JTAG Interface-Based Hardware Lock Key for Cyber Intrusion Detection in Nuclear Power Plant Control Modules

Chan Yeong Woo [a*], Je Seok Lee [a], Min Hyuk Yoon [a], Gi Ho Cho [a], Dong-Yeon Lee [a]
[a] *SOOSAN ENS Co., Soosan Building 2F, 13, Bamgogae-ro 5-gil, Gangnam-gu, Seoul, Korea, 06367*
[*] *Corresponding author: wcy0213@soosan.co.kr*

***Keywords :** Cybersecurity, JTAG Interface, Hardware Lock Key, Nuclear Power Plant

1. Introduction

The accelerated digitalization of the nuclear industry has led to an increase in cybersecurity threats. Cyberattacks on nuclear systems have been rising, posing significant risks of severe safety incidents in the event of unauthorized access [1]. Consequently, a hardware-level security system is required to complement existing software-based security mechanisms.

This study proposes a security system utilizing a hardware Lock Key integrated with the JTAG interface to prevent unauthorized use and access to control modules. The hardware Lock Key, embedded with a unique identifier (ID), enhances the security of the program download process. When the hardware Lock Key transmits a specific signal to the module, the module responds with a control signal before the JTAG interface enables the program download. Furthermore,. The module logs the Lock Key ID, port status, and download attempts in real time.

2. Background and Concept of Hardware Lock Key Development

2.1 Background

Globally, nuclear power plants (NPPs) are designed to isolate their instrumentation and control (I&C) systems from external networks to eliminate the possibility of remote cyberattacks. Additionally, newly designed nuclear power plants implement enhanced physical security, strict access controls, and a Defense-in-Depth strategy to mitigate cybersecurity threats [2].

However, such measures have limitations in preventing physical attacks or unauthorized access by insiders. To address these vulnerabilities, this study incorporates an FPGA-based security system using a hardware Lock Key, providing protection against physical hacking and unauthorized modifications. This approach strengthens the cybersecurity framework of nuclear power plants by enabling intrusion detection and response mechanisms.

2.2 Concept and Functionalities of the Hardware Lock Key

The hardware Lock Key is a security device integrated with the JTAG interface to enhance the security of the program download process (refer to Fig. 1). It contains a unique identification (ID) and regulates access through a structured authentication procedure when physically connected to a module. Specifically, when the hardware Lock Key transmits an authentication signal to the module, the module verifies the signal and returns a control signal to the hardware Lock Key before permitting program downloads via the JTAG interface.

The hardware Lock Key's unique ID is used to log access attempts, monitor port connection status, and record unauthorized access attempts. Upon connection, the module recognizes the hardware Lock Key and continuously logs related access events in real-time. These access logs allow administrators to periodically analyze access records, detect abnormal access attempts, and verify unauthorized device usage.

This system effectively blocks unauthorized access and prevents program downloads from unapproved devices while providing a foundation for post-event cybersecurity incident management.

Fig. 1 illustrates the authentication and communication process between the hardware Lock Key and the target module. The FPGA activates the JTAG interface only when the connected device is identified as a hardware Lock Key and controls communication between the external PC and the module.

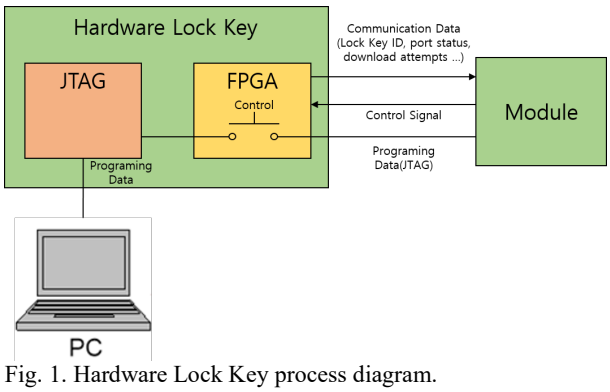

Fig. 1. Hardware Lock Key process diagram.

3. Conclusions

This study presents a concept for a cyber intrusion detection system under development, which

incorporates a hardware Lock Key integrated with the JTAG interface to address cybersecurity vulnerabilities in nuclear power plant control modules. Conventionally, the presence of a JTAG interface alone has allowed unrestricted access to critical systems, exposing them to physical and insider threats. The proposed system introduces a hardware-based access control mechanism, wherein authentication between the hardware Lock Key and the target module is required prior to enabling program download through the JTAG interface.

The design includes the assignment of a unique identifier to each Lock Key, enabling real-time logging of access attempts, connection status, and device identity. These features provide the foundation for monitoring and detecting unauthorized access at the hardware level. The system is currently under continuous development with the goal of implementing and validating its functionalities within control environments, and is expected to serve as a foundational technology for strengthening cybersecurity frameworks in nuclear power plants.

REFERENCES

[1] de Brito, I. B & de Sousa Jr, R. T., Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants, Applied Sciences, 12(15), 7942, 2022.

[2] CheolKwon Lee., Trends in Cybersecurity Technology for Nuclear Power Plant Instrumentation and Control Systems, Korea Institute of Information Security and Cryptology, 2012.

[3] Elakrat, M. A & Jung, J. C., Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network, Nuclear Engineering and Technology, 50(5), 780-787, 2018.

[4] Kumar, N., Mishra, V. M., & Kumar, A., Smart grid and nuclear power plant security by integrating cryptographic hardware chip, Nuclear Engineering and Technology, 53(10), 3327-3334, 2021.