INTRODUCTION OF A CYBERATTACK DETECTION FRAMEWORK FOR SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

TAEJIN KIM
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
DAEJEON, REPUBLIC OF KOREA
Email: taejinkim@kaeri.re.kr

YOUNG-JUN LEE
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
DAEJEON, REPUBLIC OF KOREA

INHYE HAHM
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
DAEJEON, REPUBLIC OF KOREA

Abstract

As cyberattack becomes more complex and intelligent, an air-gapped computer or network of nuclear power plants cannot guarantee 100% safety from cyberattacks. For the Iranian nuclear facility in 2010, a malicious computer worm broke into the nuclear program and disabled the key part although the target was located in the air-gapped facility. In most small modular reactors(SMRs), the instrumentation and control(I&C) systems are digitalized. They are designed to comply with codes and standards of cybersecurity, but there are few detection systems for cyberattacks. Especially for safety systems, no direct cyberattack detection system is applied because there is a big concern about impacts of safety functions as new security system is introduced in the I&C architecture. Thus, this study suggests a framework to detect cyberattacks in safety systems without affecting direct safety functions based on the study of APR1400.

1. INTRODUCTION

The instrumentation and control (I&C) systems in nuclear power plants (NPPs) of South Korea have been digitalized due to the difficulties in sourcing analog parts and the various advantages of digital systems. In the case of Advanced Power Reactor 1400 (APR-1400), most of the I&C systems are being digitalized, and especially, all safety systems such as plant protection system (PPS), reactor core protection system (RCOPS), engineered safety features – component control system (ESF-CCS) have been fully digitalized. With the shift towards small modular reactors (SMRs), it is necessary that I&C systems have to be integrated and miniaturized. It accelerates digitalization of I&C systems and the impact of a single integrated safety system increases, so importance of cybersecurity has become even more critical.

In order to cope with cyber threats in South Korea, Korea Institute of Nuclear Nonproliferation and Control (KINAC) have published technical standards for cyber security of nuclear facilities [1] and critical digital assets for nuclear facilities [2]. Thus, it is required to identify all digital assets in NPPs based on their Safety, Security, and Emergency Preparedness (SSEP) Functions and to satisfy defense-in-depth cybersecurity architecture by classifying the cybersecurity levels for all digital assets.

For industrial control systems (ICSs) of NPPs, it is expected that they are unlikely to expose threats of cyberattacks due to their air-gapped environment. However, considering the cyberattacks occurred in nuclear facilities, such as stuxnet attack occurred in Iran's nuclear facility, malware attack in the Monju NPP of Japan, malware attack in the Kudankulam NPP of India, etc., it is necessary to take measures against cyberattacks even for the ICSs separated from the external networks. As it is crucial to cope with cyberattacks in NPPs, intrusion detection systems (IDS) have been applied to networks and servers in South Korea. However, in the safety systems of NPPs, IDS has not yet been introduced because of concerns that they may affect the original safety functions of safety systems.

In this study, we introduce a cyberattack detection framework to detect cyberattacks in safety systems, ensuring that the original safety functions are intact and taking into account the characteristics of safety systems.

2. BACKGROUND

2.1. Intrusion detection system

For the purpose of detecting cyberattacks on ICSs in an operational technology (OT) environment, IDS is broadly classified into Host-based IDS which monitors states of the internal system and Network-based IDS which monitors network packets coming from the system. Specifically, a host-based IDS establishes a database to store the attributes of system objects, such as permissions, sizes, modified dates, etc. as a normal state, and periodically keeps track of them. If any abnormal changes are detected, it generates alerts. A network-based IDS monitors network packets to detect abnormal activities with various methods, such as pattern matching, behavior detection, monitoring protocols, monitoring IP or MAC addresses, encrypted traffic analysis, blocking command and control servers, and so on.

2.2. Configuration of safety systems on APR1400

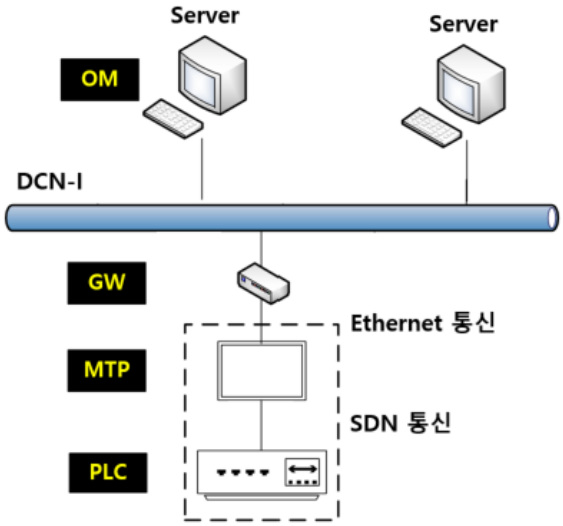

FIG. 1. Configuration of safety systems on APR1400.

Most of the safety functions in a safety system of APR1400 are implemented on the digital platform of POSAFE-Q which is programmable logic controller (PLC)-based one with safety grade real-time operating system (RTOS). In PLC, the various functions are performed such as reading process signals, comparing the signals with its setpoint, and performing two-out-of-four voting logic to generate reactor trips or engineered safety features actuation signals for safety functions.

Maintenance and test processor (MTP) is provided for periodic surveillance testing of safety functions to check their functionality. Thus, the main variables of the PLC, including process values, reactor trip status, setpoint values, alarm status, etc., are transmitted to MTP through SDN communication protocol which was developed for safety systems [3].

Through the gateway, the data which are required to operate reactors for operators are conveyed to operator module (OM). The gateway allows traffic to flow from MTP to the external network, but blocks it in the opposite direction. The OM displays the data to show the system status and the actuation status.

3. CONSIDERATION ON CHARACTERISTICS OF SAFETY SYSTEMS

3.1. Impact of a new security process on safety functions

According to the definition of IEEE std. 603-2009, the safety system is defined as “A system that is relied upon to remain functional during and following design basis events to ensure: (a) the integrity of the reactor coolant pressure boundary, (b) the capability to shut down the reactor and maintain it in a safe shutdown condition,

or (c) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10CFR100 guidelines" [4]. That is, safety functions performed by safety systems are critical to nuclear safety. Thus, an IDS must be guaranteed that there is no impact on safety functions. However, it is challenging to demonstrate that there is no impact when safety process and security process operate simultaneously on a single RTOS. To guarantee that a new security process does not impact the existing process, besides lowering the priority of the security process in the RTOS, other factors must be considered such as not interfering memory assess of the existing process, preventing excessive CPU overhead or degradation in performance caused by a new process, allocating system resources between the existing process and a new process, etc.

3.2. Logic characteristics of safety systems on APR1400

In APR1400, the representative safety functions are implemented in the plant protection system (PPS). The PPS monitors process variables and generates signals for the reactor trips and the engineered safety features. The majority of the system is implemented with simple comparison logic that triggers reactor trips and engineered safety features when the process values exceed their setpoints.

When the data is transmitted from the PLC to the MTP via SDN communication, most of the data, such as the process values, the setpoints, the alarm status, the generated signals for the reactor trips and the engineered safety features, etc., is conveyed, except for the logic in the PLC.

Thus, if the MTP has a database which stores setpoints for the reactor trips and the engineered safety features, the MTP can check whether the setpoints have been manipulated and further distinguish whether the logic in the PLC has operated correctly.

3.3. Communication characteristics between the PLC and the MTP

Digital computers in safety systems must satisfy IEEE std. 7-4.3.2, and it adopts IEEE std. 1012 for software verification and validation [5]. Software integrity level (SIL) is defined in terms of software complexity, criticality, risk, safety level, security level, desired performance, reliability, or other project-unique characteristics in IEEE std. 1012 [6]. Since the SIL is established in the light of general industrial characteristics, KEPCO E&C classifies software used in NPPs into four classes in Table 1 [7].

TABLE 1. SOFTWARE CLASSIFICATION

Software Classification	Description	Matching SIL
Protection (Safety-critical)	Software whose function is necessary to directly perform reactor protection system (RPS) control actions, engineered safety feature actuation system (ESFAS) control actions, and safe shutdown control actions.	4
Important to Safety (ITS)	Software whose function is relied on to monitor or test protection functions, software that monitors plant critical safety functions, or software that provides supplemental means to perform protection functions.	3
Important to Availability (ITA)	Software that is relied on to maintain operation of plant systems and equipment that are critical to operate the plant.	2
General Purpose (GP)	Software that performs some functions other than that described in the previous classifications.	1

In APR1400, the software in the PLC and the MTP are classified into Safety Critical (SC) and Import to Safety (ITS) level respectively. According to IEEE std. 7-4.3.2 [5] and KINAC/RS-015 [1], the MTP cannot transmit the data to the PLC since the software grade in the MTP is lower than the software grade in the PLC. In other words, assuming the IDS is installed in the MTP for detecting cyberattacks occurred in the PLC, it is not

possible to access the PLC from the MTP via communication. Thus, the IDS in the MTP does not provide any access point to the PLC in terms of cyberattacks and affect the original process of the PLC which conducts safety functions.

4. CYBERATTACK DETECTION FRAMEWORK FOR SAFETY SYSTEMS OF NPPS

Based on the characteristics of safety systems in APR1400 mentioned in Section 3.0, cyberattack detection framework is developed in Figure 2. An IDS is implemented in the MTP and a database is built based on the functions of the IDS. The database includes the data, such as setpoints of reactor trips and engineered safety features, maximum and minimum values of process values, and so on. The IDS scans the data coming from the PLC every 1 seconds and conducts its internal logic algorithm to monitor cyberattacks occurred in the PLC.

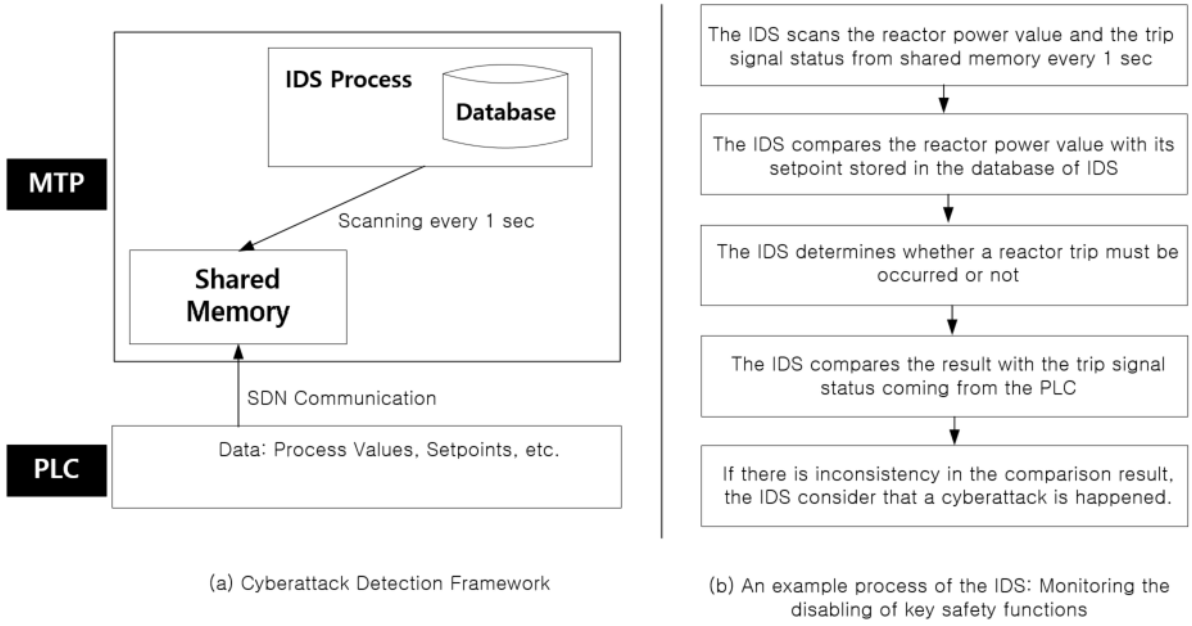

FIG. 2. CYBERATTACK DETECTION FRAMEWORK AND DETECTION PROCESS

The internal logic algorithm is developed for the four main functions as followings: a) Monitoring the manipulation of key constants, b) Monitoring the manipulation of key setpoints, c) Monitoring the disabling of key safety functions, d) Monitoring the disabling of key alerts. For an example of the algorithm process to monitor the disabling of a reactor trip function, the IDS scans the reactor power value and the trip signal status from the shared memory every 1 sec. The reactor power value is compared with its overpower trip setpoint which is stored in the database of IDS. If a reactor power value is higher than its setpoint and the trip signal status indicates no trip, the IDS considers that it is a cyberattack and provides an alert to operators.

For reference, some constants are not transmitted every communication cycle from the PLC to the MTP due to communication overload in APR1400. During the implementation of the IDS, the IDS is developed reflecting these practical design characteristics.

5. CONCLUSION

As cyberattacks become more sophisticated and complex, it is necessary to introduce an IDS for safety systems of NPPs. However, if the IDS is implemented in the PLC, it is challenging to guarantee that the IDS process does not affect the existing safety functions.

The cyberattack detection framework suggested in this paper can detect cyberattacks occurred in the PLC without any impact to the safety functions. Also, since the algorithm of the IDS utilizes the characteristics of

safety systems, it can detect different types of cyberattacks which can be detected the network-based IDS installed at the server level.

ACKNOWLEDGEMENTS

This work was supported by a grant from the Ministry of Trade, Industry and Energy in Korea (No. 20224B10100140).

REFERENCES

[1] KINAC/RS-015, Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities, KINAC (2014).
[2] KINAC/RS-019, Technical Standard on Identification of Critical Digital Assets for Nuclear Facilities, KINAC (2015).
[3] KAERI/CM-1078/2007, A Development of the Digital Reactor Safety System: Study on the High Reliable Communication for Hard Real Time Environment, Korea Atomic Energy Research Institute (2008).
[4] IEEE STD. 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, (1998).
[5] IEEE STD. 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, (2003).
[6] IEEE STD. 1012, IEEE Standard for Software Verification and Validation, (2004).
[7] KIM, Y.-B., KIM, T., JUNG, K.-H., SHIN, J.-H., YUN, J.-H., Necessity and Guideline for Development of Reg. Guide 1.97 Type A Variables Display, Information and Control Symposium (2016).