Cyber Security Function through Physical Access of Safety Level Controller Digital Output Module

Hyo-Jin Kim [a]*,Kwan-woo Yoo*, Jae-won Yun*, Dong-Yeon Lee*
[a] *SOOSAN ENS Co., Hyundai Venture Ville 3F 301, 10, Bamgogae-ro 1-gil, Gangnam-gu, Seoul, 06349, Korea*
**Corresponding author : rlagywls450@soosan.co.kr*

1. Introduction

The nuclear facility's measurement and control system uses digital-based technology. Cyber attacks such as hacking or unauthorized access(unwanted behavior and careless access) to nuclear facilities are increasing by exploiting the vulnerabilities of digital technology. In the case of nuclear facility accidents, it is a serious accident that can lead to global disasters beyond national disasters. Therefore, there is a need to strengthen cyber security.

Korea Institute of Nuclear Safety (KINS) enforces regulations based on the SDOE (Secure Development and Operating Environment). SDOE can be divided into SDE and SOE. First, SDE ensures that unwanted, unneeded, and undocumented features are not included. Second, the SOE is physical, logical, and administrative control to ensure that the reliability operation of the system is not impaired for events that may occur due to unauthorized access of the connected system.

This paper proposes a digital output module (hereinafter referred to as a digital output module) of a safety class controller that adds a SOE-based physical cyber security function as a way to prevent cyber attacks on nuclear facilities. And describe the test process to confirm the function.

2. Cyber security function through physical access

Since the firmware of the digital output module is input to the FPGA at the time of module manufacture, there is no function to prevent unauthorized actions. Therefore, by adding the hardware security key(hereinafter referred to as H / W security key), user setting key, JTAG connection status(hereinafter referred to as JTAG) to the digital output module, the cyber security function for physical access was implemented. H / W security key, user setting key, and JTAG are defined as three elements for physical access. If any of the 3 elements is not physically connected or does not match the set value, connection is not possible. This was based on physically controlling the SOE's unauthorized access.

The digital output module must match all 3 elements to access the firmware. In addition, in case of unauthorized access, the module is notified through the LED of the manager.

3. Environment for testing

3.1. Configuration for testing

A digital output module, a power module, a processor module, and a power supply are required to perform the test. A logic analyzer, a monitoring program, and VIVADO are required to check the accessibility according to the three factors. Therefore, HOST-PC must have a monitoring program, VIVADO installed.
The test environment is shown in Figure 1. The three elements of the digital output module are shown in Figure 2. And Figure 2 shows all cases of normal access.

Fig. 1. Test environment

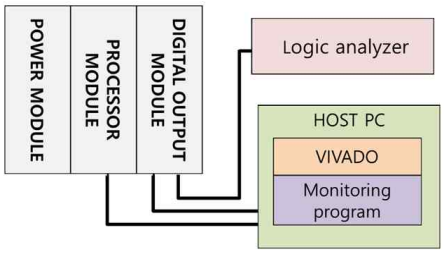
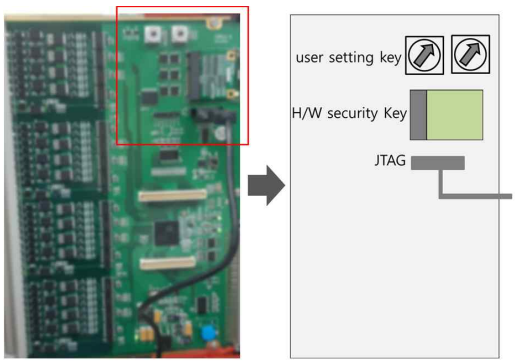


Fig. 2. Three elements of the NQ-D23QC's normal access



3-2 Three-element Applicable signal meaning

The H / W security key and user setting key correspond to key_ok_n in the logic analyzer. In the monitoring program, it corresponds to the fifth bit of %MW 2.59. Both H / W security key and user setting key are recognized as normal access only in the case of normal access. Table I shows the meaning of H / W security key and user setting key.

Table I: Meaning according to the signal of H / W security key and user setting key

H / W security key, User setting key	Logic analyzer	Monitoring program
Normal access	Low	1
Unauthorized access	High	0

Jtag corresponds to download_con [0], download_con [1], and download_con [2] in Logic Analyzer. When JTAG is not connected, it remains high. In case of connection status, data is transmitted. Also, JTAG is the sixth bit of %MW 2.59 in the monitoring program. In the monitoring program, 0 for unconnected status and 1 for connected status.

The LED indicating normal access corresponds to RUN in the logic analyzer. The LED indicating the unauthorized access corresponds to FAULT in the logic analyzer. The normal access and unauthorized access correspond to the first bit of %MW 2.56 in the monitoring program. Table II shows the meanings of RUN and FAULT signals.

Table II: Meaning according to the signal of RUN and FAULT

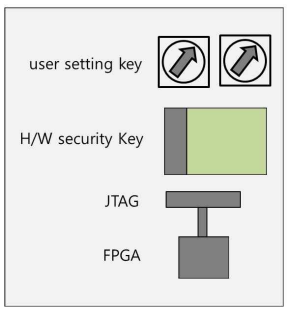
RUN, FAULT	Logic analyzer	Monitoring program
normal access	RUN: High('1') FAULT: Low('0')	0
Unauthorized access	RUN : Blinking FAULT : Blinking	1

4. Test process and results

4-1. All three elements are normal access

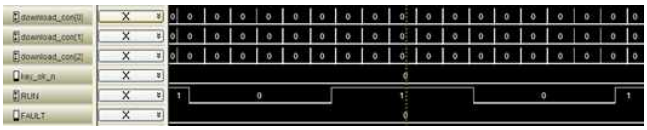
Access to H / W security key normal (H / W security key value matching, H / W security key installation), and JTAG connects while the user set key value matches. The module configuration of 4-1 is shown in Figure 3.

Fig. 3. Module configuration in 4-1



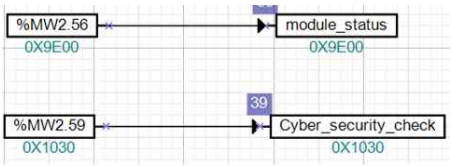
The logic waveform of the 4-1 test is shown in Figure 4.

Fig. 4. Logic analyzer test result waveform in 4-1



4-1 Monitoring program test results are shown in Figure 5.

Fig. 5. Monitoring program results in 4-1



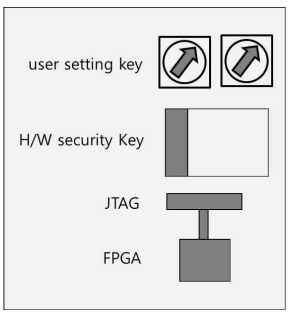
Through the 3-element logic analyzer value and the monitoring program value, it was confirmed that it is a normal approach in the case of 4-1. Since it is in the normal access state, it was possible to access the FPGA through VIVADO. Figure 6 shows that VIVADO is accessible.

Fig. 6. VIVADO approach in 4-1: Accessible

4-2. If the H / W security key among the three elements is unauthorized access

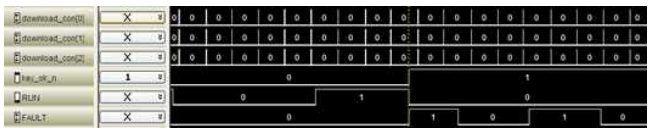
It is accessed without H / W security key installed (same as H / W security key value mismatch), and JTAG connects while the user set key values match. The module configuration of 4-2 is shown in Figure 7.

Fig. 7. Module configuration in 4-2



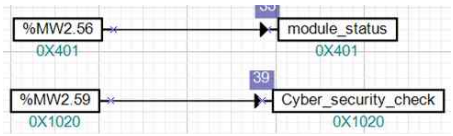
The logic waveform of the 4-2 test is shown in Figure 8.

Fig. 8. Logic analyzer test result waveform in 4-2



4-2 Monitoring program test results are shown in Figure 9.

Fig. 9. Monitoring program results in 4-2



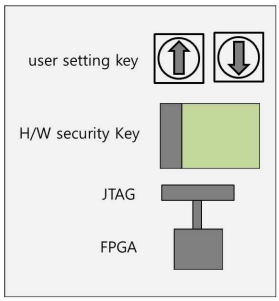
Through the 3-element logic analyzer value and the monitoring program value, it was confirmed that it is an unauthorized access in the case of 4-2. Since it is in an unauthorized access state, it was impossible to access the FPGA through VIVADO. Figure 10 shows that VIVADO access is not possible.

Fig. 10. VIVADO approach in 4-2: Inaccessible

4-3. If the user setting key among the three elements is unauthorized access

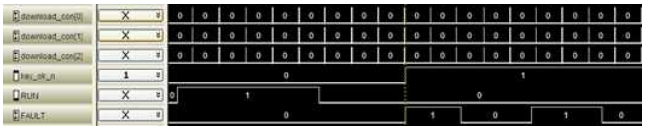
Access to H / W security key normal (H / W security key value matching, H / W security key value installation), and JTAG connects when the user set key value is inconsistent. The module configuration of 4-3 is shown in Figure 11.

Fig. 11. Module configuration in 4-3



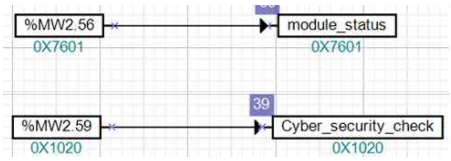
The logic waveform of the 4-3 test is shown in Figure 12.

Fig. 12. Logic analyzer test result waveform in 4-3



4-3 Monitoring program test results are shown in Figure 13.

Fig. 13. Monitoring program results in 4-3



Through the 3-element logic analyzer value and the monitoring program value, it was confirmed that it is unauthorized access in the case of 4-3. Since it is in an unauthorized access state, it was impossible to access the FPGA through VIVADO. Figure 14 shows that VIVADO access is not possible.

Fig. 14. VIVADO approach in 4-3: Inaccessible

5. Conclusion

Through 4-1, 4-2, and 4-3, access to the FPGA was possible only when all three elements for physical access were normal access. If any of the three elements is not physically connected, normal access will not be achieved. Therefore, it is suitable as the physical control of KINS's SDE. Also, in the case of unauthorized access, the FAULT signal can be sent to the module to inform the manager, so the unauthorized access status can be quickly checked.

REFERENCES

[1] MyeongKyun. Lee, Study on Cyber Security Requirement for Safety-related Controller, Transactions of the Korean Nuclear Society Autumn Meeting, October 24-25, 2019
[2] US NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Power Facilities,” 2010