Key issues and technical route of cyber physical distribution system

P X Zheng¹, B Chen², L J Zheng³, G L Zhang², Y L Fan² and T Pei³, ⁴

¹ State Grid Fujian Electric Power Co., LTD., Fuzhou 350003, China
² State Grid Fujian Electric Power Research Institute, Fuzhou 350007, China
³ Electrical Engineering, Zhejiang University, Hangzhou 310027, Zhejiang Province, China

E-mail: welcome_pt@163.com

Abstract. Relying on the National High Technology Research and Development Program, this paper introduced the key issues in Cyber Physical Distribution System (CPDS), mainly includes: composite modelling method and interaction mechanism, system planning method, security defence technology, distributed control theory. Then on this basis, the corresponding technical route is proposed, and a more detailed research framework along with main schemes to be adopted is also presented.

1. Introduction

Cyber physical system integrates computation, networks and physical environments into a multi-dimensional complex system via 3C (Computation, Communication, Control) technology, and enables large-scale project to realize real-time perceiving, dynamic controlling and information services [1]-[2]. As the level of the utilization of information enhances unceasingly, Modern distribution system has developed to be a multi-dimensional cyber physical distribution system (CPDS) which highly relies on information, and follows traditional power system process [1][3]-[4].

Although the traditional distribution system which has a complete “produce-supply-users” ternary coupling mode, has been mature enough, with varies of distributional sources, storages, protections and sensors plugging in, acute problems such as distribution system topology, information interaction, cyber-physical integration come into sight.

Compared to traditional distribution system, CPDS has distinguishing features:

(1) Multi-source isomerism, complex network.

The distributional loads and the intermittent renewable sources changed the feature that power flows in single direction, and the exponential growth in the sensors along with communication devices, also caused the physical topology to grow enormous and complex, and its dynamic behavior becomes non-linear, uncertain, time-varying, and isomeric.

(2) Frequent interaction, and hence vulnerable

Since smart meters, distributional storages and sources plug in, to realize massive information collecting, transferring, controlling and demand side response, power flow and information flow interacts frequently, thus information security becomes a serious problem. While the communication protocol, which is open and standardized, also bring new hidden dangers to traditional power system field, such as dispatching automation, relay protection and safety equipment automation, load control,
user information collection and dispatching automation, relay protection and safety equipment automation, load control, and user information acquisition.

(3) Hierarchical scheduling, difficult to defend
By applying single strategy like centralized control or decentralized control cannot synthetically take investment, control validity, and communication reliability into account. While distributed control can satisfy such system demand. However, power system adopts hierarchical scheduling, hence the system relies on the communication network heavily, and increases the difficulty to control and to defend.

CPDS is a relatively new concept, and research achievements about electric information intelligent synchronization and acquisition, intelligent and digital monitoring equipment have been made. However, how to understand and analyze the inter-action mechanism between power system and cyber system, how to build a mathematical model considering energy flow, information flow and service flow, how to utilize information technology to enhance system security, these questions have not yet been solved.

Therefore, this paper illustrates key issues on CPDS integrated modelling, system organization, security defense and distributed control, then provides research directions and preliminary solutions for other researchers to reference and feasible approaches to consider.

2. Introduction of key issues in CPDS

2.1. Integrated Modelling Method and Interaction Effect Mechanism
CPDS integrated model is the theoretical basis of control strategy, network security and organization. As for the traditional power system analysis and control, the influence made by cyber system is neglected. Generally the assumption that the system information acquired is timely, accurate and reliable. Moreover, power system use dedicated network that has less interfaces to external network, thus the reliability and security can be assured [2][5]-[6]. However, the applying of massive PMU and smart meters, distributed energy devices, and high sample rate sensors, means there will be amazing amount of data existing in the CPDS communication network. Power system’s dependency on cyber system has to go deeper. Therefore, when considering built a CPDS model, the assumption above is no longer reasonable. Network security problems such delay, packet loss, and malicious attack will bring influence on power system. Hence in the integrated model, cyber system shall deserve equal attention as power system. But how to quantize and evaluate information, how to organize operation, there is a lack of mature theatrical framework.

To study the interaction between power system and cyber system, firstly the unified modelling method, namely the cyber-physical modeling, shall be determined [3]. Physical system is a continuous system, while cyber system is a discrete system. They have different math basis and simulation method. The primary question to develop a complete modeling theory, is how to eliminate the barrier between power system and cyber system. Up till now, researches on modelling have not yet provide effective modeling theory that can both fully and accurately describe the interaction between cyber system and power system, and the traditional power system modeling architecture has not been broken, thus the influence made by cyber system cannot be accurately depicted.

This paper presents research contents on CPDS integrated modeling and interaction effect mechanism: analyze the sources, load, topology in traditional distribution system and measurement, communication, computation in cyber system, then find out the unified model which can represent the dynamic features of power system and execution order of cyber system: clarify the influence, which is caused by complex distributed cyber system, on power system from both steady and dynamic field, and study how it will affect the stability and reliability of distributed system.

2.2. Planning method
As coverage area, power capacity and the type of equipment grows larger and larger, nowadays distributed system has come close to its limit of operation. So it is vulnerable to varies interference,
and then becomes a threat to safe and stable operation for whole system. Besides, with the increase of cross-regional large-scale interconnected power grid, once the effect brought by power failure would be limited in local area, but now the effect will spread out to adjacent power areas, thus expanding the scale of the accident. Therefore security factors shall be fully considered at the stage of power system planning, and narrow the scale of accident, reduce the loss of social economy to the greatest extent.

To those traditional power system which only contains synchronous generator and loads, the main theory to determine power system subareas are: graph theory [7], slow coherency [8][9] and intelligent optimization [10][11]. However, in traditional power system there are few distribution generators, storages and other new power devices such as smart meter, PMU, those methods for subareas above cannot apply to complex power system to answer for cyber security.

This paper presents research contents on CPDS planning method: based on the interaction mechanism among distributed system, communication network and cyber system, find the composite restrain for both energy transfer property and information demand in CPDS planning, then build a composite model for multi-object CPDS planning; and this paper studies the coordinated planning based on CPDS technology for distributed system, communication network and cyber system; this paper also presents an on-line planning method based on isolated-island, which is used under conditions like serious device failure or malicious communication attack. With the proposal of planning method for CPDS, the corresponding evaluation mechanism will be updated.

2.3.  Cyber Security
CPS is a dual heterogeneous composite network, its security problems includes virtual network security for cyber space and real network security for physical space, and along with coupling risk caused by the interaction between two spaces [4][12]-[13]. Since public network and open protocol have been applied, cyberspace security risk degree increased.

At present there are relatively few researches carried on CPDS cyber security, and most researches only focus on process control system, smart meters, communication protocols, wireless communications networks, and other independent areas, lacking complete system. Therefore, to build a complete framework, firstly CPDS property should be clarified, then combined with computer network theory, high risks that threatens power system operation steadily should be analyzed.

This paper presents research contents on CPDS cyber security: the research on cyber space and power space and their risk mapping model, coupling and propagation mechanism. The illustration on vertical transmission way, namely how risks in cyber space spread across space edge and finally cause power system failures, and the back propagation way, namely how power system failures react on cyber system and finally cause cyber security threat. Based on the interaction mechanism between power system and cyber system, propose the analysis method for CPDS cyber security fragility. The research on security flaw in cyber space, and on this basis, carry out research on active defense strategies based on outlier detection and fault diagnosis technology.

2.4.  Controlling Strategy
Power balance and voltage/frequency stability is the premise for normal operation of power system. However, with high density, distributed, intermittent, heterogeneity features, renewable energy power generation system and storage system cause traditional primary control and secondary control method cannot satisfy this new situation. Furthermore, increased complexity of communication network and other power devices tightly coupled, this also increased the demand for robustness of system control and interference resistance. How to realize coordinated control under the circumstances of CPDS’s time-vary, complex network environment, and realize power balance and voltage/frequency stability control, are important problems needed to resolve.

Traditional control methods for distributed source/storage include centralized control and decentralized control.

Centralized control is one of the most common, and also the simplest kind of control methods. In centralized control mode, every power device communicates with control center (SCADA, EMS)
Flow [5]-[13]. However, when there are more and more controlled units, it is difficult for centralized operating point. The main corresponding control method for centralized control is Optimal Power Flow [5]-[13]. However, when there are more and more controlled units, it is difficult for centralized control mode to satisfy instantaneity and flexibility. And when some certain communication line or device encounter failure because of attack behaviors (physical failure, malicious data), centralized control mode will face the danger of breakdown, and the corresponding control strategy don’t possess the ability of security and stability control.

In contrast to centralized control, decentralized control is a control method that suitable for sources and storages which are decentralized geographically, and have varies features, and this control method enable loads to operate effectively and steadily, meanwhile it can increase system safety margin. The main corresponding control methods for de-centralized control are: droop method [14][15], anti-droop method [16], and maximum power point tracking methods [17][18]. In decentralized control mode, every device connect directly to its monitoring system, and realize the stable control of itself by local control. Hence it possess high flexibility, and strong ability to against network security threats. Decentralized control mode is especially suitable for the remote areas that is difficult for power grid to effectively cover. The effective control among source, storage and load can be achieved simply by local controller, and hidden risks of chain accidents can be also averted. However, because in this control mode, every power device act dedicatedly, they cannot act like “Virtual Power Plant” to support the whole power grid, such as voltage support and frequency stability. Moreover, decentralized control is not suitable for relatively concentrated power area.

With the continuous development of distributed computation, multi-agent and network control theory, distributed energy coordinated control gradually show its steady, safe and reliable control ability. In distributed control mode, every device (source, storage, load) all connect to its adjacent devices. The control method is determined according to the interaction in neighborhood, and in this way the control can control active power and reactive power coordinately, and can also avoid influences brought by cyber network failures, such as communication delay and interruption. Therefore distributed control possess high flexibility, perturbation resistance and the ability to face cyber space risks. Taking the distribution and complexion of CPDS physical environment into account, many researches aimed at CPDS distributed control method have been carried out. The coordinated control strategy using distributed power sources and reactive power compensation equipment is proposed [19]. And there is another coordinated control strategy aiming at solving massive distributed storage devices [20]. However, because of the variety of scale, structure, and control units in distributed system, and different kinds of computation restraints, CPDS distributed control is a quite challenging issue. Among these researches, the main consideration is the effect that communication part brings to control part, and control object is fair simple, moreover, these researches only discuss local optimization control, and there is a lack of the factors about communication and computation.

This paper presents research contents on CPDS control strategy: considering CPDS is a multi-level distributed system, carry out research on control strategy which contains computation, communication and physical objects; discuss proper distributed source output distribution strategy, and for the micro power grid, to find out the autonomous operation control strategy; aiming at the topology structure already exists, to propose control strategy from aspects such as convergence, robustness and flexibility.

3. Integrated Modeling Method
Further study on CPS such as control algorithm and system evaluation must have an appropriate system model to support. The problem is that cyber system and power system are based on different theoretical basis. More specifically, cyber system is generally driven by information/events, and its theoretical basis is discrete mathematics, its modeling tools are discrete mathematics tools, such as the finite automaton. On the contrary, power system is based on continuous mathematics, and its modeling tools generally are algebraic equations and differential equations. The difference on theoretical basis
and modeling tools are the basic reason for the split between power system and cyber system [1]. And up till now, no integrated model effective and accurate enough has been proposed.

Some researchers have obtained achievements on modeling theory. In [21], CPS sub-modules are divided according to its function, after comparing their features in both physical and cyber space, these sub-modules are integrated into a whole CPS model. On this base, in [16], by trial and error process, the C model and P model come to one correspondence, and according to such single cyber-physical model, all C models are used as logical node in connection, so a “C-integration” is obtained. And P model is treated as a function module, and are connected to get a “P-Integration”. Finally the two module are integrated into a whole CP model. And by this way, the CP models for photovoltaic, energy storage are deduced, and then proposed a method to simulate on the CP model by dynamic link library. In [17], a CPS computation platform based on large scale distributed computing technology was suggested to realize CPDS controlling. Besides, in [18], the conception of CPS was introduced into relaying of smart distributed system, and some detailed components of this system and their functions, structures were also presented. The paper then compared this system with traditional system, and concluded that the new system could deal with complex algorithm because of its distributed computation ability.

However, the coupling relationship among power system, communication system and cyber system, hasn’t been reflected in these modelling methods; for the dynamic property like packet loss and delay, there are not relevant researches, either. More specifically, all the models above trend to the benefits that will come from cyber system, while there is a lack of consideration about the negative effects that cyber system will bring to power system. For instance, when massive monitor data collected suffers cyber space delay, the control center of power system would not react in time, and cyber system would be a burden to power system.

There are two available ways for the co-simulation of CPDS model: simulation with power system expanded, simulation with cyber system expanded, and simulation combined physical system and cyber system.

Simulation with power system expanded means: based on the simulation platform of power system that already exist, integrate simulation model and method of discrete event system. For discrete event system description, a practical way is add continuous system simulation language as packet form into simulation platform, such like Nutaro J et al. [19]. However, because of the lack of necessary elements of discrete event system, like dynamic memory management and dynamic linking, there is difficulty to simulate the dynamic processes in cyber space accurately [20].

Simulation with cyber system expanded means: based on the simulation platform of cyber system that already exists, integrate simulation model and method of continuous system. There are some examples utilized this thought. Such as Agent/Plant and generalized discrete time system specification [21]. The advantage of this thought is high flexibility, convenience for information interaction, and it enables independent subsystem simulation. But since every single discrete event needs computation of all the network, when the continuous system is relatively large scale, the computational work would be quite heavy.

Simulation combined physical system and cyber system means: based on the simulation platforms of physical system and cyber system and the cooperation of both, realize the co-simulation of continuous system and discrete system. For instance, combine physical system platform (Modelica and VTB) with cyber system platform (NS2 and OPNET) to form a new co-simulation platform [22].

These methods described above adopted mature simulation platforms, so the accuracy and reliability of simulation results can be guaranteed; however, the order that physical system follows is time-order, while event-order for cyber system. So the problem about timing synchronization needs further study.

This paper presents a general outline for CPDS integrated modelling: first of all, build appropriate models for computation, communication and sensor devices using theory such as queuing theory, Markov chains, stochastic process, and stochastic differential equations; then, analyze the interface variances between physical and cyber space, such as network delay, message error, to clarify the
relation between the two spaces; last, fuse two models by integrate mathematical models, and obtain a complete CPDS model.

As for computation unit (usually made up of processor and cache), queuing theory and stochastic process can be chosen to build models. When a computation task reaches the computation unit, it will queue in data cache. The tasks first come will be first served, so in queue theory, D/G/c/∞ or M/G/c/
∞ can be chosen as the model for computation unit. In distributed system, computation tasks include kinds of power system analysis (power flow calculation, on-line security analyze) and control strategy decision (such as calculate the optimal control strategy for distributed sources).

The main concerns of cyber modeling are the properties of data link layer, network layer and transport layer. To simulate network congestion agreement, differential algebraic equations driven by finite automaton can be used to describe three different discrete states (empty queue, full queue and common queue), and their properties will be described by differential algebraic equation, and three states will have interconversion.

Modeling for sensor units needs to know the stochastic process that the data rate of sensor units obeys. Adoptable models include Markov process like Poisson process, and Heavy-tailed process like Pareto process. Considering that sensors may have multiple discrete work states, the model for sensors could be stochastic process driven by Markov.

In conclusion, the continuous changes of state variances (e.g. size of queue, size of congestion window) in CPS can be described by differential algebraic equations; while the discrete state variances can be described by finite automation or Markov Chain. As for uncertainty of system (e.g. data rate of sensors, processor speed), several appropriate stochastic processes can be used to depict. All the models combined with traditional power system model will come to a complete CPDS model. And the time scale conflict, which is caused by continuous time and discrete time, can be solved using ultra-dense time model, which inserts discrete time into continuous time axis, so continuous time and discrete time can be combined. For continuous and discrete transition, a new clock variance should be introduced, and this clock is an infinite discrete time series, which can discretize continuous time by sampling, hence combine continuous transition with discrete transition.

4. Planning method

For modern power system that contains distributed sources, storages, controllable loads and varies communication devices, since the high digitized degree, the planning method for traditional power system cannot satisfy the demand of safe and stable operation. Therefore, scholars home and abroad proposed new planning methods for informationized modern power system.

Arefifar S A et al. [23] proposed a partition strategy for power system which can realize self-sufficiency, with mathematical models of photovoltaic, windmill, energy storage, load and reactive power source, an optimized objective function based on power loss objective functions and power unbalance functions. When the restrictions of power and voltage are satisfied, the optimal partition strategy will be determined by tabu search algorithm, and such strategy can reduce system loss and power unbalance. Atwa Y M et al. [24] proposed a planning strategy for power system by properly configuring different kinds of renewable sources to reduce system loss, and the optimal solution was obtained via a mixed integer nonlinear programming problem whose restrictions are voltage, current, capacity and power. Kleinberg M R et al. [25] proposed a partition strategy based on capacitance reactive power domain, together with a distributed control algorithm based on exhaustive search to reduce voltage fluctuation and capacitance reactive power loss. Mehrjerdi H et al. [26] proposed a scheme for power system partition and secondary voltage control by the means of graph partition and key bus choice, meanwhile after partition the reactive power in every subarea will be controlled by fuzzy controller, so the voltage in every isolated island can keep stable. Arefifar S A et al. [27] proposed a distributed system partition method referring to previous research achievements, and this method considered communication and power in the same time. The optimal partition strategy was determined using tabu search algorithm, graph theory and power flow calculation based on Newton
Raphson, and it can satisfy communication delay and its cost, power balance, voltage, current, and frequency.

From the analysis above, a conclusion about modern power system (e.g. smart grid) can be drawn: the existing partition method only considers single aspect (e.g. reactive power balance, active power balance, power loss, communication cost), it is hard to satisfy the composite demand from communication, control, power and security in modern power system; there is a lack of analysis for interactions between physical network and cyber network, and it is difficult to obtain the mathematical description for dynamic properties of the system; and usually the attention is paid to modern power system which contains distributed sources, while for the traditional synchronous generators, the ability to face emergencies should not be neglected.

Power CPS planning method may include three level, namely property analysis for physical device, construction for communication network, and planning design for whole system.

(1) Property analysis for physical device
Physical devices in modern power system trend to be diversified, and there are quite difference in their physical properties, work modes, and control principles, so it is not easy to analysis the whole system. By using probability statistics, power electronic technology and control theory, along with the mathematical models of these devices, the descriptions for power flow and information flow will be preliminarily established, and provide basic elements for CPS integrated model.

(2) Construction for communication network
For physical network that is constructed of complex power devices and communication devices, the heuristic learning method can be used to strengthen security of communication network. Meanwhile, a communication system based on cable communication and wireless communication can be established to increase communication reliability.

(3) Planning design for whole system
First of all, establish appropriate models for computation, communication and sensor devices using proper theory such as queuing theory, Markov chains, stochastic process, and stochastic differential equations; then, analyze the interface variances between physical and cyber space, such as network delay, message error, to clarify the relation between the two spaces and realize fusion of these two models; later, obtain the steady-state operating point of cyber system via the optimal routing problem, and analyze the dynamic property based on “N-1” principle, and then discuss the reliability and security of the system.

To avoid uncontrollable splitting, and increase the ability to face security risk, at present the most efficient method is controllable island based on system partition [28]. The fundamental conception is that, when a risk or failure is detected, the system will be divided into several controllable isolated islands (or micro girds) that are self-sufficient; when the risk or failure is eliminated, these islands can connect with each other by switches, and come back to original state.

Therefore, on the base of CPS model and the analysis of interaction scheme, the partition method that based on slow coherency theory, power domain and distributed optimization can be adopted to divide the power system into controllable isolated islands. And via objective function that reflects information, power and control, the cut set of power system can be determined; when the fault is eliminated, the interconnection switch control strategy will restore the system to original state.

5. Cyber security
Cyber system and physical system have much more interaction than before, cyber security must be reconsidered. For now, three levels of security and stability standards are established for power system. Moreover, relay protection device, stability control device, and split device are applied to ensure safe and stable operation. Since these devices above need to cooperate with computer networks and communication system, hidden risks exist. For instance, the attackers could fake or tamper the message collected, thus cause mistakes in state estimation results, then incorrect operation appears; the attackers could acquire the authority of administrator by sniffing or password cracking, then tamper
the parameters of operation; also, via DoS attack, the cyber system could lose the control of physical system, then physical fault cannot be eliminated and go to further expansion.

The security protection principle of power CPS in our country should basically follow “safe partition, private network, crosswise separation, lengthways identification”. To be more specifically, the power enterprises should divide its server system into different safe regions using computers and networks, so the emphasis of system protection can be clear.

As Figure 1 shown, production control region can be divided into control region (safe region I, the core of security protection) and non-control region (safe region II); information management region can be flexibly divided due to different demand from power enterprises, such like production management region (safe region III) and message management (safe region IV). Besides, there are forward and backward physical separation existing between region I, II and region III, IV, added with firewall and encryption certification, the range that cyber risks could influence can be effectively limited, thus the safety of core region can be ensured.

However, the communication network presents the characteristics as “strong high-voltage side, weak low-voltage side”, and researches on cyber security mainly concern on generation, transmission and converter processes. Besides, still there are mistakes in daily manual operations: although the encryption scheme is mature, the hidden risks lie in producers and distributors of these encryption equipment cannot be fully eliminated. The same problem troubles servers in region I; the attack incidents against power system that are already known show that, even inside the private network that is separated from the other network, there is still chance for the cyber system to catch virus. Therefore, the traditional safety protection for power system, which mainly focus on physical separation and safe regions, cannot satisfy the demand from CPDS safety protection.

The main attacks against the network of power system are, DoS attack (e.g. SYN flood, smurf, and DDoS), virus (in 2010 nearly 1/5 nuclear power plants in Iran were affected by Stuxnet which entered from USB interface), information collection (e.g. sniffing, eavesdropping), attack against network (e.g. spoofing, replay and man-in-the-middle) and also false data injection, etc. Among them, false data injection attracts more attention, because it is hard to permeate into the rigor power dispatch center, while quite simple if the target is sensors. In [29], attackers could bypass the bad data detection and inject false data into the results of power system state estimation, and bring in errors at will. Kosut O et al. proposed a strategy against malicious data attack, and they utilized graph theory and polynomial time algorithm, deducted the minimum number of sensors that need to be attacked to make the system
unobservable [30][31]. There are other attack forms like load re-allocation, and this would change the cost of power system [32]. In the environment of power market, attacker can get economic benefits by injecting false data. The traditional method against false data injection in wireless network includes filtering in the midway and tracking back to source. Filtering in the midway filters false date passively, so the attacking nodes could launch sustained attack and avoid being discovered and separated. While tracking back to source needs plenty of packets from convergent nodes to take effect. Based on these, there are many study on the combination of two methods above to generate a new strategy against false data injection. Despite these ways discussed above, there are other methods, can be considered such as encryption and public opinion report.

The researches on cyber security is quite mature, and specific safety precautions can be applied into CPDS. However, these precautions cannot cover the physical aspect very well. Therefore, this paper presents research contents on cyber security of CPDS: first, classify hidden physical attack and its source, then, develop evaluation scheme for CPDS, and at last propose specific strategies for CPDS security defence. The technical route is shown in Figure 2.

(1) Effect of network attack

Analyse those information nodes and power nodes to find out weakness of them; the emphasis of this work is on the process where the data of power system is collected and transferred. Then find out all possibilities of attack that could be launched to break the weak nodes in CPDS. Based on power system analysis (transient analysis and steady-state analysis) and Bayesian network (conditional probability), the scheme of cross-space failure expansion can be established.

(2) Evaluation for cyber security

Evaluate the influence that communication system may bring on CPDS, and develop a scheme to evaluate weakness in both physical and cyber system: 1) Regard the random attacks as the input of system evaluation, and utilize Fuzzing test to evaluate possible risks according to cross-space failure expansion model of CPDS. 2) Build an attack-and-defence game model, and obtain the next node that the attacker would choose. Then the result of the game will be used as fundamental parameters of the cross-space failure expansion model, thus the evaluation of weakness in CPDS can be carried on.

Figure 2. Security framework for CPDS
(3) Protections for cyber security
Since the weak nodes have been found, aiming at false data injection and other attack against network channel, and armed with modern cyber security technology (including encryption, certification, integrity test, routing protocol), now the possibility to be attacked and the possibility the attack succeed can be effectively determined. And the system contains complete message or incomplete message need to be discussed by the use of game theory, and then formulate defensive strategies for CPDS. Or, use graph theory to describe all the proper message flow and control flow: view the whole message set or the operation instruction set as a graph (universal set), next take every piece of message or instruction as a directed edge, then a legal message flow or operation flow can be viewed as a directed route constructed of several directed edges (and this route may be a circle). Then, all the legal message flow and control flow are defined as known route in the graph; shall there appear any unknown route, it must mean illegal message or instruction.

6. Control strategy
A scientific and reasonable system, not only can ensure stable operation in normal situations, but also can strengthen the ability to handle bad situations like communication interference, channel failure, malicious attack and device break down. The stable operation relies on the instructions transferred among dispatching center, distributed sources and user loads. Therefore, CPDS will be a typical networked control system (NCS). NCS means a control system whose sensors, controllers and executions are located on different nodes, and they must communicate with each other via cyber network [33]. When the number of nodes and the sample rate increased, and there is communication congestion in the system, trans-mission delay and data loss will occur, and even cause instability of the system which may lead to break down. To solve this, here are some available ways: 1) reflect the effects of delay and data loss in the controlling model; 2) compensate for delay and loss, which means at any node in time scale, the control system should work out the present control instructions, and also several instructions for nodes in the future, and send them to execution at the same time.

At present, there are some problems about distributed control for CPDS: 1) the researches now only considered the distribution and complexion of the physical devices in distributed system, and mainly

![Framework](image)

**Figure 3.** Self-organizing control route for CPDS generation
focus on the controlling problem, but there are not enough attention paid to communication, computation, and the complex coupling of different levels. Thus, those control frameworks proposed cannot fully satisfy the demand of distribution controlling. 2) Although there are researches on coordinated control for distributed system, systemic solutions are still haven’t been proposed. For instance, when dealing with feeder current controlling problem, the coupling relationship between physical system and cyber system should be considered more carefully, and a mature algorithm for CPDS coordinated control should be established.

To study on coordinated control strategy for CPDS system based on open communication system, there are three steps, as shown in Figure 3:

The detailed introduction for each step is as follows:

(1) Framework

For the framework of CPDS control strategy, this paper proposed a solution: based on distributed control theory, graph theory and the property of the dynamic mathematic model in power system, build multi-time scale, local information shared distributed control model for different controlled subarea in the distributed system. Taken restraints in power system (e.g. power flow) into consideration, combined with other needs such as frequency, voltage and even the demand of game, the complete optimal coordinated mathematical model can be proposed.

(2) Coordinated distributed control

The core idea of coordinated distributed control is utilizing iteration algorithm while considering the interaction among units in CPDS at the same time.

Aiming at the coordinated distributed control, this paper presents some solutions as below: use singular perturbation and general passivation theory to reduce dimensions, thus the basic needs of coordinated control can be met; and the distributed average filter algorithm can be used to estimate all the real-time demand of the loads in CPDS.

(3) Dynamic property analysis

There are two solutions for dynamic property analysis of control strategy in CPDS. When the Lyapunov function is determined, and the convergence of the strategy is verified, then the corresponding parameter optimization method can be proposed; another solution is that, considering the incidents that could happen in actual operation such as delay and interruption, analyse the convergence and robustness of the algorithm.

(4) Topology integrity and its optimization

Several solutions are presents as below: use the convergence equivalent conditions of matrix sequence to find out the equivalent conditions of minimum logic communication topology; consider the demand of robustness of power system synthetically (e.g. the “N-1” rule) and formulate the optimized model for logical communication network; by the means of optimization theory and its computational methods, find out the optimized communication structure.

7. Conclusion

As the form of energy and electricity become diversified, the distributed system slowly turns into a cyber-physical system, which contains traditional power system, distributed renewable sources, communication devices and varies of loads, and with the cyber system and the physical system being deeply coupled. Based on a “863” project, this project introduced the key issues in developing CPDS, including integrated modelling method, planning method, cyber security and control strategy. Further, the research direction and recent development from home and abroad are introduced, and the existing problems are also pointed out. Last, specific research direction are presented in this paper.

The researches on the key issues of CPDS can promote the integration of the frontier information technology and the physical system, and this also contributes to allow the full potential of distributed devices, increase the absorption of distributed sources, strengthen the cyber security, and hence promote the level of comprehensive utilization, and provide important reference for the development of CPS theory and technology.
References
[1] Zhao J H, Wen F S, Xue Y S, et al. 2010 Cyber physical power systems: architecture, implementation techniques and challenges Automation of Electric Power Syst 34 1-7
[2] Zhao J H, Wen F S, Xue Y S, et al. 2011 Modeling analysis and control research framework of cyber physical power systems Automation of Electric Power Syst 35 1-8
[3] Dong Z Y, Zhao J H, Wen F S, et al. 2014 From smart grid to energy internet: basic concept and research framework Automation of Electric Power Syst 38 1-11
[4] Gao K L 2013 Research on security of cyber physical system China Information Security 2 86-87
[5] Tsikalakis A and Hatziargyriou N 2008 Centralized control for optimizing microgrids operation. IEEE Trans. Energy Conver 23 241-248
[6] Abdelaziz M A, Shaaban M F, Farag H E, et al. 2014 A multistage centralized control scheme for islanded microgrids with PEVs IEEE Trans. Sustainable Energy 5 927-937
[7] Dent C, Ochoa L and Harrison G 2010 Network distributed generation capacity analysis using OPF with voltage step constraints IEEE Trans. Power Syst. 25 296-304
[8] Divshali P H, Alimardani A, Hosseini S H, et al. 2012 Decentralized cooperative control strategy of microsources for stabilizing autonomous VSC-Based microgrids IEEE Trans. Power Syst. 27 1949-59
[9] Loh P C, Li D, Chai Y K, et al. 2012 Autonomous operation of hybrid microgrid with AC and DC subgrids IEEE Trans. Power Electro. 28 2214-23
[10] Guzman C, Cardenas A and Agbossou K 2014 Load sharing strategy for autonomous AC microgrids based on FPGA implementation of ADALINE&FLL IEEE Trans. Energy Conver. 29 663-672
[11] He L J, Li Y D and Harley R G 2013 Adaptive multi-mode power control of a direct-drive PM wind generation system in a microgrid IEEE J. Emerging & Selected Topics in Power Electro 1 217-225
[12] Abdelsalam A K, Massoud A M, Ahmed S, et al. 2011 High-performance adaptive perturb and observe MPPT technique for photovoltaic-based microgrids IEEE Trans. Power Electro. 26 1010-21
[13] Xin H H, Qu Z H, Seuss J, et al. 2011 A self-organizing strategy for power flow control of photovoltaic generators in a distribution network IEEE Trans. Power Syst. 26 1462-73
[14] Xin H H, Zhang M D, Seuss J, et al. 2013 A real-time power allocation algorithm and its communication optimization for geographically dispersed energy storage systems IEEE Trans. Power Syst. 28 4732-41
[15] DIllic M, Xie L, AKhan U, et al. 2010 Modeling of future cyber-physical energy systems for distributed sensing and control IEEE Trans. Systems, Man, and Cybernetics-Part A: Systems and Humans 40 825-838
[16] Zeng Z Y and Liu D 2013 Study on cyber-physical system modeling on coordinated control of photovoltaic generation and battery energy storage system Power Syst Tech 37 1506-13
[17] Zhao J H, Wen F S, Xue Y S, et al. 2010 Cloud computing: implementing an essential computing platform for future power systems Automation of Electric Power Syst 34 1-8
[18] Zhuang W and Mu D H 2012 Study on cyber-physical relaying protection system of intelligent distribution network Power Syst Protection & Control 40 113-118
[19] Nutaro J, Kuruganti P T, Protopopescu V, et al. 2011 The split system approach to managing time in simulations of hybrid systems having continuous and discrete event components Simulation 87 1-18
[20] Hua L, Sambamoorthy S, Shukla S, et al. 2011 Power system and communicationn network co-simulation for smart grid applications IEEE PES Conference on Innovative Smart Grid Technologies 1-6
[21] Nutaro J 2011 Designing power system simulators for the smart grid: combining controls, communications, and electro-mechanical dynamics Proceedings of IEEE Power and Energy
Society General Meeting 5 1-5

[22] Godfrey T, Mullen S, Dugan R C, et al. 2010 Modeling smart grid applications with co-simulation IEEE International Conference on Smart Grid Communications 291-296

[23] Arefifar S A, Mohamed Y A and El-Fouly T 2012 Supply-adequacy-based optimal construction of microgrids in smart distribution systems IEEE Trans. Smart Grid 3 1491-1502

[24] Atwa Y M, El-Saadany E F, Salama M and Seethapathy R 2010 Optimal renewable resources mix for distribution system energy loss minimization IEEE Trans. Power System 25 360-370

[25] Kleinberg M R, Miu K, Segal N, Lehmann H and Figura T R 2014 A partitioning method for distributed capacitor control of electric power distribution systems IEEE Trans. Power System 29 637-644

[26] Mehrjerdi H, Lefebvre S, Saad M and Asber D 2013 A decentralized control of partitioned power networks for voltage regulation and prevention against disturbance propagation IEEE Trans. Power System 28 1461-69

[27] Arefifar S A, Mohamed Y and El-Fouly T 2015 Optimized multiple microgrid-based clustering of active distribution systems considering communication and control requirements IEEE Trans. Industrial Electro 62 711-722

[28] Anderson P and LeReverend B K 1996 Industry experience with special protection schemes IEEE Trans. Power System 11 1166-79

[29] Liu Y, Ning P, Reiter M K 2009 False data injection attacks against state estimation in electric power grids Proceedings of the 16th ACM conference on Computer and communications security 21-32

[30] Kosut O, Jia L, Thomas R J, et al. 2010 Malicious data attacks on smart grid state estimation: attack strategies and countermeasures IEEE International Conference on Smart Grid Communications 220-225

[31] Kosut O, Jia L, Thomas R J, et al. 2011 Malicious data attacks on the smart grid IEEE Trans. Smart Grid 2 645-658

[32] Yuan Y, Li Z and Ren K 2011 Modeling load redistribution attacks in power systems IEEE Trans. Smart Grid 2 382-390

[33] Xue B, Li N, Li S, et al. 2010 Robust model predictive control for networked control systems with quantization IET Control Theory and Applications 4 2896-2906