Real-time Network Intrusion Detection System with Supporting Cyber Security Regulations for Nuclear Power Plants

Jae-Hee Roh [a*], Seok-Ki Lee [a], Choul-Woong Son [a], Cheonghwan Hwang [b], Jaehyun Park [b]
[a]*NSE Technology Inc., I&C Cyber Security Team, Daejeon, Rep. of Korea*
[b]*Inha University, Information & Communication Dept., Incheon, Rep. of Korea*
[*]*Corresponding author: jhroh@nsetec.com*

1. Introduction

APR1400 is the Korean nuclear power plant (NPP) model which was first applied to Shin Kori Units 3/4 in 2006. Since then, a total of more than 6 units including Shin Hanul Units 1/2 and Shin Kori Units 5/6 have been designed and under construction.

The MMIS of the APR1400 model is implemented in a computer-based digital method from the existing analog method, which has high accuracy and efficiency, but the importance of cyber security has increased in proportion. In existing nuclear power plants, all instrumentation and control (I&C) systems have been based on the hard-wiring devices, but recently, network-based instrumentation and control systems such as high-speed fieldbus have been used instead of hard-wiring. However, as the proportion of digital device-based measurement and control systems increases, cyber security, especially network security, has also emerged as a very important issue.

Due to increasing national anxiety about nuclear safety caused by cyber threats from a group of nuclear hackers in December 2014, Korea nuclear regulatory agency requires nuclear licenses to establish Cyber Security Plan in accordance with the Radiological Emergency Preparedness Law and related regulatory guidelines [1-5] and to implement the plan in seven phases by 2018 [6]. The network used in the safety and non-safety control system of a nuclear power plant must satisfy a special requirement to meet high reliability, such as one-way communication and network buffering, unlike the network used in general factory automation. This means ordinary commercial network security systems are hardly used in the nuclear power plants. Hence, a specially designed cyber security system is required to meet the NPP-related regulations.

One of the efficient ways to protect a network node form the unknown or suspicious network activities is to adopt a network intrusion detection system (NIDS) that analyzes the incoming network packets and warns the users upon detection of a malicious network packet or a suspicious network access form unknown network nodes. Most of the network monitoring and intrusion detection systems currently used are software-based systems that are difficult to detect high-speed network packets in real time, so that are used for the purpose of identifying root-causes or taking follow-up actions rather than defending against abnormal packets in real time. These software-based NIDS usually run on the target network nodes that should be protected or on a standalone server to protect the network subnets. While these software-based NIDS are flexible and easily reconfigurable, they still have shortcomings: First, since the incoming network packets are analyzed by software, it takes a relatively a long time to detect an abnormal packet and suspicious cyberattacks. This means that a real-time network protection is hardly implemented. Second, a server or system running a NIDS software consumes a large amount of resource that results in the packet loss, even in a low-bandwidth network environment [7].

In order to overcome the problem of the software-based NIDS, a hardware-based NIDS using a FPGA has been proposed [8-9]. Although such a hardware-based network monitoring device greatly improves real-time network security, additional administrative facilities are required to satisfy various regulatory conditions required for a nuclear power plant information and control systems. In this paper, we proposed a cyber security system that can be used in control networks of nuclear power plants that require high levels of reliability. The proposed system consists of DACS (Detection on Attacking Control System), DACS Management Program (DMP) to centrally manage multiple DACS, and Central Monitoring Server (CMS) to store system logs. The proposed system is designed to meet the requirements of the US Nuclear Regulatory Commission and the Korea Nuclear Cyber Security Regulations [1-5].

2. Proposed Architecture

2.1 Cyber Security Regulation Requirements Analysis and Derivation for NPPs

The regulatory standard of cyber security for domestic nuclear facilities (KINAC/RS-015) includes requirements for establishing cyber security system that the licensee should carry out such as roles and responsibilities of cyber security team, identification of Critical Digital Assets (CDAs), Defense-in-Depth protective strategies, implementation of security controls, continuous monitoring and assessment and an incident response plan. And licensees are implementing cyber security measures gradually to establish the system for the operating nuclear power plants, but some of measures are security requirements to be considered from the development phase of CDAs such as logical access control, log function, security design, security test, configuration management, supply chain control,

and acceptance test. KINAC/RS-015 is configured as shown in Fig.1.

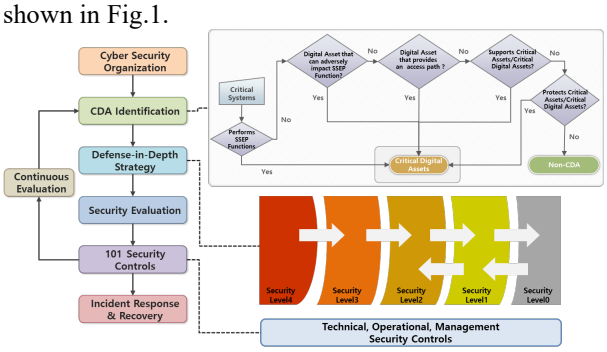

Fig. 1. KINAC/RS-015 Configuration

In this paper, selected the target devices (CDAs) for security evaluation as shown in Table 1.

Table I: Security Evaluation Target Devices (CDAs) Selection

CDAs	Major Functions	Security Evaluation Target
DACS (Hardware)	· Packet collection · Packet Parsing · Packet Analysis · Abnormal Packet Detection	●
DMP (Software)	· Rule Set · DACS Management	●

And then, cyber security design requirements for network intrusion detection systems and management program have been derived, and the implementation functions for each item are as follows.

Table II: Cyber Security Design Requirements for DACS and DMP

Division	Requirements ID	Requirements Title
DACS	SEC-DACS-01	DACS Account Management
	SEC-DACS-02	DACS Device Identification and Authentication
	SEC-DACS-03	DACS Information Flow Enforcement
	SEC-DACS-04	DACS Log Record and Inquiry
	SEC-DACS-05	DACS Session Lock
	SEC-DACS-06	DACS Denial of Service Protection
	SEC-DACS-07	DACS System Use Notification
	SEC-DACS-08	DACS Previous Logon Notification
	SEC-DACS-09	DACS Removal of Unnecessary Services and Programs
	SEC-DACS-10	DACS Software and Information Integrity
	SEC-DACS-11	DACS Hardware Configuration
	SEC-DACS-12	DACS Error Handling
DMP	SEC-DMP-01	DMP Account Management
	SEC-DMP-02	DACS Account Management
	SEC-DMP-03	DMP Communication Cryptographic
	SEC-DMP-04	DMP Protocol
	SEC-DMP-05	DMP Log Record and Inquiry
	SEC-DMP-06	DMP Session Lock
	SEC-DMP-07	DMP System Use Notification
	SEC-DMP-08	DMP Previous Logon Notification
	SEC-DMP-09	DMP Removal of Unnecessary Services and Programs
	SEC-DMP-10	DMP Software and Information Integrity
	SEC-DMP-11	DMP Error Handling

2.2 Concept of Cyber Security using NIDS

The network systems used in nuclear power plants have some special characteristics. First, the network of the safety system and the non-safety system must be completely separated, and all data must be transmitted in one direction form the safety system to the non-safety system. Second, all devices participating in the control network are identified in advance and unauthorized nodes cannot participate in the network.

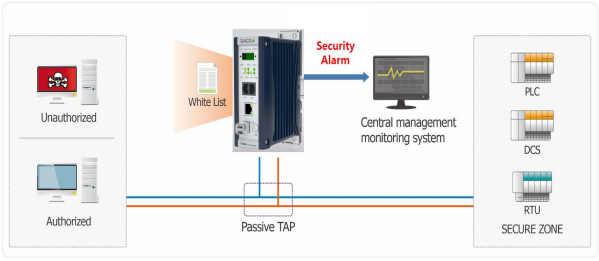

Fig. 2. Concept of Cyber Security using NIDS

In consideration of these characteristics, this paper adopts a network security method based on whitelist, that is, only data exchange between authorized nodes. In addition, because the added software or hardware must not affect the existing control function for network security, instead of installing additional security software on the existing controller, a separate node configures the security system by monitoring network packets through passive taps. The concept of cyber security using the network intrusion detection system proposed in this paper is shown in Fig 2. The network intrusion detection system proposed in this paper exists between the external network and the internal network connected to the control system, and monitors network packets by passive tap. On the other hand, by adopting such a passive tap method, real-time performance can be improved, but since an unauthorized network packet can reach a destination, a technique for detecting and processing and unauthorized packet in real time is essential.

2.3 Detection on Attacking Control System (DACS)

The DACS (Detection on Attacking Control System) developed in this paper is designed to be installed in the sub-network through the internal passive tap in order to detect anomalies by collecting and analyzing all the network packets. The internal function of DACS is configured as shown in Fig.3.

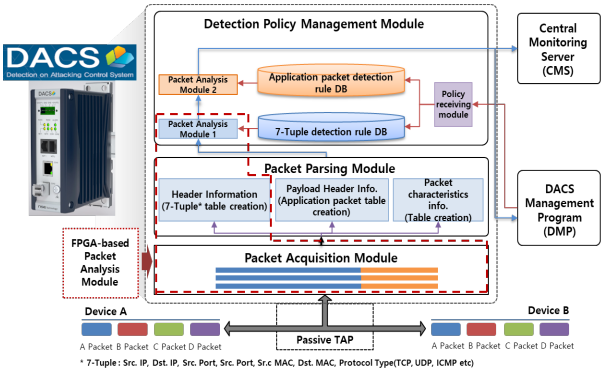

Fig. 3. Block diagram of DACS

The hardware of DACS consists of a passive tap interface for collecting packets, a packet collection module, a packet parsing module, and a detection policy

management module. The hardware of DACS is based on the NXP's LS1043A microcontroller, which has an ARM Core running at 1Ghz or higher speed, and 5 or more Ethernet ports. The operating software of the network anomaly detection system is equipped with QNX7.0, a real-time operating system (RTOS), and installs and uses only the service and device drivers necessary for system operation. It performs security functions by communicating with the Central Monitoring Server (CMS) and DACS Management Program (DMP).

When an intrusion detection policy, a whitelist composing of 7-tuple (MAC Source/Destination, IP Source/Destination, Port Source/Destination, Protocol Type), is set by DMP, the actual packet analyzing and detection function is performed by packet detection module implemented in FPGA. The detail structure of the packet detector is shown in Fig.4.

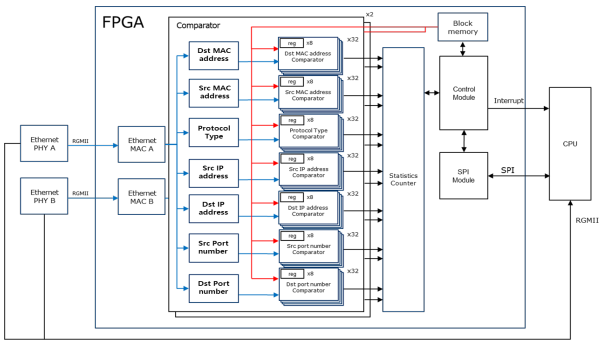

Fig. 4. Block diagram of FPGA

It consists of three blocks; the packet parser for parsing Ethernet packets into 7-tuple, the comparator for comparing the data parsed with the whitelist ruleset, and ruleset store implemented in the block RAM(BRAM) inside FPGA. Since the whitelist rule is composed of 7-tuple, a single comparator block consists of 7-tuple parallel comparators to compare a whitelist rule at once.

2.4 DACS Management Program (DMP) and Central Monitoring Server (CMS)

The control network is composed of several sub-networks as necessary, and an integrated management system is needed to efficiently manage security for the entire network. DACS Management Program (DMP) shown is a tool that enables centrally manage a control network that has been divided into several sub-network. The main role of DMP is to centrally manage the types of network protocols to be analyzed by each DACS and the addresses of nodes included in the whitelist in DB format. The management program can be used for the purpose of setting policies on the anomaly detection system or for program upgrade and maintenance, and provides a user interface environment. Communication between DACS and DMP is done through AES-128 encrypted secure communication network. Major functions of DMP includes protocol management, Asset management, DACS security management, DACS management, and communication module.

Central Monitoring Server (CMS) acts as a DB server that centrally manages information on network packets detected by each DACS. CMS functions can be operated on one server in combination with DMP, but can be operated separately or in combination depending on the security policy of the site. Information managed by CMS includes alarm log, security log, and event log. In addition, one of the important roles of CMS is to synchronize the time between all DACSs and DMP. The synchronized time is an important function for analyzing the sequence of cyberattacks. DMP and CMS is configured as shown in Fig. 5.

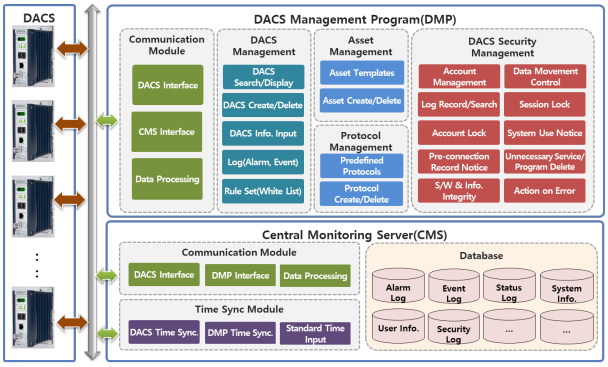

Fig. 5. Block diagram of DMP and CMS

2.5 Safety class Data Diode (SDD)

In accordance with the requirements defined in the Defense-in-Depth protective strategy of KINAC/RS-015, communication between the safety and non-safety regions of nuclear power plants must strictly observe unidirectional communication from the safety system to the non-safety system.

The safety class Data Diode (SDD) developed in this paper transmits data in one direction in the optical isolation section between the safety and non-safety systems to physically block the reverse signal and optical It is developed for the purpose of electrical isolation, and the overall configuration of the unidirectional transmitter and receiver module is shown in Fig. 6.

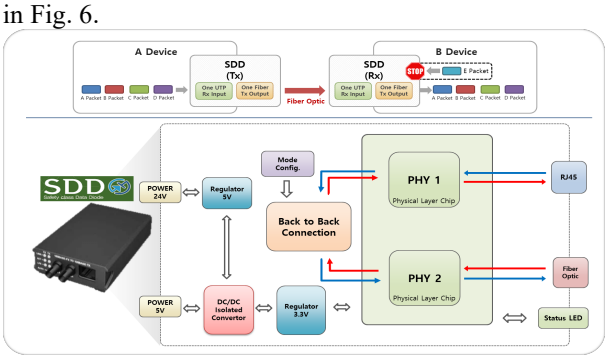

Fig. 6. Block diagram of SDD

The connection method between Ethernet PHYs to implement the unidirectional transmission function is

that packets received through the RJ45 port are output to MII_RXD of PHY1 and PHY2 for back-to-back connection. It is input to MII_TXD of and transmitted to Fiber Optic Port. PHY1 supports Cooper Cable connection method through RJ45 Connector, and PHY2 supports Fiber Optic connection method through ST Connector. In addition, clock synchronization between PHY1 and PHY2 is performed by using Dual Port PHY, and one-way transmission method.

3. Application to Nuclear Power Plants

The control system of a nuclear power plant is largely divided into two categories: a safety system and a non-safety system. Of these, the safety system directly controls the nuclear reactor and plays an important role in the safety of the power plant. Therefore, very strict standards and regulations apply to the configuration of the digital control system of the safety system and the network to connect the controller.

To prove the concept of the proposed system, Fig. 7 shows an example configuration that is applied to the nuclear power plants. In order to satisfy the security requirements applied to nuclear power plants, DMP and CMS are composed of separate systems, and all communication used end-to-end encryption with the AES-128 algorithm. The network protocol analyzed by DACS supports not only general automated control network protocols such as Modbus over TCP/IP, but also non-standard communication network protocols used to monitor and control the reactor, In order to satisfy unidirectional requirements, some network sections are installed to protect network separation requirements by installing *data diodes*, and this section is also configured to be protected through separate DACS. This configuration has been tested in the nuclear power plant simulator to verify whether it satisfies all the safety requirements of the nuclear power plants.

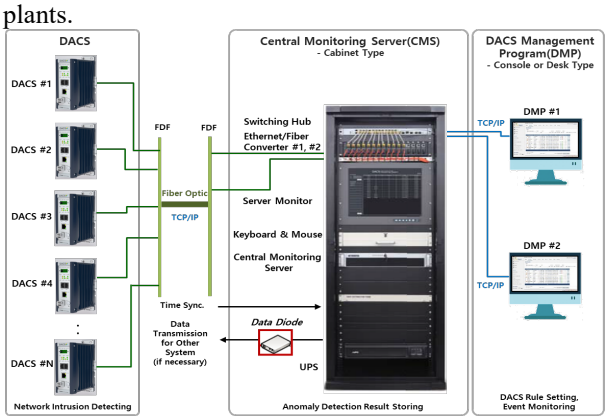

Fig. 7. Overall Configuration of DACS for NPPs

4. Conclusions

In this paper, we proposed a cyber security system that can be used in instrumentation and control (I&C) networks of nuclear power plants that require high levels of reliability. The proposed system consists of DACS with FPGA-based network packet detection function to detect network intrusion in real time, DACS Management Program (DMP) to centrally manage multiple DACS, and Central Monitoring System (CMS) to store system logs. DACS detects packets in real time by applying whitelist-based security rules in consideration of the characteristics of the control network, and notifies the CMS and DMP of the results. The packet detection function of DACS is handled by a real time packet detector implemented in FPGA, based on a whitelist composed of 7-tuples. The whitelist ruleset used in this paper consists of 7-tuples; MAC address, IP address, TCP/UDP port number of the source and destination network nodes, and protocol type. This paper showed the usefulness of the proposed system by presenting an example of applying the proposed system to the nuclear power plants information and control system. However, it was shown that the proposed system is not limited to nuclear power plants, but can be applied to industrial control networks in various fields.

ACKNOWLEDGEMENTS

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20171510102110)

REFERENCES

[1] U.S. NRC, “Cyber Security Programs for Nuclear Facilities”, Regulatory Guide 5.71, Jan. 2010.
[2] KINAC, KINAC/RS-015, “Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities”, Oct. 2014.
[3] KINAC, KINAC/RS-019, “Technical Standard on Identification of Critical Digital Assets for Nuclear Facilities”, Dec. 2015.
[4] IEEE Std. 7-4.3.2: Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std., August 2016.
[5] NEI 13-10: Cyber Security Control Assessments, Nuclear Energy Institute Std., Nov. 2016.
[6] Siwon Kim, “A Study on the Effectiveness of Grouping of the Critical Digital Assets at the Nuclear Facilities”, The Korean Institute of Communications and Information Sciences, Oct. 27-28, 2016.
[7] H. Chen, Y. Chen, and D. H. Summerville, “A survey on the application of FPGAs for network infrastructure security,” IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 541–561, April 2011.
[8] J. Kim and J. Park, “FPGA-based network intrusion detection for IEC 61850-based industrial network,” ICT Express, vol. 4, no. 1, pp. 1–5, March 2018.
[9] J. Kang, T. Kim, and J. Park, “FPGA-based real-time abnormal packet detector for critical industrial network,” in 2019 Workshop on Communications in Critical Embedded Systems (as part of IEEE ISCC 2019), July 2019, pp. 1199–1203.