Technological Trends and Challenges for Detecting and Responding to Cyber Threats in NPP I&C Systems: A Literature Review.

Jae Hwan Kim [a], Gwang Seop Son [b*], Jeong Woon Lee [b], Jae Gu Song [b], In Koo Hwang [c], Chul Kwon Lee [c],

[a]*Multi-purpose Small Reactor System Develop Div., Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon 305-353, Republic of Korea*
[b]*Security R&D Section, Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon 305-353, Republic of Korea*
[c]*Advanced Control Research Section, Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon 305-353, Republic of Korea*
[*]*Corresponding author: ksson78@kaeri.re.kr*

1. Introduction

In recent years, there has been a noticeable increase in the complexity and intelligence of cyber threats targeting industrial control systems (ICS). These attacks are often sustained over an extended period and are becoming more sophisticated. As cyber threats continue to evolve, it is essential to develop cybersecurity technologies capable of detecting and responding to these threats in domestic nuclear power plants. To address this need, KAERI is developing specialized detection and response technology for nuclear power plant instrumentation and control (I&C) systems through research and development. This paper investigates the trends in cyber threat detection technology for industrial control systems to develop effective cyber threat detection and response technology for nuclear power plant I&C systems.

2. Literature Review

2.1 Risks of Cyber Threats to ICS in National Infrastructure

The components that comprise the instrumentation and control (I&C) system of a nuclear power plant can be considered a type of industrial control system. These systems are widely used in various fields and are integral to national infrastructure such as telecommunications, finance, transportation, power plants, and more. Consequently, cyber threats targeting these systems can result in more than just physical damage; they can also cause substantial economic harm and social disruption. In the past, early ICS were considered relatively safe from external attacks by organizing independent networks and physically blocking connections to external networks. However, with the development of IT technology in recent years, the system has gradually shifted from a closed environment to an open technology that connects to the external network for efficient control and management. As a result, the possibility of being exposed to various cyber-attacks from the outside is increasing, and attack methods are diversifying.

2.2 Requirement for ICS Security

Security requirements for industrial control systems significantly differ from those of traditional IT systems. While security in traditional IT systems aims to prevent unauthorized individuals or organizations from accessing, modifying, stealing, or compromising personal or sensitive data, security in industrial control systems primarily focuses on safety. Its goal is to prevent hardware or software failures from causing harm to plant safety, public safety, and property. The security requirements of industrial control systems can be characterized by the following features:

- Real-time operation
- Limited computing resources
- Inflexible business logic
- Dependence on legacy systems
- Difficulty in updating and restarting industrial equipment
- Security vulnerabilities in industrial protocols

2.3 Classification of Intrusion Detection Systems (IDS) for ICS

Intrusion detection systems are crucial for securing industrial control systems, but the existing systems designed for traditional IT systems have limitations. Intrusion detection systems for industrial control systems can be categorized by detection technique or data source. Misuse-based systems identify known attacks by comparing system information with known signatures, while anomaly-based systems compare current behavior to normal patterns. Data sources can be network-based or host-based. Network-based systems analyze network communication data but may have difficulty identifying the source of an attack, while host-based systems monitor specific hosts for intrusive behavior [1].

New classification methods for intrusion detection in industrial control systems can be categorized into three types: protocol analysis-based, traffic mining-based, and control process analysis-based. The first two types primarily analyze network traffic data, while the third type utilizes knowledge of control systems and physical processes to detect attacks. Protocol analysis-based detection depends on the accuracy of the detection rules and can have a high false positive rate. Traffic mining-

based detection defines complex relationships between traffic and system behavior to detect attacks. However, both of these methods have weaknesses that can be exploited by attackers. Control process analysis-based detection, on the other hand, uses process data, control commands, and physical models to detect intrusions, making full use of the unique information and characteristics of industrial control systems [2].

2.4 Trends in Cyber Threat Detection Technology for ICS

J. Giraldo et al. have developed techniques for detecting cyber-physical system (CPS) attacks based on physical phenomena. They used a time series model of sensor readings to identify anomalies [3]. R. Mitchell et al. categorized CPS intrusion detection system techniques based on cyberattack detection techniques and attack triage data, emphasizing the importance of quickly detecting cyberattacks [4]. Rubio et al. analyzed existing intrusion detection systems in industrial systems and recommended combining various solutions due to the diversity of process components and protocols [5]. Y. Hu et al. presented a new classification method for intrusion detection systems in industrial control systems and discussed the need for a cybersecurity strategy that satisfies safety and security requirements in modern smart plants [6].

3. Conclusions

This paper reviews the development trends of cyber threat detection systems for industrial control systems with the goal of developing cyber threat detection and response technologies for nuclear power plant I&C systems. Through a literature survey, the unique security requirements of industrial control systems were identified, and the advantages and disadvantages of various intrusion detection systems were analyzed. Based on the results of this technology trend analysis, various approaches and methodologies for developing specialized cyber security threat detection technology for NPP I&C systems can be referenced.

REFERENCES

[1] M. Bijone, A Survey on Secure Network: Intrusion Detection & Prevention Approaches, American Journal of Information Systems, Vol.4, p. 69-88, 2016.
[2] S. Anwar, J. Zain, M. Zolkipli, Z. Inayat, S. Khan, B. Anthony and V. Chang, Analysis of Intrusion Detection Systems in Industrial Ecosystems, Journal of Algorithms, 2017.
[3] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. Tippenhauer, H. Sandberg and R. Candell, A Survey of Physics-Based Attack Detection in Cyber-Physical Systems, ACM Computing Surveys, Vol.51, p. 1-36, 2018.
[4] R. Mitchell, I. Chen, A Survey of Intrusion Detection Techniques for Cyber-physical Systems, ACM Computing Surveys, Vol.46, p. 1-29, 2014.
[5] J. Rubio, C. Alcaraz, R. Roman and J. Lopez, Analysis of Intrusion Detection Systems in Industrial Ecosystems, Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017), Vol.4, p. 116-128, 2017.
[6] Y. Hu, A. Yang, H. Li and L. Sun, A Survey of Intrusion Detection on Industrial Control Systems, International Journal of Distributed Sensor Networks, Vol.14, Issue.8, 2018.