FORMAL MODELING AND VERIFICATION METHOD OF POWER GRID CYBER PHYSICAL SYSTEM BASED ON COUPLING OF INFORMATION AND ENERGY FLOW

Boya QIN
Shanghai Jiao Tong University – China
qinboya@sjtu.edu.cn

Dong LIU
Shanghai Jiao Tong University – China
dongliu@sjtu.edu.cn

ABSTRACT

This paper focuses on the coupling mechanism between power system information flow and energy flow. Based on the analysis of power grid cyber physical system (GCPS), a formal modeling and verification method is proposed. By decomposing GCPS into power and load subsystems, the behavior and state modes are expressed mathematically, and network structure diagrams are constructed. By analyzing the logical and functional connection between information and physical system objects, we proposed the networking rules to construct the GCPS architecture. Verification tool SPIN is applied in formal verification for key features of GCPS, ensuing the logical correctness of modelling topology. The IEEE 9-Bus system is used as a test case in the simulation of the proposed formal modeling and verification methods.

INTRODUCTION

The Cyber-physical System (CPS) is generally regarded as the coupling mechanism of primary and secondary systems in the power grid. As one of the most typical application scenarios, the smart grid is highly integrated with advanced measurement systems, intelligent electronic devices and flexible control technologies. Through the deep integration and real-time interaction between cyber and physical space, a new solution is provided for the safe operation of power grid.

In the situation that power systems are increasingly dependent on information feedback and decision-making, anomalies in information flow may cause chain reactions in the physical world [1-3]. It is urgent and necessary to analyse the deep correlation between information flow and physical flow as well as the fusion mechanism between information system and physical system.

Key technologies in the field of Grid Cyber-Physical System (GCPS) include: cyber-physical coupling analysis, system modelling, system control and formal verification [4]. The construction of fusion model for information system and physical system is regarded as the basic scientific problem of GCPS and the basis of other related application researches, as it portrays the information-physical interactions in the power system. The generator and load dynamic models are established considering the coupling of the information system and the physical system [5]. The modelling method of information network and power network based on dynamic system and graph theory is proposed in [6]. The impact of network attack on physical system is analysed, using improved IEEE-13 node system as the case. Based on the discussion of GCPS fusion architecture, static and dynamic analysis models are established in [7], providing the analysis of grid reliability and safety. Considering the spatial and temporal heterogeneity of information and physical systems, an energy Internet model based on cyber-physical fusion mechanism is proposed in [8]. Complex network theory is used for the modelling of GCPS in [9-10], analysing the application of actual power outage event. Based on the CPS modelling framework of heterogeneous entities, a collaborative modelling method considering the structure and dynamic behaviour of CPS systems is proposed in [11]. The complexity of power system equipment and the correlation between information flow and energy flow are the two main challenges for GCPS modeling. The interactive topology of the cyber-physical interaction process and the information-energy flow correlation are the two coupled system operational elements. The existing GCPS research fails to deeply analyse the cyber-physical interaction characteristics of GCPS operation. It is difficult to completely describe the essential characteristics of GCPS and the dynamic interaction between discrete states and continuous processes. There exists an overall lack of a complete framework and research method.

This paper focuses on the coupling mechanism of power system information flow and energy flow. Based on the logical structure of grid cyber-physical system (GCPS), a formal modeling and verification method is proposed. The set theory describes the cyber-physical interaction features of GCPS model and its subsystems, providing a unified mathematical description for information and physical systems with different structures. By analyzing the logical and functional connection between information objects and physical objects, GCPS is decomposed into power subsystem and load subsystem, expressing information-physical interaction formal characteristics. The network structure diagram of subsystem achieves the coupling and interconnection of GCPS subsystems, building a complete GCPS architecture. Verification tools such as SPIN are used to formally define and verify the key features of GCPS topology, ensuring logical correctness of the theory. The IEEE 9-Bus system is used as a test case to analyze the proposed modeling and verification methods.

ANALYSIS OF GCPS CHARACTERISTICS

A typical feature of CPS is the deep integration of computation, communication, and control. Autonomous adaptation to changes in the physical environment can be achieved through sensing and control functions. The GCPS characteristics are reflected in the tight coupling and strong correlation between primary system and secondary system [11]: Energy flow is transmitted to the load through power plant, substation, transmission line, etc. Secondary system collects the state data of primary system through information equipment. System control, protection and

monitoring are realized through post-processing and analysis.

The cyber-physical coupling architecture of GCPS is constructed as follows:

1) Physical side → Information side: The information system obtains various types of numerical information and topology data of the primary system through sensors, and transmits them to the control center of secondary system with communication network.

2) Information side → Physical side: The control center generates control commands according to the multi-level processed status data. The controller acts on the physical system by means of changing operating state or operating parameters of equipment to adjust energy flow distribution of the power grid.

GCPS is a large nonlinear system composed of many interconnecting subsystems. To analyze the correlation between signal and energy in the system, basic units with similar information-physical coupling characteristics is defined as GCPS subsystems. In addition to the physical objects used to implement specific functions, there also exists a corresponding set of sensors and controllers in the GCPS subsystem to achieve data upload, command release, and interaction tasks with other subsystems.

GCPS MODEL DESCRIPTION

According to the idea of system decomposition, the GCPS model is established by means of "model + rules". The macroscopic mathematical description of the whole GCPS is carried out using set theory. The basic characteristics of the GCPS subsystem can be expressed from three aspects: network structure, behavior pattern and state mode. According to the subsystem interconnection rules, the logical and functional connections of the GCPS subsystem are realized, and the complete GCPS macro-micro architecture is constructed.

Mathematical model for GCPS and subsystems

The system is a unity formed by several interacting parts. The general formalization of the GCPS system according to set theory is described as defining a relationship (subset) S on the non-empty set $\times\{V_i: i \in I\}$.

$$S \subset \times\{V_i: i \in I\}$$

$\times$ is the direct product of each set in $\{\}$; I is the index set; V_i is the component object of the system.

Thus, an effective solution is proposed for simultaneously expressing discrete structures and continuous systems. GCPS is defined as a relationship between finite sets by merging the objects in the GCPS system into several sets according to their properties and interactions:

$$Sys \subset CC \times S \times C \times O$$

Sys represents the system. CC represents the control center. S is the sensor set. C is the controller set, and O is the physical device object set. The sets are interconnected through the physical distribution network and the cyber communication network. If $cc \in CC, s \in S, c \in C, o \in O$, $(cc, s, c, o) \in Sys$.

According to the logical structure of GCPS, the power subsystem and the load subsystem are represented by $Power = (cc_P, s_P, c_P, o_P)$ and $Load = (cc_L, s_L, c_L, o_L)$. The network structure diagram is constructed as shown in Fig.1. The network structure diagram clearly expresses the connection between the information object and the physical object in the GCPS subsystem, providing a unified and clear expression for the complex relationships within the system.

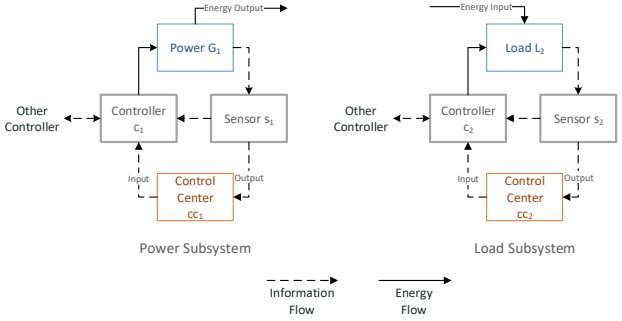

Fig.1 Structure of Power Subsystem and Load Subsystem

The behavioral pattern describes the relationship between the input-output of the system. According to the signal transmission and energy flow between the information and physical objects in the power system, the behavior of the subsystem is described by the quaternary Bhv:

$$Bhv = \{(cc_i, s_i), (cc_i, c_i), (o_i, o_j), (c_i, c_j)\}$$

(cc_i, s_i) is sensor s_i sending physical device information output to control center cc_i ; (cc_i, c_i) is controller c_i accepting the control commands from control center cc_i; (o_i, o_j) is the energy transfer between current physical object o_i and another physical object o_j ; (c_i, c_j) is the information exchange between controller c_i and another local controller c_j in the subsystem.

The state mode describes the physical state of nodes in the system. The state data of each physical node in the power system is determined by the dynamic system model and the function of network element. In continuous time, the node state Sys evolves according to deterministic rules:

$$\dot{Sys} = f(Sys, Signal)$$

$\dot{Sys}$ is the time derivative of Sys, describing the change of system state; $p = \{p_1, p_2, \ldots, p_m\}$ is the set of factors affecting the state change, varies with the type of physical node. Typically, p includes control signals, switching states, etc.

GCPS subsystem interconnection rules

In order to couple a large number of subsystems with auxiliary equipment to form a complete GCPS architecture, the subsystem connection rules of the GCPS vertical aggregation and horizontal interconnection are established. According to the logical connection between the electrical connection of the physical system and the information system, the coupling function and logic of GCPS network architecture are established step by step.

Note that cc, s, c in the subsystem $(cc, s, c, o) \in S$ are logical nodes, and o is a functional node. The specific

description of the interconnection rules is as follows:
1) Horizontal interconnection: The logical nodes cc, s, c together with the function node o realize data acquisition, monitoring and control through signal transmission. The logical nodes are associated according to the required feature functions. The electrical connections are realized between functional nodes.
2) Vertical aggregation: According to the role and status of GCPS subsystems in the entire power system, regional interconnection is realized. Auxiliary equipment is integrated into regional GCPS interconnection to construct a complete GCPS network architecture.
Traditional power systems use electrical or geographic wiring diagrams to describe the electrical constraints of the physical system. On the basis of not changing the wiring of physical system, the GCPS network structure diagram integrates information devices such as control centers, sensors, controllers, etc., and interconnects all devices according to subsystem interconnection rules, which can reflect information flow, energy flow and information-physical coupling relationship at the same time.

FORMAL METHODS FOR GCPS

Formal modeling and verification process

The application of the formal method in GCPS is embodied in the modeling and verification of the key attributes and features contained in the process of merging the physical system and the information system using mathematical methods and logical processes. In order to combine the realization of engineering technology with universal mathematical theory, a more specific and practical verification theory is proposed, and used as the tool to guide related research and application in engineering field.
The implementation of a formal method is generally composed of three parts: a framework for system modeling, a specification language for describing the characteristics for verification, and a verification method determining whether the system description satisfies the specification. In the formal modeling process, the system description is a set of logical formulas Γ, and the specification Φ is another formula. The verification method is an attempt to find the proof of $\Gamma \vdash \Phi$, that is, the requirements of the specification are satisfied for all models. The specification may describe a single feature of the system, or it may describe its full nature. The verification focuses on certain specific attributes such as security or reliability, and is mostly a verification of core attributes.
There are two main methods for formal verification: theorem proving and model checking.
Theorem proving is a proof process that uses the inference rules to gradually derive desired characteristics from the axiom system. It uses structured derivation to process systems with infinite state spaces.
Model checking uses state space search to automatically verify whether a finite state system satisfies specifications. When the property is not satisfied, the search aborts and returns a counterexample. The verification result gives feedback on system design and provides direction for the correction. In this paper, the key attributes of GCPS are verified by software detection tool SPIN, aiming at the automation of model detection. The Non-Deterministic Finite Automata (NDFA) provided by SPIN's modeling language Promela makes it easy to model the operational uncertainty of the system.

Formal verification of GCPS

Using formal theory to model and verify GCPS involves two procedures:
1) Accurately describe the features of topology analysis using well-defined mathematical definitions;
2) Based on the established formal specifications, analyze and prove relevant attributes.
Direct extraction of the topology analysis logic will cause explosion of state space in the verification process. It is necessary to extract the key attributes during the formal verification process.
The electrical device is selected as the minimal description unit. For any electrical device o, the topology analysis state is defined as reachable and unreachable, represented by o and ¬o.
Topology analysis is a process of traversing iterative model analysis. "Device o is reachable in kth topological analysis but unreachable in (k+1)th topological analysis" is regarded as a basic attribute, which is necessary to be clearly expressed.
By adding integer [N] to state quantities, the state of the device during the iteration is specified.
o[k]: After the kth topology analysis process, the state of device o is reachable;
¬o[k + 1]: After the (k+1)th topology analysis process, the state of device o is unreachable.
The logical formula Γ is the key of formal modeling. The core logic describing the conversion of state quantities in power systems is the basis for application of formal theory. The key attributes defined include:
a) Observability: Each physical device can be connected to the control center via an upstream communication line through sensors, that is, the device can be measured.
For any device o, note that:
o: Device o is observable;
¬o: Device o is unobservable.
The child node set of the parent node of o is represented as $o_S^P\{o_S^P(1), \ldots, o_S^P(m), o\}$.
After a bottom-up traversal searching, o is denoted as o[1].
After a following top-down traversal searching, o[1] is updated to o[2].
After k traversal processes, o is converted to o[k].
According to the definition of distribution network states, the state transition logic theorem applicable for formal reasoning is expressed as:
Rule-A: If all child nodes of node o are observable, node o is observable, expressed as:

$$\forall x \cdot o(x) \longmapsto [] \, o$$

Rule-B: o is an observable point regardless of the way makes it observable:

$$o \vee o[1] \vee \ldots \vee o[k] \longmapsto []o$$

Rule-C: o is an observable point regardless of the operation performed on o:

$$[]o \longmapsto o \wedge o[1] \wedge \ldots \wedge o[k]$$

Rule-D: The parent node of o is observable, and there are no unobservable points in the child node set of the parent node except o, then o can be observed:

$$[]o \longmapsto o \wedge o[1] \wedge \ldots \wedge o[k]$$

Rule-E: If the state of a device changed from unobservable to observable, there are two possibilities: all child nodes become observable, or the root node is observable and all other child nodes except the device itself are observable.

$$\left(\neg o[k] \wedge o_S(1) \wedge \ldots \wedge o_S(n)\right) \vee (\neg o[k] \wedge o^P[k] \wedge o_S^P(1) \wedge \ldots \wedge o_S^P(i)) \longmapsto o[k+1]$$

b) Controllability: Each physical device can be controlled by the control center via a downlink communication link through controllers, that is, the device can be controlled.

$$\forall i, o_i \in O, \longmapsto \exists c_i \in C, c_i \in o^P \wedge (c_i, o_i)$$

c) Open-loop Operation Feature: There exists the only one root node.

For any device o, define its parent node as o^P. A set with N child nodes of o can be characterized as: $o_S(n) = \{o_S(1), o_S(2), \ldots, o_S(n)\}$

According to the operation characteristics of distribution network, the open-loop operation features are defined as:

Axiom-A: Let P be the root node of a radial network, then $P^P = \emptyset$.

The power system is an industrial application system and must be finite in nature:

Axiom-B: For any grid, there must be a device o, such that $o_S = \emptyset$.

d) Regional Closed-loop Feature: For the regional structure of $\{s_i, c_i, o_i\}$, there exists a regional closed loop of $\{(c_i, o_i), (o_i, s_i), (s_i, c_i)\}$. Under the circumstance of regional network, physical devices are controllable, observable, and information flow channels are connected. The formal expression is as follows:

$$\forall i, s_i \in S, c_i \in C, o_i \in O \longmapsto \exists\{(c_i, o_i), (o_i, s_i), (s_i, c_i)\}$$

CASE ANALYSIS

The IEEE 9-Bus system is used as the test case in the simulation of the proposed GCPS formal modeling and verification method. The GCPS model and interconnection structure are constructed, and simulation is carried out in following steps. The system includes generator nodes G_1, G_2, G_3, load nodes L_1, L_2, L_3, transformers T_1, T_2, T_3, and associated buses $B_1 - B_9$.

With the transformer and busbar as the auxiliary objects, the IEEE 9-Bus GCPS is described as Sys $\subset$ CC $\times$ S $\times$ C $\times$ O. O $= \{g_1, g_2, g_3, l_1, l_2, l_3\}$ represents the 3 generators and 3 loads respectively. CC $= \{cc\}$ is the control center. S $= \{s_1, s_2, \ldots, s_6\}$ is the set of sensors. C $= \{c_1, c_2, \ldots, c_6\}$ is the set of controllers.

Elements are grouped and labeled with physical and logical connections to establish power and load subsystem diagrams. All devices in the subsystem are interconnected to form a GCPS architecture, as shown in Fig.2 and Fig.3. The electrical topology diagram and subsystem structure diagram describes the coupling and logical connection between the information flow and energy flow, providing a concise expression of the interconnection between information devices and physical devices in GCPS. The GCPS architecture diagram effectively integrates the information network with the physical network, building the foundation for simulation and analysis of GCPS.

The steps for the formal verification of the constructed IEEE 9-Bus system GCPS architecture are as follows:

a) Describe the subsystems associated with attributes to be verified using the Promela language identified by the SPIN verification tool;

b) Express the features as Linear Temporal Logic (LTL);

c) Perform verification with the verification tool SPIN.

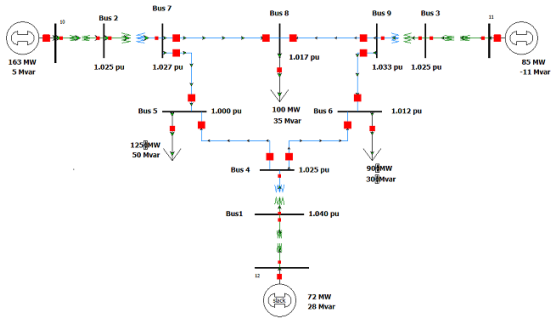

Fig.2 IEEE 9-Bus System

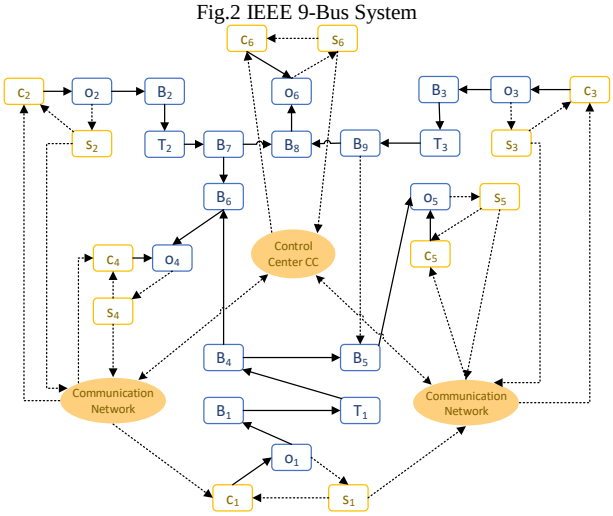

Fig.3 Topological Architecture of IEEE 9-Bus GCPS

In order to ensure the completeness of verification state space, the measurement data of each node and the nodes for state transition are randomly generated. The criterion of verification is that the observable area generated by top-down traversal process is larger than or equal to the observable area of random traversal process.

The verification interface is shown in Fig 4.

The box on the left side of Fig.4 shows the Promela input code describing the model. The LTL formula input box on the upper right corner is the logic that needs to be verified.

The box on the right shows the verification results of SPIN, as shown in Fig.5.

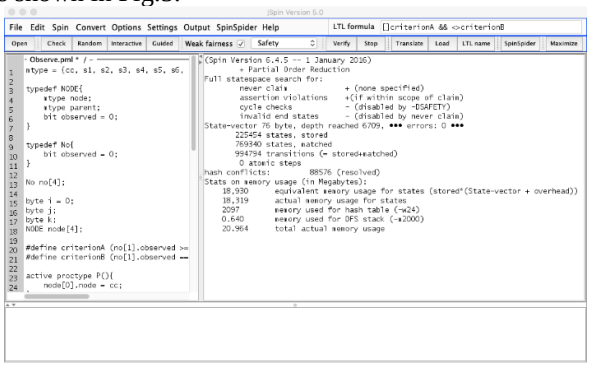

Fig.4 Observability Verification Interface

```
(Spin Version 6.4.5 -- 1 January 2016)
        + Partial Order Reduction
Full statespace search for:
        never claim             + (none specified)
        assertion violations    +(if within scope of claim)
        cycle checks            - (disabled by -DSAFETY)
        invalid end states      - (disabled by never claim)
State-vector 76 byte, depth reached 6709, *** errors: 0 ***
         225454 states, stored
         769340 states, matched
         994794 transitions (= stored+matched)
          0 atomic steps
hash conflicts:         0 (resolved)
Stats on memory usage (in Megabytes):
    18,930  equivalent memory usage for states (stored*(State-vector + overhead))
    18,319  actual memory usage for states
    2097    memory used for hash table (-w24)
    0.640   memory used for DFS stack (-m2000)
    20.964  total actual memory usage
```

Fig.5 Observability Formal Verification Results

Using the model verification tool, the LTL formula is used to describe properties that the system must satisfy. It can be applied to the distributed systems as an effective error detection method. In the trend of increasingly closer information flow-physical flow coupling, anomalies in the information system is very likely to cause chain reactions in the physical system. Analysing and verifying the grid information flow-physical flow coupling model through formal methods are of great significance to ensure the safety and stability of power system operation.

CONCLUSION

By analysing the interaction between grid information flow and energy flow, a GCPS modelling method based on set theory and topology analysis is proposed. We put forward the networking rules of vertically aggregating by function and horizontally connecting through logic to construct a complete GCPS network architecture. The modelling method comprehensively analysed the cyber-physical interaction mechanism of GCPS, providing a unified mathematical expression for heterogeneous information and physical systems. It supports the research on co-simulation, calculation and application of GCPS. The formal verification method can verify the logical correctness of the topology architecture, ensuring the security and reliability of the system.

Acknowledgments

Project Supported by the National Key Research and Development Program of China (Basic Research Class 2017YFB0903000) and National Natural Science Foundation of China (51677116).

REFERENCES

[1] S.Sridhar, A.Hahn, M.Govindarasu, 2012, "Cyber-Physical System Security for the Electric Power Grid", Proceedings of the IEEE, 2012, 100(1): 210-224.

[2] R.Liu, C.Vellaithurai, S.S.Biswas, et al, 2015, "Analyzing the cyber-physical impact of cyber events on the power grid", IEEE Transactions on Smart Grid, 2015, 6(5): 2444-2453.

[3] Y.Tang, Q.Wang, M.Ni, et al, 2016, "Analysis of Cyber Attacks in Cyber-physical Power System", Automation of Electric Power Systems,2016, 40(17): 59-69.

[4] D.Liu, W.Sheng, Y.Wang, 2015, "Key technologies and trends of cyber-physical system for power grid", Proceedings of the CSEE 35.14 (2015): 3522-3531.

[5] M.D.Ilic, L.Xie, U.A.Khan, et al, 2010, "Modeling of future cyber-physical energy systems for distributed sensing and control", IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2010, 40(4): 825-838.

[6] D.Kundur, X.Feng, S.Mashayekh, et al, 2011, "Towards modelling the impact of cyber attacks on a smart grid", International Journal of Security and Networks, 2011, 6(1): 2-13.

[7] J.Zhao, F.Wen, Y.Xue, et al, 2011, "Modeling analysis and control research framework of cyber physical power systems", Automation of Electric Power Systems, 2011, 35(16): 1-8.

[8] B.Wang, Q.Sun, D.Ma, et al, 2011, "A Cyber Physical Model of the Energy Internet Based on Multiple Time Scales", Automation of Electric Power Systems, 2011, 35(10): 104-107.

[9] S.V.Buldyrev, R.Parshani, G.Paul, et al, 2010, "Catastrophic cascade of failures in interdependent networks", Nature, 2010, 464(7291): 1025.

[10] J.Gao, S.V.Buldyrev, H.E.Stanley, et al, 2012, "Networks formed from interdependent networks", Nature physics, 2012, 8(1): 40.

[11] Q.Guo, S.Xin, H.Sun, et al, 2016, "Power system cyber-physical modelling and security assessment: motivation and ideas", Proceedings of the CSEE, 2016, 36(6): 1481-1489.

[12] J.Yan, J.Xu, M.Ni, et al, 2016, "Impact of communication system interruption on power system wide area protection and control system", Automation of Electric Power Systems, 2016, 40(5): 17-24.

[13] R.Akella, H.Tang, B.M.McMillin, 2010, "Analysis of information flow security in cyber–physical systems", International Journal of Critical Infrastructure Protection, 2010, 3(3-4): 157-173.

[14] Y.Mo, T.H.J.Kim, K.Brancik, et al, 2012, "Cyber–physical security of a smart grid infrastructure", Proceedings of the IEEE, 2012, 100(1): 195-209.