems," *IEEE Circuits Syst. Mag.*, vol. 4, no. 3, pp. 16–23, 3rd Quart., 2004.

[20] A. G. Beccuti, T. Geyer, and M. Morari, "A hybrid system approach to power systems voltage control," in *Proc. 44th IEEE Conf. Decis. Control*, Dec. 2005, pp. 6774–6779.

[21] Y. Wang, D. Liu, and Y. Lu, "Research on hybrid system modeling method of cyber physical system for power grid," *Proc. CSEE*, vol. 36, no. 6, pp. 1464–1470, Mar. 2016.

[22] Y. Xue, M. Ni, and W. Yu, "Approach for studying the impact of communication failures on power grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[23] W. Yu, Y. Xue, J. Luo, M. Ni, H. Tong, and T. Huang, "An UHV grid security and stability defense system: Considering the risk of power system communication," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 491–500, Jan. 2016.

[24] Y. Xue, M. Li, J. Luo, M. Ni, Q. Chen, and Y. Tang, "Modeling method for coupling relation in cyber physical power system based on correlation characteristic matrix," *Autom. Electr. Power Syst.*, vol. 42, no. 2, pp. 11–19, Jan. 2018.

[25] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.

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

MANLI LI received the B.S. and M.S. degrees from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012 and 2015, respectively. He is currently an Engineer with NARI Technology Company Ltd., Nanjing. His primary research interests are cyber physical power systems (CPPSs) and stability analysis and the control of power systems.

YUSHENG XUE (Life Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Shandong University, Jinan, China, and the State Grid Electric Power Research Institute, Nanjing, China, in 1963 and 1981, respectively, and the Ph.D. degree in electrical engineering from the University of Liege, Belgium, in 1987. He has been an Academician with the Chinese Academy of Engineering, Beijing, China, since 1995. He is currently the Honorary President of NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing. He is also an Adjunct Professor with several universities in China.

MING NI (Senior Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from Southeast University, Nanjing, China, in 1991 and 1996, respectively. He is currently a Special Expert with NARI Technology Company Ltd., Nanjing. His current research interests include cyber physical power systems (CPPSs) and stability analysis and the control of power systems.

XIAO LI received the B.S. and M.S. degrees from Shandong University, Jinan, China, in 2016 and 2019, respectively. He is currently an Engineer with NARI Technology Company Ltd., Nanjing. His primary research interests are cyber physical power systems (CPPSs) and security assessment and control of power systems.