Cyber Threat Response System Design and Test Environment

Taewoo Tak, Young-Jun Lee
Security R&D Team
Korea Atomic Energy Research Institute
Daejeon, Korea
e-mail: ttwispy@kaeri.re.kr, yjlee426@kaeri.re.kr

Taejin Kim
Research Reactor Design and Construction Agency
Korea Atomic Energy Research Institute
Daejeon, Korea
e-mail: taejinkim@kaeri.re.kr

***Abstract*—Incidents like the Stuxnet attack, which targeted uranium centrifuges, have proven that systems can be compromised even without direct Internet connectivity. This has underscored the importance of cybersecurity in nuclear facilities. To develop effective detection systems for Nuclear Power Plants (NPPs), it is essential to conduct research on identifying data available for system and device-specific detection based on instrumentation and control systems of NPPs. When analyzing cyberattacks that induce abnormal data and identifying intrusion indicators, the detection of cyber threats is broadly divided into host-based and network-based. This paper describes the design and test environment of cyber threat response systems for NPPs.**

Keywords-cybersecurity in NPP; NPP cybersecurity response system; cybersecurity test environment.

I. INTRODUCTION

The global increase in cyber threats extends beyond Information Technology (IT) to critical infrastructure fields. Historically, the nuclear power field received less attention due to its perceived immunity from cyber threats owing to its closed network environment. However, incidents like the Stuxnet attack, which targeted uranium centrifuges, have proven that systems can be compromised even without direct Internet connectivity [1]. This has underscored the importance of cybersecurity in nuclear facilities. Consequently, NPPs in operation are now integrating additional cybersecurity measures and conducting research to swiftly detect cyber threats for ensuring the safety of nuclear operations.

II. RELATED WORKS

A. *Weakness of Cybersecurity in Nuclear Power Plant*

Nuclear power plants have traditionally employed conservative technologies, largely relying on analog systems in their instrumentation and control systems. These systems were isolated from the internet, which significantly reduced the risk of cyber-attacks and minimized the plants' vulnerability to such threats. As a result, cybersecurity was not a primary concern in the design of these systems. However, with the advance of Information Technology, Instrumentation and Contral (I&C) systems in NPPs have been increasingly implemented with digital control devices, wired communication networks, and software. This shift has introduced new vulnerabilities, making these plants more susceptible to cyber-attacks. As these digital systems become integral to the operation and safety of nuclear facilities, it is crucial to incorporate robust cybersecurity measures to protect against potential threats and ensure the continuous safe operation of nuclear power plants.

Figure 1 provides an overview of the digital systems used in both safety and non-safety systems in the latest Nuclear Power Plant model. As depicted in the figure, the control, monitoring, and protection systems in the safety systems employ Programmable Logic Controller (PLC) platforms. Meanwhile, the non-safety systems utilize Distributed Control System (DCS) platforms. These systems work together to provide integrated Human-Machine Interface (HMI) information to operators in the main control room, enhancing overall plant monitoring and control efficiency [4].

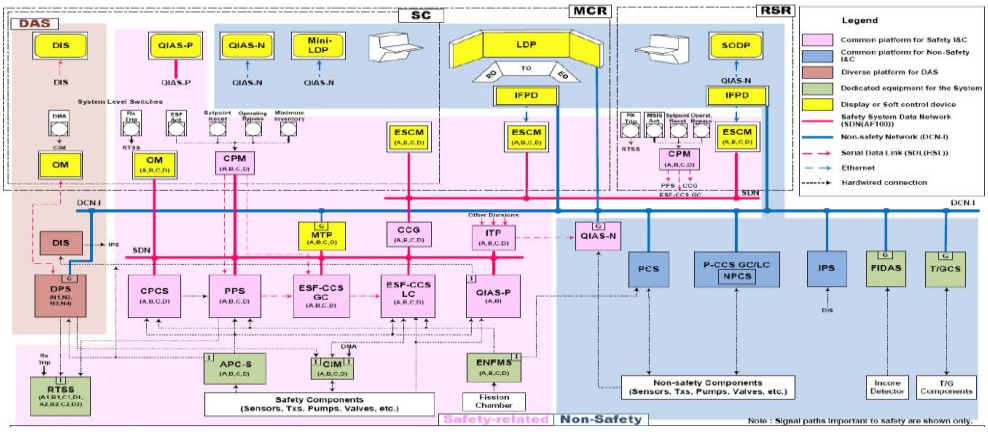


Figure 1. Overview of the digital system.

Recent cybersecurity research has predominantly focused on safety systems like the Plant Protection System (PPS), which are essential for the safe shutdown and protection of nuclear power plants. These systems are critical as they directly influence the plant's operational integrity during emergency situations. However, attention must also be given to non-safety systems, such as the Divers Protection System (DPS). DPS, while classified as non-safety, has the capability to initiate plant shutdowns depending on its functionality. The potential for cyber-attacks to exploit vulnerabilities or induce physical malfunctions in the DPS control system is a matter of significant concern. Such vulnerabilities could prevent the DPS from functioning correctly during critical shutdown phases, posing a substantial risk of severe incidents. As digital systems have increasingly incorporated into NPPs, the importance of securing both safety and non-safety systems against cyber threats becomes paramount to ensuring overall plant safety.

B. *The Need for the Design and Testing Technology of Nuclear Power Plant Cyber Threat Response Systems*

As cyber intrusion attempts increase, government and public agencies are strengthening their cyber crisis response systems by establishing or expanding dedicated information security teams and conducting cyber-attack response drills [5]. These drills require the development of cyber-attack detection technologies based on intelligent information technology, enabling responses to evolving threats. Modern cyber-attacks are highly sophisticated, involving complex actions, such as control logic manipulation, sensor signal tampering, and HMI display alterations. Detection of such attacks cannot rely solely on IT security measures; nuclear power plants require specialized detection technologies tailored to their systems. Current industrial security measures are insufficient for detecting and countering these advanced cyber threats.

To develop effective detection systems for nuclear power plants, it is essential to conduct research on identifying data available for system and device-specific detection based on nuclear instrumentation and control systems. Additionally, selecting appropriate detection methods and analyzing and verifying detection performance for potential cyber-attacks on the target systems and devices are crucial.

III. CYBER THREAT RESPONSE SYSTEM DESIGN AND TEST ENVIRONMENT

Figure 2 illustrates the configuration of a Nuclear Power Plant digital instrumentation and control (I&C) system [7]. As observed in the figure, while the nuclear power plant digital I&C system does operate some general PCs and servers commonly used in IT, it predominantly utilizes industrial equipment, such as Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), industrial PCs, and industrial networks. Therefore, directly applying existing cyber security threats identified for general IT systems to this specialized environment is not suitable.

To identify cyber security threats applicable to the nuclear power plant digital I&C system, a comprehensive approach is required. This involves comparing and analyzing the research results and security guidelines on cyber security threats identified in both IT and Industrial Control Systems (ICS). Additionally, an in-depth analysis of the specific functions and characteristics of the target system must be conducted. Based on these analyses, cyber security threats relevant to the nuclear power plant environment can be derived. In nuclear power plants, ensuring the continuous operation and safety of the plant is of utmost importance. This leads to a robust design where safety systems are isolated from any potential vulnerabilities that could arise from communication uncertainties. By adopting a deterministic communication structure, the systems are able to operate with high reliability, ensuring that all commands and data transmissions occur in a predictable and controlled manner. This approach minimizes the risk of unexpected behaviors or failures in the safety-critical functions of the plant, thereby enhancing the overall security and resilience of the nuclear power plant's operations.

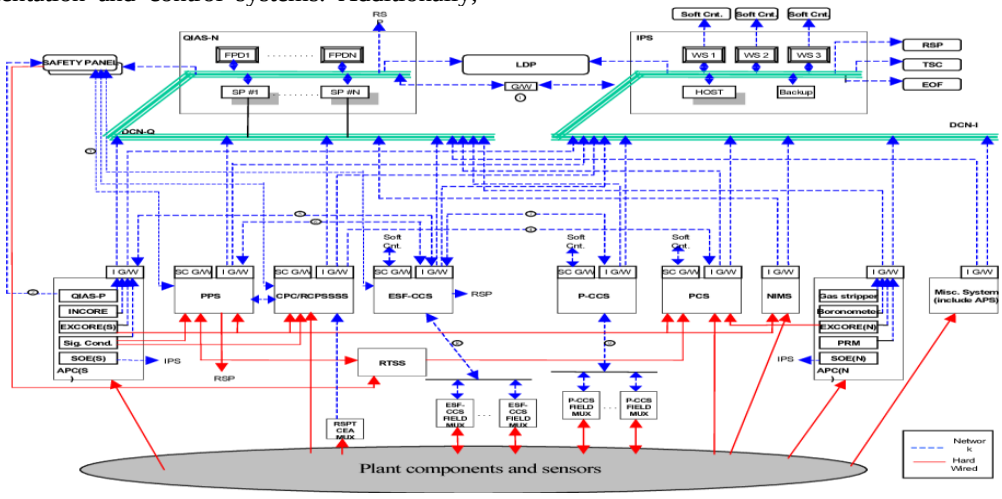


Figure 2. Configuration of a nuclear power plant digital I&C system.

A. *Cyber Threat Response System Design*

The development targets for configuring the cyber threat response system for nuclear power plants are as follows:

- Development of Safety System Applications for Nuclear Power Plants: Design and development of applications for the safety system. Development of simulation applications for normal and abnormal data of the safety system.
- Development of Non-Safety System Applications for Nuclear Power Plants: Design and development of applications for the non-safety system. Development of simulation applications for normal and abnormal data of the non-safety system.
- Design of Cyber Threat Response System: Design and development of the Man Machine Interface Systems (MMIS) cyber threat response system. Development of a system that provides operators with information on threat responses for both safety and non-safety systems in the System Status Overview (SSO) of the MMIS.
- Construction of On-Site Normal/Abnormal Big Data: Design and development of the big data server and interface (REST) for the MMIS. Storage of normal and abnormal state data for both safety and non-safety systems of the MMIS in a database server and development of an interface (REST) for AI learning.
- Development of Test/Verification Technology: Development of abnormal state scenarios through MMIS cyber threats. Development of a system for comparing data of abnormal states induced by MMIS cyber threats with normal state data. Development of a system for comparing simulated data of safety and non-safety systems with database data in the MMIS.

B. *Cyber Threat Response System Test Environment*

Figure 3 shows the configuration of the cyber threat response system design and test environment setup. As illustrated in the figure, the signal simulator is configured to simulate scenario-based input and output signals. The on-site Nuclear Power Plant big data is established using the Testbed owned by the Korea Atomic Energy Research Institute (KAERI), and for the latest non-safety systems not included in the Test-Bed, the big data is constructed using the RTP controller applied to the Shin-Kori Units 5 and 6 CDMS systems.

Experiments for building the on-site Nuclear Power Plant big data are conducted in accordance with KAERI's strict security regulations. Key data from safety and non-safety systems can be simulated as packet signals by developing application software. These packet signals are then used to perform network-based and process-based detection in conjunction with the cyber threat response detection engine server.

The signal simulator reproduces input and output signals based on various scenarios that may occur in the actual operating environment, thus verifying the stability and reliability of the system. This helps ensure that the system operates correctly even in unexpected situations.

Additionally, the on-site Nuclear Power Plant big data construction includes both normal and abnormal state data of the plant, which is used for AI learning and analysis. This data plays a critical role in enhancing the operational efficiency of the plant and applying advanced operational techniques, such as predictive maintenance.

Key data from safety and non-safety systems is converted into network packet signals and analyzed in real-time by the cyber threat detection engine. This process involves both network-based detection and process-based detection, enabling the rapid identification and response to potential cyber threats.

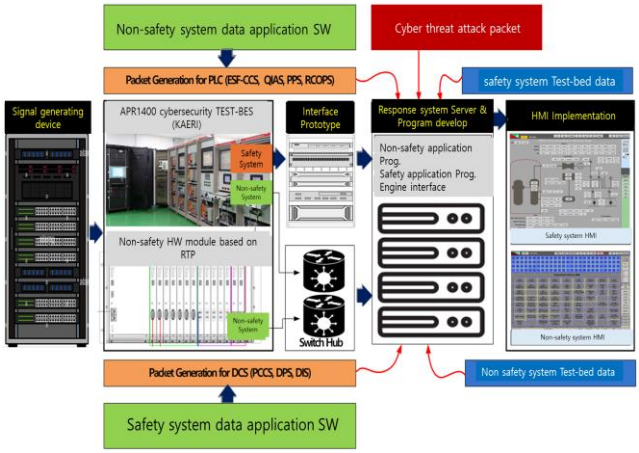
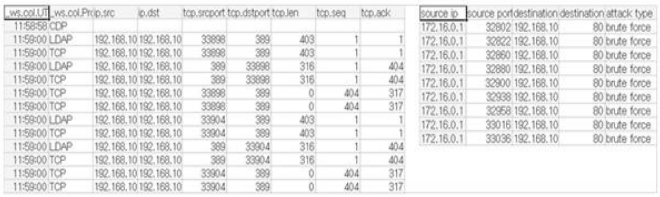


Figure 3. Cyber threat test environment.

C. *Investigation and Analysis of Big Data Utilized in Cyber Threat Response Systems*

Figure 4 shows the Information security Research and Development dataset. The data for cyber threats was utilized by investigating and analyzing the dataset used in the "Network Threat Detection" track of the security challenge competition. Various data were generated and shared according to different purposes, configurations, and network types.



ws.col.Utc	ws.col.Prop.src	ip.dst	tcp.srcport	tcp.dstport	tcp.len	tcp.seq	tcp.ack
11:58:58 CDP							
11:59:00 LDAP	192.168.10	192.168.10	33898	389	403	1	1
11:59:00 TCP	192.168.10	192.168.10	33898	389	403	1	1
11:59:00 LDAP	192.168.10	192.168.10	389	33898	316	1	404
11:59:00 TCP	192.168.10	192.168.10	389	33898	316	1	404
11:59:00 TCP	192.168.10	192.168.10	33898	389	0	404	317
11:59:00 TCP	192.168.10	192.168.10	33898	389	0	404	317
11:59:00 LDAP	192.168.10	192.168.10	33904	389	403	1	1
11:59:00 TCP	192.168.10	192.168.10	33904	389	403	1	1
11:59:00 LDAP	192.168.10	192.168.10	389	33904	316	1	404
11:59:00 TCP	192.168.10	192.168.10	389	33904	316	1	404
11:59:00 TCP	192.168.10	192.168.10	33904	389	0	404	317
11:59:00 TCP	192.168.10	192.168.10	33904	389	0	404	317

Source ip	source port	destination ip	destination port	attack type
172.16.0.1	32802	192.168.10	80	brute force
172.16.0.1	32822	192.168.10	80	brute force
172.16.0.1	32860	192.168.10	80	brute force
172.16.0.1	32880	192.168.10	80	brute force
172.16.0.1	32900	192.168.10	80	brute force
172.16.0.1	32938	192.168.10	80	brute force
172.16.0.1	32958	192.168.10	80	brute force
172.16.0.1	33016	192.168.10	80	brute force
172.16.0.1	33036	192.168.10	80	brute force

Figure 4. Information security R&D dataset.

TABLE I. VARIOUS NETWORK DATASETS

dataset	Normal traffic	Attack traffic	Meta data	feature	count	Traffic kind	attack
AWID	yes	yes	yes	other	37M packets	emulated	802.11 attack (authentication request, ARP flooding, injection, probe request)
Booters	no	yes	no	packet	250GB packets	real	DDoS attack 9
Botnet	yes	yes	yes	packet	14GB packets	emulated	botnet (Menti, Murlo, Neris, NSIS, Rbot, Sogou, Strom, Virut, Zeus)
CIC DoS	yes	yes	no	packet	4.6GB packets	emulated	application layer Dos attack (executed through ddossim, Goldeneye, hulk, RUDY, Slowhttptest, Slowloris)
CICIDS 2017	yes	yes	yes	packet, bi. flow	3.1M flows	emulated	botnet (Ares), XSS, DoS (executed through Hulk, GoldenEye, Slowloris, and Slowhttptest), DDoS (executed through LOIC), heartbleed, infiltration, SSH brute force, SQL injection
CIDDS-001	yes	yes	yes	uni. flow	32M flows	emulated and real	DoS, port scans (ping-scan, SYN-Scan), SSH brute force
CIDDS-002	yes	yes	yes	uni. flow	15M flows	emulated	port scans (ACK-Scan, FIN-Scan, ping-Scan, UDP-Scan, SYN-Scan)
CTU-13	yes	yes	yes	uni. and bi. flow, paket	81M flows	real	botnet (Menti, Murlo, Neris, NSIS, Rbot, Sogou, Virut)
ISCX 2012	yes	yes	yes	packet, bi. flow	2M flows	emulated	Attack scenario 4
ISOT	yes	yes	yes	packet	11GB packets	emulated	botnet (Storm, Waledac)
KDD CUP 99	yes	yes	no	other	5M points	emulated	DoS, privilege escalation (remote-to-local and user-to-root), probing
Kyoto 2006+	yes	yes	no	other	93M points	real	Honney pot attack (backscatter, DoS, exploits, malware, port scans, shellcode)
LBNL	yes	yes	no	packet	160M packets	real	port scans
NDSec-1	no	yes	no	packet, logs	3.5M packets	emulated	botnet (Citadel), brute force (against FTP, HTTP and SSH), DDoS (HTTP floods, SYN flooding and UDP floods), exploits, probe, spoofing, SSL proxy, XSS/SQL injection
NSL-KDD	yes	yes	no	other	150k points	emulated	DoS, privilege escalation (remote-to-local and user-to-root), probing
PU-IDS	yes	yes	no	other	200k points	synthetic	DoS, privilege escalation (remote-to-local and user-to-root), probing
SANTA	yes	yes	no	other	n.s.	real	(D)DoS (ICMP flood, RUDY, SYN flood), DNS amplification, heartbleed, port scans
SSENET-2011	yes	yes	no	other	n.s.	emulated	DoS (executed through LOIC), port scans (executed through Angry IP Scanner, Nessus, Nmap), various attack tools (e.g. metasploit)
TRAbID	yes	yes	no	packet	460M packets	emulated	DoS (HTTP flood, ICMP flood, SMTP flood, SYN flood, TCP keepalive), port scans (ACKScan, FIN-Scan, NULL-Scan, OS Fingerprinting, Service Fingerprinting, UDP-Scan, XMAS-Scan)
TUIDS	yes	yes	no	packet, bi. flow	250k flows	emulated	botnet (IRC), DDoS (Fraggle flood, Ping flood, RST flood, smurf ICMP flood, SYN flood, UDP flood), port scans (FIN-Scan, NULL-Scan, UDP-Scan, XMAS-Scan), coordinated port scan, SSH brute force
Twente	no	yes	yes	uni. flow	14M flows	real	Open service (FTP, HTTP, SSH) honey pot attack
UGR 2016	yes	yes	some	uni. flow	16900M flows	real	botnet (Neris), DoS, port scans, SSH brute force, spam
Unified Host and Network	yes	n.s.	no	bi. flows, logs	150GB flows (compressed)	real	n.s.
UNSW-NB15	yes	yes	yes	packet, other	2M points	emulated	backdoors, DoS, exploits, fuzzers, generic, port scans, reconnaissance, shellcode, spam, worms

D. Analysis of Scenarios for Generating Normal/Abnormal Cybersecurity Data

Normal/abnormal cybersecurity data will be generated through other projects. In order to support the simulation of cybersecurity normal/abnormal data scenarios in the Testbed being built through this project, communication protocols of safety and non-safety systems, as well as configuration information of CPU and IO modules, will be analyzed. This analysis will provide the requirements for the Packet Generator that is planned to be developed.

- The communication protocols for the safety system and DPS are as follows: Physical Layer (Ethernet), Transport Layer (UDP-Unicast), Application Layer (IPS Standard).
- The communication protocols for the non-safety system and DPS are as follows: Physical Layer (Ethernet), Transport Layer (UDP-Unicast), Control Network Transport Layer (TCP/IP), Information Network (UDP-broadcast), Application Layer (DCS Vendor protocol).

Within the CPU and IO module configuration information, there are types of simulated data for both safety system signals and non-safety system signals. The process monitoring data for safety systems requires signal provision

by system and node, while state monitoring data requires provision by system and channel. Similarly, process monitoring data for non-safety systems requires signal provision by system and node, and state monitoring data requires provision by system and node. The Packet Generator implements status monitoring data (SSO DB) and class bit information (Class bit Info) for each system.

When analyzing attacks that induce abnormal data and identifying intrusion indicators, the detection of cyber threats is broadly divided into host-based detection and network-based detection. Representative intrusion indicators for both detection methods are illustrated in Table II.

TABLE II. INTRUSION INDACATORS

Category	***Intrusion Indicators***
Host based indicator	Registry key
	File name
	Test string
	Process name
	Mutex
	File hash value
	User account
	Directory path
Network based indicator	IPv4 address
	IPv6 address
	X509 authentication hash value
	Domain name
	Test string
	Communication protocol
	Fil name
	URL

IV. CONCLUSION AND FUTURE WORK

The cyber threat detection system proposed in this paper can be utilized as the technical security measures of cybersecurity plan for NPPs. This system allows for continuous and in-depth response to cyber threats beyond traditional access restriction and prevention strategies. It supports operator' response to cyber threats by integrating with nuclear emergency procedures. Additionally, it enables the acquisition of intelligent information technology-based cyber-attack detection techniques capable of countering sophisticated and intelligent cyber-attacks. This technology can be also applicable to other various areas, such as small modular reactors and nuclear systems in space, polar, and marine environments.

The systematic and consistent development and application of nuclear cybersecurity technologies and devices can enhance the safety, reliability, and operational performance of nuclear power plants. By leading the development of nuclear cybersecurity technologies, which are not yet internationally established, the developed technologies will improve capabilities to detect and respond cyber-attacks in an effective and efficient way for NPPs.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021M3C1C4039576).

REFERENCES

[1] WIRED, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. Accessed: Nov. 3, 2014 .

[2] International Atomic Energy Agency, *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook*, IAEA, 1999.

[3] Kaspersky ICS CERT, "Threat landscape for industrial automation systems, H2 2019," Kaspersky Lab, 2019.

[4] APR1400 Design Control Document, *Tier 1*, vol. 7, NRC, 2018.

[5] Republic of Korea, *National Cybersecurity Strategy*. Published Aug. 2, 2024.

[6] University of California, Berkeley, *Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies*, Sep. 2017, doi:10.13140/RG.2.2.34430.69449.

[7] GENES4/ANP2003, "Advanced MMIS design characteristics of APR1400," presented at GENES4/ANP2003, Kyoto, Japan, Sep. 15-19, 2003.

[8] IAEA, *Computer Security at Nuclear Facilities*, IAEA Nuclear Security Series No. 17, Technical Guidance, 2011.

[9] International Atomic Energy Agency, "Computer Security Incident Response Planning at Nuclear Facilities TDL005 (NST-038)," 2016.

[10] U.S. Nuclear Regulatory Commission (U.S. NRC), *Regulatory Guide 5.71 (R.G 5.71): Cyber Security Programs for Nuclear Facilities*, 2010.

[11] Nuclear Energy Institute (NEI), *NEI 08-09 (Rev. 6): Cyber Security Plan for Nuclear Power Reactors*, 2010.