Cyber-Physical System Security and Protection Strategies for the Smart Substation

Sicheng Zeng[1,2,a], Yimin Qiu[1,b], Yongyi Shi[3,c]

[1] Globe Energy Interconnection Research Institute, Beijing 102209, China

[2] China Electric Power Research Institute, Beijing, 100192, China

[3] Zhejiang Electric Power Company, Hangzhou, 310007, China

[a]orgazeng@163.com, [b]qiuym2000@163.com, [c]shiyy@zj.sgcc.com.cn

Keywords: Smart substation, Cyber attack, Cyber-physical system, Secondary intelligent unit, Hardware reliability.

Abstract. As an important part of the smart grid, smart substation is the key operating parameters collection point and control execution point, thus its safe and stable operation is one of the fundamental bases of ensuring the grid continues to provide a reliable energy resource for the development of the national economy. Using more and more new information and communication technologies, which greatly improve the operating efficiency and grid intelligence, smart substation is a typical cyber-physical system (CPS), facing various of security risks. Different from the traditional view point of cyber security and power system safety, this paper analysis the security threats substation faced with on the perspective of CPS three layer architecture, which consists of perception-execution layer, transport layer and application-control layer, and puts forward the corresponding protection strategies.

Introduction

Smart substation is a key point to connect the generation, transmission, transformation, distribution, consumption and dispatch of smart grid [1]. It serves not only as a data resource of electrical power automation, but also as an executive termination of the control system. Smart substation is a typical CPS, whose security includes both virtual network security and physical entity reliability. If the data transmitted in the communication network can be modified artificially, attacker can order malicious instructions to the power grid, which might cause power grid fault and blackout of some area. When the physical components of information and communication infrastructure in substation go wrong, the information might transmitted irregular, making the grid out of control, bringing extremely dangerous risks to the safe and stable operation of the grid. Therefore, it is necessary to conduct research on the CPS security and protection strategies for smart substation.

The traditional research of substation's security focus on either cyber security or power system safety, which cannot makes a complete comprehension of the whole problem. This paper proposes a CPS hierarchical architecture of smart substation, then it analysis the security risks smart substation faced with and corresponding protection strategies in four parts, which are perception-execution layer, transport layer, application-control layer and external network.

CPS Hierarchical Architecture of Smart Substation

CPS can be divided into three layer structure, which are perception-execution layer, transport layer, application-control layer [2], as depicted in Figure 1. The perception-execution layer is the integration of physical devices mainly consist of sensors and actuators. The transport layer is the support for real-time communication and Information interaction. The application-control layer uses data to make control instruction based on control algorithm.

The perception-execution layer of smart substation mainly includes the merging units (MUs) and intelligent electronic devices (IEDs). The major function of MU is to receive the signal of three phase voltage and current, and receive the switch signal of primary equipment, then export them to the secondary protection unit in prescribed data format. The IED is mainly used for collecting status of

primary equipment, then use GOOSE signal to upload these to the equipment in the bay layer, meanwhile receiving the control command from the protection equipment to realize real-time control for the primary equipment [3].

The industrial Ethernet switches (IES) and optical fibers are the most important hardware devices of the transport layer in substation, whose reliability is prerequisite of the whole information and communication system's security. Different from the traditional substation, smart substation substitutes optical fibers for a great number of electric cables used in the past.

The application-control layer of smart substation is the heart of CPS, which consists of desktop applications and operation systems. The desktop applications used in substation include protection system, monitoring system, fault recorder, network analyzer, and so on. The operation system is either Windows or UNIX.

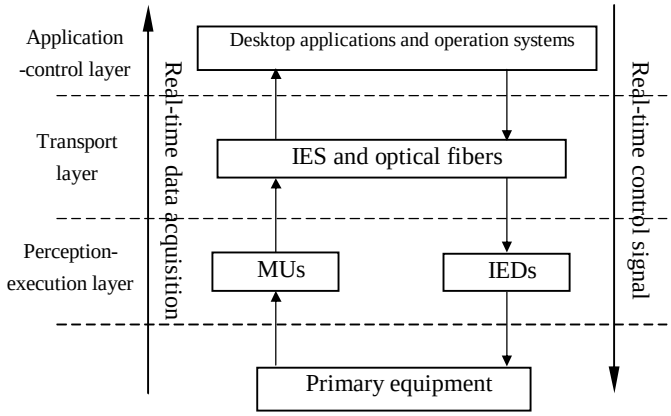

Figure 1. The CPS three layer architecture of smart substation.

CPS Security Risks Of Smart Substation

Risks of Perception-Execution Layer

Hardware and Software Reliability. Since 2009, the smart substation has been promoted vigorously and researched considerably in China, but it is still in the developing stage. Not having been operated for a long time in power system, the hardware reliability of MU is far from perfect. For instance, error cannot be ignored when MU measures frequency and harmonic waves, and the decay time constant is out of acceptable range in the transient performance test. The defects exist in the design of software programs, such as the unconformity between configuration and standard, and the test fail of analog quantity, communication error-tolerant rate, and network traffic, which bring some accident to the safety production. For example, because of the configuration of MU's software having been set wrong, the primary transformer and some lines tripped by mistake in a 500kV substation when a failure happened outside the protection area of this substation, leading the voltage of north 220kV bus lose stability, which brings significant impact to the local grid.

Implementation of Standards. The comprehensions and executions to IEC 61850 standard of different secondary intelligent unit manufacturers are not the same. Therefore, the corresponding test standards are not clear, and the performance tests and the regulatory measures are not enough, making the qualities of products vary greatly, stability and reliability cannot be guaranteed effectively. Moreover, the product models which are not pass the grid access test have been used in the design and supplies purchasing sections.

Environment. The secondary loops of substation, which are sensitive to electromagnetic interference (EMI) signals, are in the area of strong electromagnetic field. Reference [4] analyzed the applicability of current domestic standard for electro-magnetic compatibility immunity test, and pointed out that such standard is an insufficient evaluation of the intelligent unit in the local control cabinet. So far, the MUs and IEDs are basically installed in the intelligent terminal cabinet outdoors, hence the effect of the ambient temperature cannot be ignored. A south province has detected the

temperature inside the cabinet of smart substations which are just brought into operation in 2014, and the highest temperature turns out to be 54 degrees Celsius, which might cause the defect rate of secondary intelligence unit increase.

Risks of Transport Layer

IES. The major defects and failures of IES are represented by Table 1.

Table 1. Security Threats of IES

Security threats	Detailed description
Power failure	The switch does not function normally, data cannot be uploaded and downloaded correctly.
Port fault	Port data cannot exchange correctly, communication is interrupted, packets are lost or unable to be sent.
Network congestion	The message is blocked when sending large amounts of information in a short time, resulting in system's misjudgment of station conditions.
High network delay	Actuator cannot receive the control command immediately, resulting in abnormal operation of protection.
Poor hardware performance	The switch cannot suppress the occurrence of network storm effectively, which may lead to network paralysis when seriously.

Optical Fibers. The features of optical fibers in smart substation are wide applicable areas, large amounts, complex loops, high technological requirements, and directly affecting the reliable operation of information networks. All kinds of risks can make the information and communication in uncontrollable state, affecting the safe and stable operation of the substation.

Risks of Application-Control Layer

Risks of Desktop Applications. The desktop applications, such as protection system, monitoring system, fault recorder, and network analyzer, use various software extensively. Defect of equipment manufacturers' development software is one of the most significant security vulnerabilities, such as architecture design flaws, coding vulnerabilities, inadequate safety testing, lacking of quality control, and so on. These lead the concealed defects and vulnerabilities to exist in the system software and network of substation, which are the attack's preferred target.

Risks of Operation Systems. The current operation system in substation is either Windows or UNIX, whichever may has "back door" that development company leaves intentionally or unintentionally, which can be used by criminals or hostile elements through network to intrude smart substation's host. If such intrusion happens in wartime, the enemy would destroy a critical equipment in substation, bringing power blackouts to a wide area, and threatening the life and property safety of local residents if seriously.

Risks of External Network. In China, State Electricity Regulatory Commission's formal documents, "The Security Protection Scheme for Substation's Secondary System", requires clearly that electric power enterprise must conduct effective security isolation between production control region networks and management information region networks. However, the power system is not a closed "isolated" system, and the whole information network of power system cannot isolate these two region completely. As long as the information of smart substation has to be transmitted through the network telecontrol channel, there exist several threats as follows:

Intercepting Transmitted Information. This means the illegal access to information transmitted between the substation and dispatch system. In the view of security, intercepting information will not affect the transmission of information, but it will expose the deficiencies in the substation network systems, which tends to be the prelude of hackers' intrusion [5].

Tampering Transmitted Packets. After the data packets on the network have been intercepted by hackers during transmission, they would be modificated maliciously and then sent to the other recipients of system, undermining the authenticity of the information data processed by the recipient and threatening the safe operation of the grid. For instance, tampering with the substation's

measurement data sent to the dispatch network will lead the control center to make wrong decisions, affecting the stability of power transmission. Tampering with the control system's command sent to the remote substations or modificating parameter values might lead the circuit breakers, disconnectors and other physical devices to malfunction or refuse to move in substation, causing grid to disintegration if seriously.

Interrupting Information Communication. This is realized by forcing the communication between substation network and dispatch system to break off, making the primary and secondary physical devices' real-time operating conditions unknown to the main dispatch station, so that the control command can not be executed promptly and correctly.

Malicious Programs. Viruses, such as Trojans, computer worms, and logic bombs, can be implanted into the substation's information network systems. Once the virus outbreak, it will bring serious impact to the correctness, timeliness and reliability of the substation's information network systems, making the primary and secondary physical device out of control, leading to serious consequence. Nowadays, the viruses have evolved into something sophisticated and advanced, such as the Stuxnet virus first discovered in 2010, which can cause harm in a hidden way [6,7].

CPS Protection Strategies for Smart Substation

Protection Strategies for Perception-Execution Layer

Testing. China National Testing Center for Relay Protection and Automation Equipment and The Quality Inspection & Test Center for Automation Equipment of Electric Power System carried out inspection works on MUs and IEDs of 220kV and above voltage level substation, and published a qualified products list of analog input MUs and IEDs which passed the professional test. The secondary intelligent unit which about to be operated in power system must pass the access quality inspection, and the one which has been operated yet out of the qualified products' list must be replaced in time [8]. Particularly, the qualified products' programs are sometimes modified after testing, which need to be test again.

The current situation in China is that the factory testing of MUs before they leave the factory expose and fix only a part of their conventional problems, hence the large numbers of MUs' performance needs large-scale access test through professional performance test tools [9].

Environment Improvement. Optimizing the way to install MUs can improve the overall anti-EMI capability of the apparatus. It is recommended that manufacturers should increase electromagnetic compatibility test level of the secondary intelligent device appropriately, and that increase the current domestic electromagnetic compatibility test standard level to megahertz band [13]. Various ways can reduce the temperature inside the IED effectively, such as installing thermal insulation cabinet, air conditioning, heat exchangers and so on.

Protection Strategies for Transport Layer. IES is an important core equipment of the smart substation cyber-physical system, for which IEC 61850-3 made very strict requirements. Requirements for the use of smart substation switches are concluded as follows:

Functional Requirements. It should ensure service quality and support fast store and forward mode, which make sure that the important network's GOOSE / SV packets transmitted in real-time. Meanwhile, it should support VLAN isolation and redundant network topology and rapid spanning tree protocol.

Environment Requirements. It can ensure the normal operation of IES that meeting the requirements of insulation, temperature, working power, and low pressure.

For optical fibers which be used largely in the substation, regularizing the install process makes significant contribution to their reliability [10].

Protection Strategies for Application-Control Layer. When power enterprises consider the issues of software and equipment bidding, they should strengthen the investigation of suppliers. For instance, they should audit qualification rigorously for external units, particularly the foreign manufacturers, and

ban illegal storage of company's data. Moreover, they should strengthen the security of the device in variety of ways, such as contracts, confidentiality agreements, confidentiality undertaking, etc.

Equipment tender units should strengthen the management of control, protection and monitoring subsystem software's development, specify code writing of supplier's software, and require software manufacturers writing code in accordance with unified national and industry secure programming specification. The manufacturers' developing environment should be separated physically from the actual operation environment of power system. After the software is developed, it should be tested by qualified third party software testing unit [11], and issued a detailed report on safety testing to ensure that there are no loopholes and no "back doors" in the system and software.

Protection Strategies for External Network

Physical Isolation Technology. As the power monitoring system security protection requires, dedicated power forward and reverse isolation device should be used to achieve physical isolation of electricity production control network and management information network, cut off general network protocols penetration.

Network Protocols Isolation Technology. In management information network, we should use strong logical isolation device based on proprietary communication protocol to achieve separation of inner and external information network. Using two interfaces of device, inner and external network can exchange data seperately through proprietary protocol. When using protocol isolation technology, the inner and external network of electric information are disconnected. Only if there is need for information exchange can inner and external network be connected temporarily.

Virtual Private Network (VPN) and Virtual Local Area Network (VLAN) Technology. In order to prevent sensitive data theft, VPN technology applys techniques, such as dedicated digital certificates of electric power dispatch and longitudinal authentication encryption device, to encrypt and encapsulate data from the smart substation's integrated monitoring system, and transport them to the remote dispatch (control) centers through virtual network tunnel. Substation's VLAN technology puts the devices belongs to the same gap in a small LAN to transmit information, which will optimize configuration of network traffic [12].

Intrusion Detection and Intrusion Tolerance Technology. Intrusion detection technology is to monitor and control the process of communication actively, and supervise the network port and node information in real time [13,14]. It should detect intrusion in time, and maintain system's certain functions after intrusion occurres to avoid significant damages.

Other Safety Measures. The security of substation's information network, which is comprehensive and dynamic, should be achived by integrated multiple technologies other than by one single security technology [15]. For example, we can enabled the station platform's mechanisms of user permission and user policy to restrict user access, and use third-party encryption and digital signature technology for the initial sensitive data in the process of applications programming. [16]. To ensure the safe and reliable operation of substation's communication networks, we can take comprehensive measures including operating system security, fault-tolerant technology, access control, security monitoring, data backup and recovery techniques and other means, such as trusted computation [17]

Conclusion

It should be noted that the security threat substation's cyber-physical system faced with is often a combination of various situations. Therefore, we need to combine smart substation's physical elements and cyber elements as a whole to analyze its cyber-physical security and reliability [18] voiding emphasizing one aspect while ignoring the other. In this paper, a CPS three layer architecture of substation is proposed, which consists of perception-execution layer, transport layer and application-control layer. The security threats substation faced with and the corresponding protection strategies are analyzed in this three layer architecture.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61471328), and Science and Technology Project of State Grid Corporation of China (No.SGRIDGKJ[2013]548).

References

[1] Z. Liu: State Grid No. 01 (2014), p. 30
[2] Z. Li, Y. Peng, F. Xie, Y. Gao, D. Chen, G. Xu: Journal of Tsinghua(Science and Technology) Vol. 52 No. 10 (2012), p. 1482
[3] B. Wang, L. Huang, R. Cao, X. Dong and M. Kang: Power System Protection and Control Vol. 42 No. 1 (2014), p. 119
[4] J. Ji, Y. Yang, Y. Yuan, L. Wang: High Voltage Engineering Vol. 41 No. 3 (2015), p. 998
[5] W. Chen, T. Zhang: Sichuan Electric Power Technology Vol. 31 No. 3 (2008), p. 75
[6] T. Chen, S. Abu-Nimeh: Computer Vol. 44 No. 4 (2011), p. 91
[7] R. Langner: IEEE Security & Privacy Vol. 9 No. 3 (2011), p. 49
[8] A.Wu: Science and Techonology Innovation Herald Vol. 12 No. 1 (2015), p. 85
[9] X. He, Z. Feng, M. Wang, H. Zhou, X. Yang, B. Zhu: Zhejiang Electric Power Vol. 35 No. 4 (2015), p. 22
[10] H. Zhao, R. Zhang, Z. Chen: Electrical & Energy Management Technology NO. 18 (2010), p. 14
[11] X. Ren, D. Zhang: Modern Enterprise Education No. 21 (2011), p. 268
[12] X. Yuan: Guide to Business No. 14 (2015), p. 134
[13] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, et al: IEEE Transactions on Power Delivery Vol.25 No. 4 (2010), p. 2376
[14] J. Hong, C. Liu, M. Govindarasu: IEEE Transactions on Smart Grid Vol. 5 No. 4 (2014) p. 1643
[15] Z. Gao, Y. Luo, G. Tu, T. WU: Automation of Electric Power Systems Vo. 26 No. 1 (2002), p. 53
[16] B. Vaidya, D. Makrakis, H.T. Mouftah: IEEE Network Vol. 27 No. 1 (2013), p. 5
[17] K. Gao, Y. Xin, Z. Li, W. Sun, G. Nan, H. Tao, B. Zhao: Automation of Electric Power Systems Vol. 39 No. 1 (2015), p. 48
[18] H. Lei, C. Singh, A. Sprintson: IEEE Transactions on Smart Grid Vol. 5 No. 5 (2014) p.2194