FPGA-Based JTAG Interface Gating with Hardware Key and Device DNA Authentication for Secure Maintenance of Nuclear I&C Control Modules

Chan Yeong Woo [a*], Je Seok Lee [a], Min Hyuk Yoon [a], Yeong Ik Son [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

As the digitalization of instrumentation and control systems in nuclear power plants expands, both the number of assets requiring protection and the overall attack surface continue to grow. In a digitalized nuclear environment, vulnerabilities may arise not only from direct network intrusion but also from multiple pathways, including PLC engineering routes, sensor and actuator signal paths, and indirect propagation routes involving human factors and the supply chain. A systematic understanding of these potential propagation paths and corresponding controls is therefore necessary [1]. Cyber threats in the nuclear domain can lead to physical consequences by altering control functions or inducing unintended behavior, rather than remaining limited to information compromise. This characteristic calls for approaches that differ from conventional IT security. Recent work classifies cyberattack scenarios by physical impact and links them to initial events in probabilistic risk assessment (PRA), enabling integrated treatment of cyber–physical risk [2].

In this context, this study focuses on the exposure of hardware interfaces, particularly JTAG, that may be abused during maintenance and program download activities for nuclear plant control modules. We propose a hardware-level access control logic that integrates a hardware lock key, device DNA authentication as a unique identifier, and encrypted MCS-based download control.

2. Development Background and Concept of the Proposed Security Logic

2.1 Development Background

Digital I&C systems in nuclear power plants are often designed with network separation to reduce remote intrusion opportunities. However, during maintenance and testing in operating environments, external digital devices such as laptop-based engineering workstations and removable media can be connected to critical digital assets, and this connection process itself may serve as an attack vector [3]. Accordingly, program download and debug interfaces used in maintenance environments introduce risk at the moment they are connected. This motivates hardware-level access control that can structurally exclude unauthorized devices and media during on-site work.

2.2 Architecture and Operating Concept

The proposed logic deliberately separates enabling JTAG access from establishing actual communication and download capability. The overall application process is divided into an initial provisioning phase and an operational maintenance phase, and the authentication and download conditions required in each phase are explicitly defined. Figure 1 conceptually illustrates the authentication and download flow among the maintenance PC, the hardware lock key, and the controller.

2.2.1 Default Deny Policy

During normal operation, the control module keeps the JTAG interface locked by default. Gateway logic, such as an FPGA, blocks the JTAG signal path so that connecting an unauthorized PC or device does not immediately enable download or debugging communication. This provides a first layer of restriction against accidental access and simple connection attempts before maintenance procedures begin.

2.2.2 Maintenance PC and Hardware Lock Key Authentication

To initiate maintenance, authentication must first be completed between the maintenance PC and the hardware lock key. Only upon successful authentication are the conditions required to proceed toward JTAG access established, preventing access by unapproved tool and media combinations. This stage functions as a practical control point to validate the legitimacy of field equipment.

2.2.3 Initial Provisioning with Encrypted Download Mode and eFuse Programming

During initial provisioning, an encrypted download mode is used to program an encrypted MCS file into the eFuse region. This procedure establishes an internal trust baseline for subsequent operation and reduces the likelihood of unauthorized configuration or abnormal image injection during installation and registration. The initial setup process is therefore structured to proceed only on the basis of an encrypted MCS file.

2.2.4 Operational Phase with Device DNA Authentication for Physical Connection Control

After provisioning, the operational phase performs device DNA authentication between the hardware lock key and the controller. Only when authentication succeeds does the gateway logic physically connect JTAG and related communication lines, allowing practical communication to be established. When authentication fails, the signal path remains disconnected, preventing actual communication and download even if other preliminary conditions appear to be met.

2.2.5 Encrypted MCS-Based Download Control for Update Restriction

A key feature of the proposed logic is that opening the JTAG path does not by itself permit new downloads or updates. Updates are allowed only when an encrypted MCS file is provided and the encryption and verification conditions are satisfied. Files that fail to meet these conditions are rejected during download or application, thereby suppressing unauthorized image injection. As a result, even if an on-site actor temporarily obtains JTAG access conditions, an MCS update cannot be completed without an officially approved encrypted file.

2.2.6 Logging of Access Attempts for Detection and Post-Event Analysis

The control module records port connection status, the results of maintenance PC and lock key authentication, the results of device DNA authentication, and download attempt outcomes. These logs can support detection of anomalies such as repeated failures, unusual-time access attempts, and unauthorized device patterns, and can also be used for post-event analysis and improvement of operational policies.

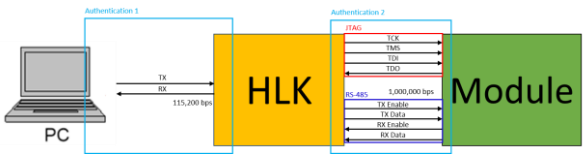

Fig. 1. Hardware Lock Key Authentication and Communication process diagram.

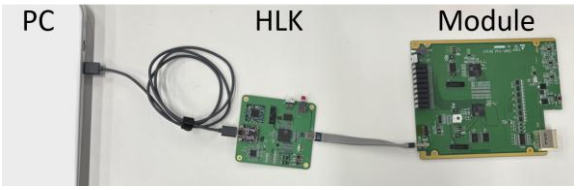

Fig. 2. Photograph of the prototype setup

3. Conclusions

This study proposes a hardware-level access control and download control logic for JTAG interfaces in nuclear power plant control modules, with emphasis on physical access and insider threat scenarios. The logic locks JTAG by default and forms maintenance access conditions through maintenance PC and hardware lock key authentication. During initial provisioning, an encrypted MCS file is programmed into eFuse using an encrypted download mode to establish a device-internal trust baseline. During operation, practical communication is enabled only when device DNA authentication succeeds, by physically connecting JTAG and related communication lines through gateway logic. In addition, MCS updates remain restricted to encrypted and verified files even when JTAG is opened, reducing the risk of unauthorized image injection. The design also supports intrusion detection and post-event analysis by logging access, authentication, and download attempts.

Future work will implement and validate the logic in representative control environments to assess operational feasibility and reliability. The study will also refine application scenarios, including key management and device registration and decommissioning procedures, to extend the approach into a hardware-based security framework suitable for nuclear control environments.

REFERENCES

[1] Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I., & Ahmed, H., Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors., Progress in Nuclear Energy, 161, 104738, 2023.
[2] Yoo, S., & Zhang, F., Cybersecurity initial events of digital instrumentation and control systems using physical accident scenarios., Annals of Nuclear Energy, 227, 111926, 2026.
[3] Song, J. G., Lee, J. W., Park, G. Y., Kwon, K. C., Lee, D. Y., & Lee, C. K., An analysis of technical security control requirements for digital I&C systems in nuclear power plants., Nuclear Engineering and Technology, 45(5), 637-652, 2013.