AN OPERATION VERIFICATION STRATEGY AGAINST NETWORK ATTACK OF DCS IN NUCLEAR POWER PLANT

Chao Guo, Jianghai Li, Zhe Dong, and Xiaojin Huang
Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing 100084, China
guochao@tsinghua.edu.cn; lijianghai@tsinghua.edu.cn; dongzhe@tsinghua.edu.cn; huangxj@tsinghua.edu.cn

ABSTRACT

Digital Instrumentation and control (I&C) system serves as the "senses and nervous system" of a nuclear power plant (NPP). It plays an important role in the safe and economic operation in the NPPs. Digital I&C system has a series of advantages compared with analogue ones, but the introduction of the operation system platform, the application software, and the network communication structure are causing security risk to the power plant. Different kinds of procedures have already been adopted against these risks such as the communication isolation, but the security attacks still occur from time to time in the industrial fields around the world. This paper presents two computer security methods based on the thought of software verification and validation with step-by-step operation identification. First, three scenarios of security attack are proposed according to the structure of a distributed control system (DCS). Then a method with two network bypasses and a security computer are adopted to obtain the operation commands, the actuation signal, and the operation feedback in case of the first two scenarios by identifying the consistency of the obtained data. Furthermore, the method is optimized by combining the operation procedure and the camera shot to identify the anomaly of the information flow, thus to improve the effectiveness against the computer security issues. In the end, the influence and feasibility of this method is discussed.

Key Words: Digital instrumentation and control system, computer security, operation verification, computerized operating procedure

1 INTRODUCTION

The instrumentation and control (I&C) system architecture, together with plant operations personnel, serves as the "senses and nervous system" of a nuclear power plant (NPP). With the rapid development of the computer science and technology, the I&C system is getting more and more important for a modern NPP and digital I&C systems are being employed widely in the NPPs [1]. Compared with analogue ones, digital I&C system has a series of advantages in reliability, maintainability, availability, computation ability, and the human-machine interface [2]. While there are also computer security challenges together with these characteristics [3]: the function of every component relies heavily on the computer software, and the data transmission between different components relies on the network communication. The risks of computer security include the theft of information, the malicious modification of data, the illegal access of control, and so on [4]. The operation system platform, the application software, and the network communication structure have becoming the breakthrough in computer attacks [5], and this problem has received growing attention of the regulatory authority, the development agencies, and the stakeholders.

The non-safety distributed control system (referred to as DCS) is responsible for the implementation of plant-wide power control, process control, and human-machine interface functions with an integrated

system as a control system platform. It realizes a comprehensive monitoring of all process system and equipment parameters, equipment status and control actions with network rings which makes it one of the core targets for network attacks [6]. And the vulnerabilities of the operating system that the operator stations employ are also easy to become the attack objects because of the reasons such as the zero-day vulnerability. In addition, DCS is a complicated system with an integrated network mounted by different types of equipment including the process control stations, I/O servers, operator stations, gateways, printers, and so on. Hidden malware of these components increase the risk of being attacked [7].

This paper proposes two methods against different computer security scenarios both of which base on multiple verification of operation command. In this paper, the characteristics of computer attack are first introduced in Section 2 and three scenarios of computer attacks are introduces according to a common topology of DCS system. Then two computer security methods are proposed in Section 3 and Section 4, respectively. The feasibility and the effect on the DCS system of this method is analyzed in Section 5. In the end, a summary of this paper is given in Section 6.

2 SCENARIOS OF SECURITY ATTACK

Security attacks occur more and more frequently in the industrial field during last decade, and the impact of the attacks are also growing. The most typical events include the Stuxnet worm that attacked the Iranian Bushehr nuclear power plant in 2010 [8], the “Flame” worm that infected the Middle East energy industry in 2012, the OpenSSL “Heartbleed” security bug that affected Siemens, ABB and other companies’ industrial products in 2014, and the “BlackEnergy” that attacked the system vulnerabilities of Siemens WinCC system of the Ukrainian power grid system in 2015.

Direct connection with Internet is one of the major reasons for computer security attack. While for the digital I&C systems in the NPP, data can only be transmitted from the 1E network to the non-safety network through one-way communication. And the network of DCS only connects to the emergency command center and information management system by one-way communication. So traditional security attack cannot easily involve the I&C systems of the NPP directly. However, in addition to the real-time attack through the Internet, the virus may also invade the DCS through a U-disk, then it hides in the system without any action. Once the status of the system satisfies with the predetermined one, the virus starts security attack at once. Stuxnet worm is the representative of this kind of attack. From 2009 to 2010, the uranium enrichment plant in Natanz of Iran was attacked and 30% of the computer facilities were controlled by this worm. The characteristics of the Stuxnet worm include: 1) The object of the worm is precise. 2) It spreads in a variety of ways. 3) It can destroy devices by infecting the control software and then send spurious control commands. Specifically, the Stuxnet worm takes control of the centrifuges, while the fault situation is covered and “normal” status is transferred to the operator, resulting in misjudgment for decision-making.

The typical security attack scenarios against DCS are shown in Figure 1. There are two ring networks in the DCS, namely the Monitor Network (MNET) and the Control Network (CNET). The MNET connects the equipment of the human-machine interface layer and the server equipment layer; the CNET connects the IO server and the process control stations of the nuclear and the conventional islands. Each process control station, operator station, server, gateway and other equipment are connected to two redundant networks through network interface and communication cables, respectively.

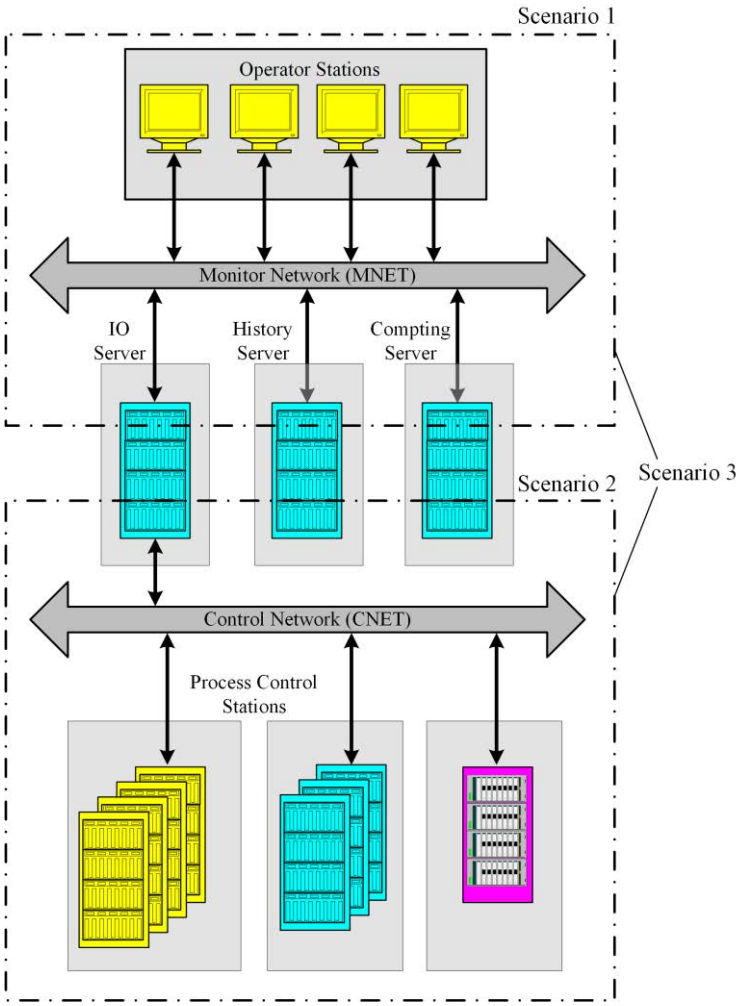

Figure 1. Scenarios to computer attacks against DCS.

There are three kinds of scenarios for the computer attacks according to the structure of DCS in Fig. 1. Scenario 1: the worm locates in the operator station. It can change the command transmitted from the operator station to the I/O server and the feedback information transmitted from the I/O server to the operator station. The Stuxnet worm can result in this kind of scenario. Scenario 2: the worm locates in the process control stations (PCSs). It can change the command transmitted from the I/O server to the PCSs and the feedback information transmitted from the PCSs to the I/O server. Scenario 3: the worm locates both in the operator station and the process control stations (PCSs). It can change the command of the operator, the actuation and feedback signal of the PCS, and the feedback signal displayed on the human-machine interface of the operation station. It can be found that Scenario 3 is the most difficult one to be detected as every step of the data flow has been invaded in this case.

3 A METHOD AGAINST SECURITY ATTACK

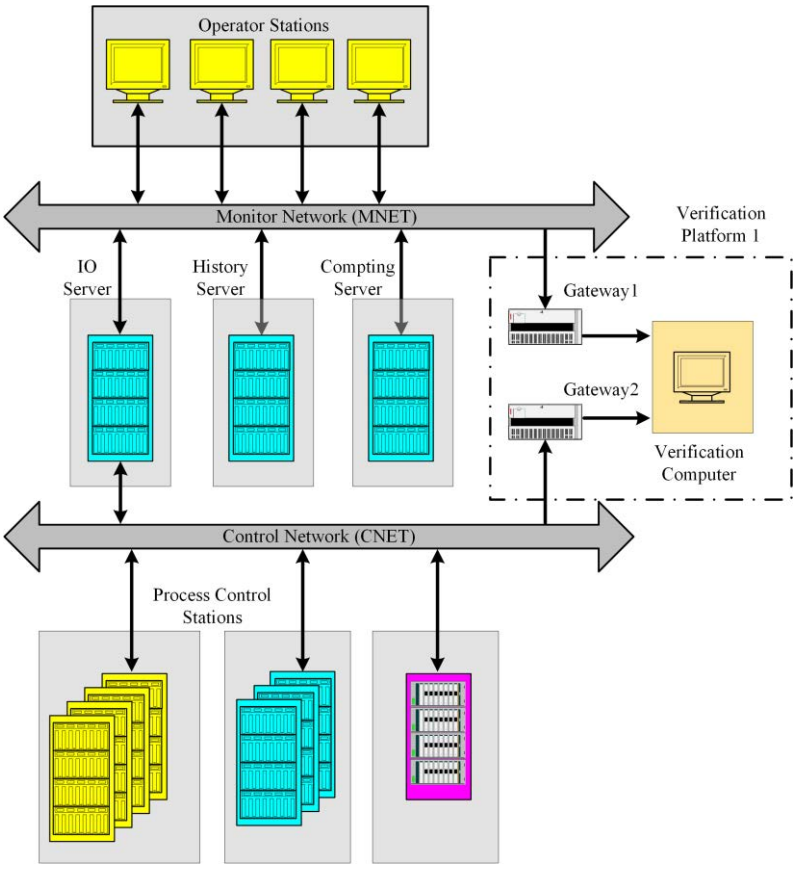

Figure 2. A verification method against computer security attack.

The first proposed method is shown in Fig 2. A verification platform with two sets of gateways added in the MNET and the CNET is used to collect: 1) the operation command of the operator from the MNET; 2) the feedback signal of the process control station from the CNET; 3) the displayed feedback signal on the visual display unit from the MNET.

Scenarios 1 and 2 of the security attack introduced in Section 2 can be identified easily by the topology in Fig. 2. For example, let's suppose the operator send out the command to "insert the control rod", and the command is modified to be "raise the control rod" in the operator station for the case of Scenario 1. Correspondingly, the feedback signal coming from the position measurement system of control rod sends the signal with "control rod raised" to the operator station. However, since the operator's intention is to insert the control rod, the feedback signal shown to the operator must be tampered again by the worm at the operator station to be "control rod inserted". This scenario can be identified with the verification platform 1 in Fig. 2: The gateway 1 acquires the tampered operation command to be "raise the control rod" (operation 1). And the actual feedback signal of the control rod signal collected by the gateway 2 is still to be "control rod raised" (operation 2), which is consistent with the fake operation command. While the rod operation feedback signal collected by the gateway 1 is "control rod inserted" instead (operation 3). Compared operations 1, 2, and 3 with each other and it can be easily determined that the operational signal flow has been tampered with the existence of computer security attack behavior.

4 AN OPTIMIZED METHOD AGAINST THE SECURITY ATTACK

The conflict caused by the Scenarios 1 is easy to recognize, but for Scenarios 2 and 3, the worm changes the signals of both the operator station and the process control station simultaneously. In this case, if the system is suffered from this kind of worm, the operation 1, 2, and 3 are all collected to be "insert the control rod", which means that the method in Section 3 should be modified for this occasion.

As shown in Fig. 3, an optimized verification platform is proposed. In addition to the gateways

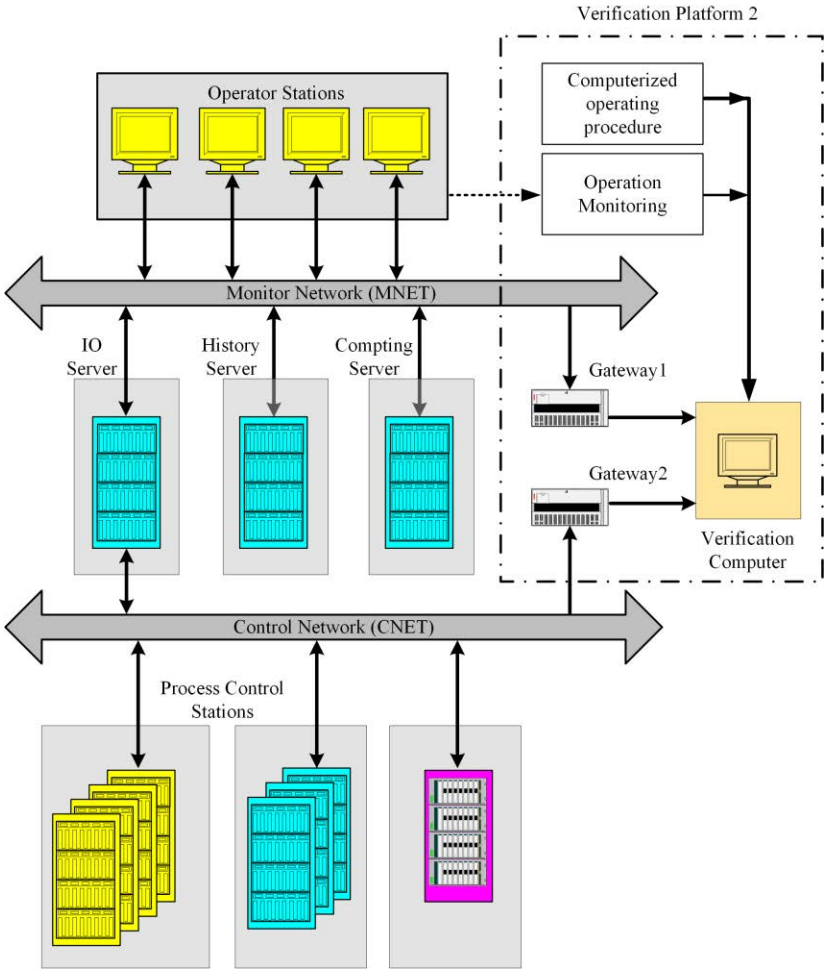

Figure 3. An optimized verification method considering the input of the system.

connected to the MNET and the CNET, the computerized operating procedure and the operation monitoring are included in the verification platform. The computerized operating procedure is used as the input of the platform, every other operations should be compared with it directly. The operation monitoring is the process in which the action of the operator is monitored. There can be two possible ways for the operation monitoring: The first one is the camera shooting and screenshot identification; the second way is adding data collecting device between the operator station and the input equipment such as the keyboard and the mouse.

The verification steps can be realized as follows:

1) Confirm the actual operation command through the computerized operating procedure.

2) Sample the action of the operator and verify it with the operating procedure, if there exists a conflict, the operator may send the wrong command.

3) Sample the operation command send by the operator station.

4) Sample the actual command output of the PCS.

5) Collect the feedback signal from the PCS.

6) Collect the feedback signal that displayed by the operator station.

When these signals collected from Step 3) to Step 6) does not match with the procedure, it can confirm easily that the existence of the network attack. This optimized verification platform can also overcome the problem mentioned in the first paragraph of this section for Scenarios 2 and 3.

5 DISCUSSIONS

a) Feasibility of the proposed methods

Two verification platforms were proposed in this paper. The platform 1 employs two gateways to obtain the operation command and the feedback data from MNET and CNET, respectively. Then the parameters are used for security attack identification of the operator stations, the MNET, and the IO server according to the consequence of the command. Two gateways are connected to the network by one-way communication in case of extra security risk. This identification platform is easy to realize as the data acquisition, command verification and decision making are common techniques.

Based on the platform 1, the optimized verification platform 2 added two processes: the computerized operating procedure and the operator action sampling. Firstly, the computerized operating procedure is a database that includes major processes of the control tasks, which means the verification process cannot be fulfilled automatically as the operator has to input the procedure before the operation. Secondly, the operator action sampling is the most difficult part in this platform. It refers to the image processing and human-machine interface. If this step is hard to realize, the computerized operating procedure can also work for three attack scenarios.

b) Influence on the DCS

For both verification platforms, two gateways are connected to the network by one-way communication, and there is no direct influence on the DCS. For the verification platform 2, the computerized operating procedure can also obtained for DCS by one-way communication. The sampling camera is also independent of the DCS. So all the equipment of two platforms have no influence on the DCS.

6 CONCLUSIONS

As the development and employment of digital I&C systems in the NPPs, security attacks have become more and more frequent around the world and the influence are getting more and more serious. More attention should be paid on this field. DCS is the most important monitoring and control system in the NPP, and it is also a vulnerability for the computer security.

In this paper, three kinds of scenarios of security attacks for the DCS are analyzed and two computer security verification platforms against DCS security attacks are proposed. Firstly, a computer security method based on operation verification was proposed and two gateways were adopted on the network of the DCS structure to obtain the operator command, the feedback of process control station, and the feedback signal displaying on the operator station. A verification computer is used to compare the obtained information to identify the network attacks. In addition, an optimized verification platform was proposed for the attack Scenarios 2 and 3: the computerized operating procedure and the operation action

sampling were introduced to the verification platform to meet the diagnostic process which could improve the accuracy of diagnosis. The method proposed in this paper can effectively identify the tampering and camouflage of the information flow caused by the network worms and improve the computer security of the DCS in the nuclear power plant.

7 ACKNOWLEDGMENTS

This research was supported by Tsinghua University Initiative Scientific Research Program, National Science and Technology Major Project of China (Grant No. ZX06901), and National Natural Science Foundation of China (Grant Nos. 61502270, 61374045).

8 REFERENCES

[1] M. C. KIM, "Reliability analysis of digital I&C systems at KAERI," *Nuclear Safety and Simulation*, **vol. 3**, pp. 276–280 (2012).

[2] S. A. Arndt, "Digital Instrumentation and Control Systems in Nuclear Power Plants," in *Proceedings of the 18th International Conference on Nuclear Engineering*, 2010, pp. 1–8.

[3] Y. Soupionis, R. Piccinelli, and T. Benoist, "Cyber Security Impact on Power Grid Including Nuclear Plant," in *Proceedings of the Federated Conference on Computer Science and Information Systems*, 2016, **vol. 8**, pp. 767–773.

[4] D.-Y. Kim, "Cyber security issues imposed on nuclear power plants," *Annals of Nuclear Energy*, **vol. 65**, pp. 141–143 (2014).

[5] H. S. Cho and T. H. Woo, "Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs)," *Annals of Nuclear Energy*, **vol. 99**, pp. 47–53 (2017).

[6] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, **vol. 46**, pp. 583–594 (2007).

[7] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Transactions on Industrial Informatics*, **vol. 9**, pp. 277–293 (2013).

[8] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, **vol. 53**, pp. 23–40 (2011).