Academic Journal of Computing & Information Science
ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

# Research on Anti-interference Control of Information Physics System

**Li Meijun, Wang Miao, Li Shuai, Chen Youhui**

*State Grid Liaoning Electric Power CO,LTD. Power Electric Research Institute, Shenyang, Liaoning110015, China*

***ABSTRACT.*** *The Information Physics System (CPS, Cyber Physical System) integrates computing systems, communication networks and physical environments through computation, communication and control technologies to form a multi-dimensional heterogeneous complex system integrating real-time sensing, dynamic control and information services. Enable on-demand response, fast iteration, and dynamic optimization of resource configuration and operation within the CPS system. CPS is a comprehensive technical system that supports the deep integration of informationization and industrialization, and is of great strategic significance.*

***KEYWORDS:*** *CPS, Dynamic optimization, Optimal fit*

## 1. Introduction

The Ministry of Industry and Information Technology released the White Paper on Information Physics Systems (2017), stating that the essence of information physics system is to construct a set of state-aware, real-time analysis, scientific decision-making, and precise execution based on automatic data flow between information space and physical space. The closed-loop enabling system solves the complexity and uncertainty of manufacturing and application services, improves resource allocation efficiency, and realizes resource optimization. In 2017, the "Guiding Opinions of the State Council on Deepening the Integration of Manufacturing and Internet Development" further clearly stated that "the construction of the CPS model and the comprehensive technical standards system, the construction of a test verification platform, and the support for compatibility adaptation, interconnection and interoperability test verification". In the field of distribution network, through the "informatization, automation, interactive" intelligent distribution network construction and transformation work, distribution automation, PMS2.0, electricity information collection system, smart meter, terminal and other information communication systems The distribution network is gradually popularized, and distributed energy or electrical equipment based on flexible control such as photovoltaic, wind power, energy storage, and charging piles

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

further strengthens the controllability of the distribution network and the dependence on the information control system. Integrating advanced measurement system, data acquisition equipment, computing equipment and embedded flexible control equipment, the two physical networks of distribution network and information communication network are deeply interconnected, so that the primary system and the secondary system are coupled to each other in the distribution network. Contact, with the basic characteristics of typical CPS, distribution network CPS fusion system has become the development direction and form of smart grid and energy Internet [1-2].

Therefore, the dynamic interaction relationship between the physical equipment layer and the information layer of the distribution network under multi-scene disturbance and the evolution mechanism of the operational state are analyzed. The corresponding anti-interference control strategy is studied, and the CPS simulation application of the distribution network is carried out to improve the distribution dispatching physical information system. Reliability and safety management and control capabilities are important issues that need to be solved in distribution network CPS research, and have important theoretical and practical value.

## 2. Information physics system

Multi-level, multi-dimensional modern power system situational awareness and optimal control requires a large amount of real-time data exchange. The information layer and the physical layer establish an interdependence relationship, and the physical layer node provides energy support for the information layer node with which the dependency relationship is established; the information layer node provides 3C (communication, calculation, control) support for the physical layer node with which the dependency relationship is established. Interdependence is used as the interface between information layer and physical layer information and energy interaction. It improves the data collection type and communication efficiency, increases the real-time control capability of the system and enriches the control functions, but also introduces new reliability risks and faults. Form of development. The interdependence of the interdependent relationship becomes the channel of fault propagation, which leads to the decrease of the reliability of the system. The faults alternate between the physical layers of the information layer and bring about interactive cascading failures. The failure of the information layer will cause the grid control center to lose the ability to monitor and collect operational data of some power equipment or lose some control functions [3].

Based on the physical depth fusion characteristics of CPS information in distribution network, considering the multi-power constraints, multi-information constraints and the coupling relationship between information systems and physical systems, this paper studies the deep fusion and real-time interaction process of distribution network information physical systems under multi-disturbance scenarios. On this basis, the corresponding anti-interference control strategy is studied, which has important theoretical and practical significance for understanding the mutual

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

influence mechanism and fault risk management of the information layer-physical layer of the grid information physical system [4].

In view of the above-mentioned status quo, we will focus on the real-time fusion interaction and operation state evolution mechanism, fault process analysis and anti-interference control strategy of the information system and physical equipment system under multi-operation state of the distribution network, and achieve the following objectives:

(1) Study the dynamic interaction effects of distribution system information system and physical system and the evolution mechanism of system operation state under multi-scenario disturbances such as communication congestion, multi-type faults and information tampering, and provide theory for the study of overall safety control strategy of distribution network system. Basis and decision-making basis.

(2) Study the anti-interference control strategy of the distribution network under the multi-scene information system and physical system disturbance, and solve the problem of stable operation and reliability of the distribution network under multi-scenario disturbances such as communication congestion, multi-type faults and information tampering.

(3) Develop CPS anti-interference simulation technology for distribution network under multi-scenario information system and physical system disturbance to improve the reliability and power supply security of distribution network.

## 3. Economic benefits

It has a significant impetus to the development of CPS anti-interference simulation analysis technology for distribution network, which can effectively improve the safe and reliable economic operation level of distribution network, and has high economic and social benefits.

The dynamic interaction analysis of the distribution network information system and physical system under multi-scene disturbance and the research on the evolution mechanism of the system operation state can realize the simulation under the physical disturbance of CPS information of complex distribution network, which is communication congestion, multi-type fault, information tampering, etc. The dynamic change process and the real-time interaction influence provide simulation means, which provide decision-making basis for the safe and stable operation of the distribution network, and have good economic benefits [5-9].

## 4. Distribution Physical Information System

Today's information and communication technologies have been widely used in power systems, achieving the close integration of information space and grid physical systems, greatly changing the physical form and operation mode of power systems, and forming cyber-physical systems (CPS). ), power system operation analysis has also evolved into a CPS system operation analysis that considers the

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

interaction between information space and grid physical systems. In the future, CPS and its related theories will be the important realization of the next generation of power systems and the theoretical basis of analytical control technology. At present, the academic community has tried to explore the information-physical interaction process in the operation of CPS system, and has made some research in the fields of interaction between information space and grid physical system interaction, discrete information state (information flow) and continuous power process (energy flow). Progress, firstly, part of the literature constructs the interactive topology of information space and grid physical system in PGCPS, and discusses the dynamic changes of interactive topology in typical business scenarios and the impact of this change on the vulnerability of PGCPS. Second, some documents from PGCPS The system operation level discusses the cooperation mechanism between information flow and energy flow. Thirdly, some documents discuss the information-physical interaction process in the actual business scenario of PGCPS system operation. However, the above research results but the current research results still have great limitations. On the one hand, the information-physical interaction characteristics of CPS system operation are not deeply analyzed, and the analysis methods of CPS in other industries are applied. It is difficult to accurately describe the dynamic interaction process between discrete information state and continuous power process; on the other hand, the information-physical interaction topology ( The path of the system operation) and the information flow-energy flow dynamic drive (the event of system operation) are two closely coupled system operation element splitting research, and the research results only reflect part of the mechanism of information-physical interaction process, lack of information-physical A comprehensive study of the interaction mechanism makes it difficult to effectively explain the operating mechanism and evolution of the CPS system. CPS is a typical complex heterogeneous system. The information-physical interaction process of the system operation includes the information-physical interaction topology between the information node and the power node, the synergistic interaction between the information flow and the energy flow, and the superposition of the two. A number of information-physical interactions such as the evolution of the operating state of the generated CPS system.

There are multiple connection modes between the information node and the power node, and the connection state changes dynamically with the running state of the CPS system. On the one hand, CPS nodes have different functions and forms, so there are various connection methods, such as one-way single-channel type (one-way data transmission between transformers and merging units, etc.), two-way dual-path type (protection device and primary device) The device state monitoring path and the protection action execution path, etc., the two-way multi-channel type (three remote functions and protection paths between the power distribution terminal and the switch), etc.; on the other hand, under different operating states of the CPS, The connection status between nodes can be "connected and active" (normal work), "connection inactive" (alternate or faulty), "connected disconnected" (overhaul or fault). The above-mentioned information-physical interaction topology makes it difficult to directly establish a graph-based accurate CPS system operation model.The direct effect of an information system on a physical system means that

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

the failure of the information system component or function directly causes the corresponding physical component to fail. When the intelligent electronic device (IED) of the circuit breaker fails, the circuit breaker is shut down. The indirect effect of an information system on a physical system means that failure of the information system does not cause physical component failure, but it can lead to deterioration of physical system performance. This kind of influence can be divided into two kinds of situations. One is the potential impact of the failure of monitoring, control or protection function on the operation of the grid when the physical system is in normal operation. For example, when the grid monitoring fails, the line will not be able to know the operating status. Unable to deal with issues such as tidal crossing. The other is that when a physical system fails, the simultaneous failure of information will affect the troubleshooting process and worsen the system state. If the transmission network fails, the failure of the circuit breaker control function will cause a cascade failure.

The direct analysis of information physics takes into account the impact of information failure on physical components, and the analysis method pays more attention to the establishment of logical relationships between components. The indirect relationship of information physics is more concerned with the impact of information failure on the state of the physical system. This effect requires the simultaneous simulation of the information element fault and the physical state solution. Therefore, the analysis method used by different information physical action modes And the related models established are also different.

Aiming at the CPS coupling characteristics and its modeling methods, several related research groups at home and abroad have conducted some related research. A related scholar from Texas A&M University proposed a dynamic framework for characterizing the interaction between information system and physical system between generator and load. By introducing the input/output signals of physical system and information system, the role of information is reflected in each. The internal dynamics of the CPS module, local sensing and execution behavior. In view of the interrelated, interactive and tight coupling characteristics of the distribution network information system and the physical system, the Austrian National Institute of Technology (AIT) used the continuous time model and the discrete event model to model the CPS, and analyzed and compared the two types. Applicability of model pairs to CPS. To fully demonstrate the coupling between information systems and physical systems, the University of Ottawa, Canada proposes a CPS utility model in which each information system node has a support link with only one physical system node, and each physical system node is connected to Multiple information system nodes. The School of Computer Science of the University of Malaga in Spain corresponds to the CPS coupling characteristics and the smart grid. It analyzes the interaction principle between the information system and the physical system in the smart grid, and further proposes the possible security of the relationship between the systems. Sexual problems. In order to deeply study the coupling characteristics between smart grid information systems and physical systems, Power World of the United States proposed a CPS online simulation model architecture for smart grids, focusing on the analysis of possible interactions between information systems and

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

physical systems. The impact of grid reliability. In these existing CPS modeling studies, the main network and distribution network in the power system are not distinguished, and the fusion modeling research of the distribution network CPS needs further study.

Aiming at the modeling of active distribution network information system, the physical layer model of distribution network information communication system is established based on graph theory. The vulnerability of the distribution network information system and the impact characteristics of the distribution network are analyzed through the communication line. The link layer model of the substation communication network, which can reflect the detailed information parameters of the information system, such as the information transmission rate and transmission delay, except for the on-off of the line, and contributes to the network performance analysis and sensitivity analysis of the distribution network information system. the study. Aiming at the information part of the distribution network CPS, a physical layer model including multiple communication devices is established, and the influence of information system failure on the physical system is discussed.

In view of the modeling of the influence characteristics of the active distribution network information system on the physical system, the complex distribution network information system and the physical system joint model, and the results of the physical system state estimation under the condition that the information system data is incomplete and attacked Sexual analysis. The operating state of the physical equipment of the distribution network information system is classified. At the same time, the stochastic Bayesian network model is used to model the distribution network information system, and the influence characteristics of the information system on the physical system under different operating conditions are analyzed. The operation process of the distribution network control center is decomposed into discrete events. Firstly, the influence of communication delay and malicious attack on the operation process of the control center is analyzed, and then the influence characteristics of the discrete events of various information systems on the operational characteristics of the physical system are analyzed. The critical indicators of various discrete events occurred were quantified. Based on the above research status, it can be seen that the analysis of the impact characteristics of the distribution network information system on the physical system is mostly to discretize the operation process of the information system, and the physical system operation process is equivalent to multiple time sections, and the joint simulation analysis with the information system. There is no relevant quantitative analysis of the discretization of the physical system operating state and the critical index of the information system to the physical system control process.

## 5. Research Status of Anti-disturbance Control Strategy for Distribution Information Physics System

Information physics attacks are a serious threat to the security of critical infrastructure, so security analysis is increasingly important. Current mainstream methods for information security assessment include attack trees, attack graphs,

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

Petri nets, and game theory. The methods used in this paper include attack graphs and game theory. The attack graph is based on the attacker's perspective, comprehensively analyzing the configuration of various topologies and the relationship between the vulnerabilities, and the potential threats. Wang Yufei et al. improved the attack graph algorithm to make it suitable for quantitative evaluation. Liu abstracts the information domain and the physical domain into a whole structure, establishes a Petri net model and a hybrid game model, and quantifies the information physical attacks. Zonouz et al. extended the traditional attack graph and converted it into a hidden Markov model, making it possible to depict all possible attack paths. However, the impact of the attacker's proficiency on the assessment results was not considered. Zhang et al. established a Bayesian attack diagram to illustrate the attack process in the case of known vulnerabilities and zero-day vulnerabilities, calculate the average attack time of network vulnerabilities, and evaluate the reliability of the information physical system. From the above analysis, it can be seen that there are many security aspects in the context of information physics fusion at home and abroad, but it is less involved in attack path prediction. The graph-based attack path analysis can describe the causal relationship between multiple attacks and attack behaviors, and analyze the impact of unknown attacks and attacker capability levels on subsequent attacks. Wu Wenbo comprehensively considers the inherent characteristics of the vulnerability and the attacker's ability to calculate the probability of attack success, and calculates the attack consequences according to the importance of the host and the exploit pattern. This method can model the information domain and the physical domain as a whole, considering multiple cross-domains. The impact of an attack on system risk. Liu analyzes the dependence between assets by constructing the information physical dependence model and the probability matrix, and then introduces the security index to quantify the security state of the information physical system, and designs an information physical security assessment algorithm to calculate the index value and discover the potential threat propagation path. In recent years, based on optimization theory, Markov decision process (MDPs) and game theory, a large number of methods for defending against various attacks have been studied. Kim proposed a method based on optimization theory to protect the grid state estimator. The attack vector is considered to be a linearized measurement model. In this work, it is shown that such a network attack can be defended against a small number of measurement devices without being attacked. The grid attack graph generated by the existing model detection technology is interpreted as MDPs, and a value iterative algorithm is introduced to calculate the probability of successful attack. However, these studies ignore the attacker's decision-making process, and most of the research solutions can only optimize the defender's behavior through the expected benefits of the attack behavior. From the above analysis, it can be seen that there are many security aspects in the context of information physics fusion at home and abroad, but less involved in attack path prediction and defense resource allocation. From the above analysis, some problems exist in the current security analysis methods in the power information physical system:

(1) Due to the deep integration of the information domain and the physical domain in the power CPS, the network attack is not limited to the information

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

domain, and may even be infiltrated into the physical domain through the information domain to affect or destroy it. There are still deficiencies in the existing analytical methods for this type of permeable cross-domain attack.

(2) The current defense strategy is implemented in the power CPS. Different devices will be provided with protection measures to isolate each other. Usually, the target cannot be directly attacked. It is necessary to use the loophole on the device as a bridge to achieve the purpose of attack. Existing analytical methods for such multi-step attacks have their own drawbacks. Moreover, the traditional attack graph method cannot accurately reflect the impact of the complexity of the attack behavior on the subsequent attack path, so that the accuracy of the attack path prediction is not high.

(3) Information physical cooperative attack is an attack behavior adopted by an attacker to achieve the maximum attack effect with minimum cost. Game behavior can be analyzed for this behavior, but the existing information physical cooperative attack against power CPS Most of the research did not take into account the fact that the participants in the actual offensive and defensive situation are selfish, that is, bounded rational behavior. Neglecting this behavior, the modeling and analysis of information physics collaborative attacks will deviate from the actual situation, resulting in the selected defense strategy will be weakened in accuracy and guidance value.

CPS establishes an information physical simulation fusion system through abstract information, calculation process and physical components, and increases the correlation between energy flow and information flow, so that information system and physical system can better cooperate. Traditional information system modeling is passively matching physical system modeling. Depending on the physical system, the mutual benign influence between the two is small. Information system modeling cannot be separated from physical system modeling. The service-oriented CPS architecture can flexibly access model objects and services, establish a fusion model of information process and physical dynamics, and fully describe the global relationship model of information flow and energy flow. The challenges faced in the CPS modeling process, and given solutions such as model of computation, modularity, object-oriented modeling, etc. When analyzing CPS modeling methods, mentioning hierarchical and temporal parallel features, and It can be applied to the modular structure of the hybrid system model, which has been widely used in distributed computing. The basic steps of CPS modeling and application are detailed from the perspective of state machine model. The control effect of the model is demonstrated by examples. The combination of CPS technology and power grid is proposed. Object-oriented modeling is used to establish a grid with similar forms. The component model and the information flow model can interactively simulate the information model described by UML with the physical model based on Matlab/Simulink, which can verify the missing information of the simulation system. From the two aspects of network parameters and service parameters, a comprehensive analysis is carried out, but the influence of parameters such as signaling length and channel quality is not fully considered. It will be applied to the automation of distribution network. The design and improvement of some network

ISSN 2616-5775 Vol. 3, Issue 3: 9-17, DOI: 10.25236/AJCIS.030302

components in the system implementation are given at the physical layer and the data link layer, and it is pointed out that the network is a difficult way to build a communication network in a small-scale distribution automation system. An economically viable approach. The distribution network communication system is used to complete all the functions of the distribution network, and each device in the distribution network is assigned a network address reflecting its location information, and the distribution network devices communicate in the form of datagrams, but The problem of data link layer in technology application to distribution network communication is not involved. Traditional substation automation and distribution automation rely on proprietary communication networks, and communication-based methods can support multiple application services simultaneously in a single network, and analyze the advantages of technology applications in a business case. The modeling of distributed power supply in control and communication system introduces the expansion of the two in distributed power supply. From the perspective of control and communication, it describes the operation and management of distribution network with distributed power supply. It shows how to pass the application case. The control center coordinates the various distributed power output to minimize distribution network operating costs.

**References**

[1] Xue Yusheng, Yu Xinghuo. Beyond smart grid-a cyber-physical-social system in energy future[J]. Proceedings of the IEEE, 2017,105(12): 2290-2292.

[2] Sheng Chengyu, Gao Haixiang, Chen Ying, et al. Overview and prospects of network simulation of information physics power system [[J]. Power System Technology, 2012, 36(12): 100-105.

[3] Liu Dong, Sheng Wanxing, Wang Yun, et al. Key Technologies and Progress of Grid Information Physics System[J]. Proceedings of the CSEE, 2015, 35(4): 3522-3531.

[4] Park K J, Zheng R, Liu X. Cyber-physical systems: milestones and research challenges [J]. Computer Communications, 2012, 36(1): 1-7.

[5] Zhao Junhua, Wen Fuzhen, Xue Yusheng, et al. Research framework for modeling analysis and control of power information physical fusion system [[J]. Automation of Electric Power Systems, 2011, 35(16): 1-8.

[6] Buldyrev S V, Havlin S, Parshani R, et al. Catastrophic cascade of failures in interdependent networks [J]. Nature, 2010, 464(7291): 1025-1031.

[7] Wang Yufei, Gao Kunlun, Zhao Ting, et al. Assessment of cross-space cascading failures of power information physics systems based on improved attack graphs[J]. Proceedings of the CSEE, 2016, 36(6): 1490-1499.

[8] Chen Yuanfei, Zhu Zhenmin, Lu Xiaowen. Intelligent space modeling method based on information-physical spatial mapping[J] Journal of System Simulation, 2013, 25(2): 216-219, 227.

[9] Wang Yun, Liu Dong, Lu Yiming. Research on hybrid system modeling method for grid information physics system[J]. Proceedings of the CSEE, 2016, 36(6): 1464-1470.