Implementation of the HDTS with cybersecurity

Minwoo Lee[a]*, Kyungchul Kim[a], Jiye Jeong, Young-San Choe, Sangjun Park
*Corresponding author : leemw@kaeri.re.kr

***Keywords : HANARO, HDTS, KINAC, Cyber Security**

1. Introduction

HANARO (High-flux Advanced Neutron Application Reactor) is a 30MWth multi-purpose research reactor. Since the first criticality achieved in February 1995, the HANARO has been utilizing in various fields such as nuclear in-pile tests, radioisotope production, neutron beam research, neutron transmutation doping, and neutron activation analysis.

In 2015, a seven-phase cybersecurity implementation plan for HANARO was established in accordance with KINAC's guidelines for Computer and Information System Security for Nuclear Facilities (RS-015). Since then, significant efforts have been made to enhance the cybersecurity framework for HANARO.

In 2024, the HANARO Data Transfer System (HDTS) was developed to facilitate data transmission from HANARO to the regulatory body, incorporating cybersecurity measures to ensure secure operations. This paper provides a summary of these developments.

2. Purpose of a HDTS

HANARO control system comprises the HANARO control computer system (HCCS), the CNS Control computer, the Operator Workstation (OWS), and the Historian server as illustrated in Figure 1. HCCS is responsible for controlling reactor power and auxiliary system while providing comprehensive status information to the operator. For real-time data processing between control system and OWS, communication occurs each 200 milliseconds within an independent network configuration.

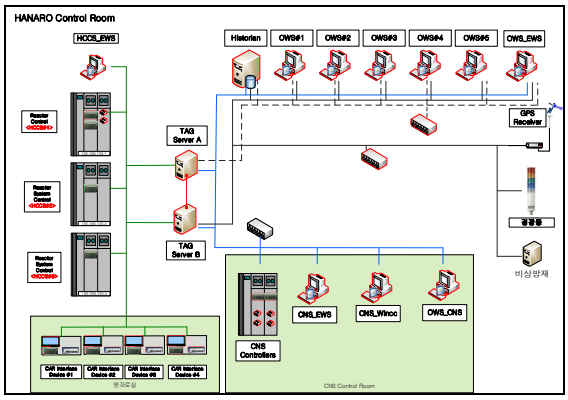

Fig 1. Control Computer Configuration

According to the Nuclear Safety and Security Commission(NSSC) Notice of 2022, all safety-related information must be provided to NSSC and KINS in a digitalized format. To comply with this requirement, the HDTS was newly developed to facilitate the secure transmission of the data.

3. Importance of cybersecurity in HDTS

With advancements in information and communication technologies, including the internet, cyberattacks have become prevalent across various domains, causing significant disruptions. One approach to mitigating such threats is to completely isolate a system from external networks. However, when isolation is not feasible, it is essential to implement robust cybersecurity measures to prevent unauthorized access and to continuously enhance security protocols.

While all HANARO control systems operate on closed networks, HDTS is required to transmit safety-related data externally. As a result, an external internet connection is unavoidable, necessitating the implementation of a more stringent cybersecurity strategy to safeguard data integrity and system security.

4. Designing HDTS with HANARO cyber security

HDTS was designed to receive Historian server data from the HANARO control system using RS-232 for one-way communication only, ensuring that data flows from Historian to HDTS without the possibility of reverse transmission. As illustrated in Figure 2. HDTS then transmits this data to the KINS server, with the transmission line firewalled at both ends to enhance security.

After installing RS-232 unidirectional communication, tests confirmed that data transmission occurs exclusively in one direction, further verifying its security, as depicted in figure 3.

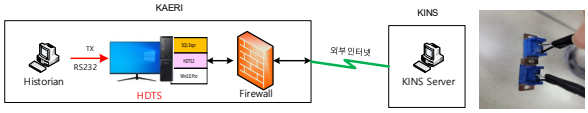

Fig 2. RS-232 unidirectional communication

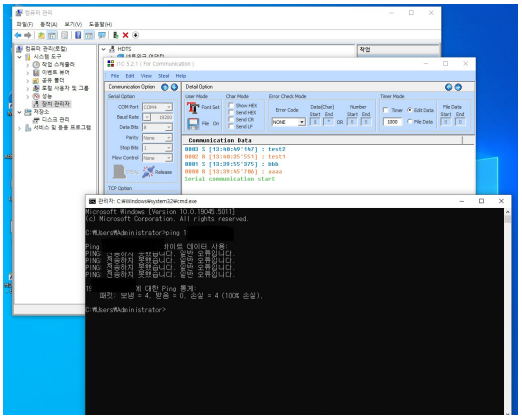

Fig 3. unidirectional communication test

Additionally, to strengthen the security of the communication line between HDTS and KINS, a dedicated line secured by the telecommunications provider was utilized. HANARO control systems are classified as Critical system(CS) and Critical digital asset(CDA) in accordance with HANARO cybersecurity regulation, as shown figure 4. Assets categorized as CDA are subject to rigorous monitoring and management in compliance with cybersecurity protocols. Furthermore, CDAs are classified into different security levels based on the he defense-in-depth strategy, with each level managed accordingly, as illustrated in figure 5. The Installed HDTS adheres to HANARO cybersecurity regulation. Since it is designed with one-way communication, it is classified as a Level 2 based on the results of the cybersecurity impact assessment in accordance with digital asset impact evaluation guidelines, which is considered a lower security level than the HANARO control system.

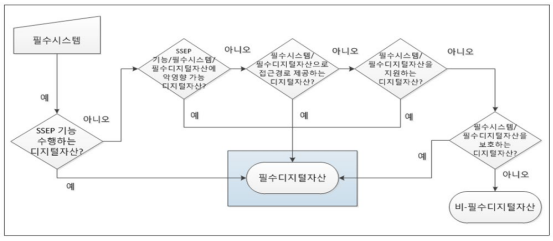

Fig 4. CDA identification procedure

Fig 5. Cybersecurity defense-in-depth architecture

5. HDTS data transmission test

HDTS was designed in compliance with the HANARO cybersecurity regulation, ensuring unidirectional communication between the HANARO control system and HDTS.

A transmission test was conducted to verify data transfer from the HANARO control system to the KINS data server. The test confirmed that data was successfully transmitted every 15 seconds, as required by KINS, as illustrated in Figure 6.

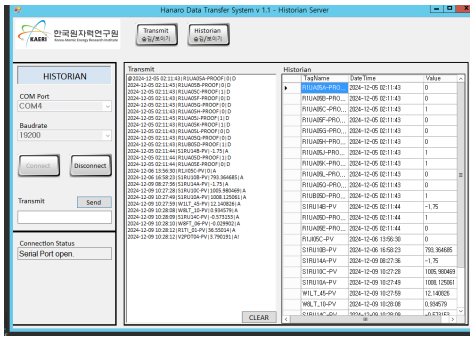

Fig 6. Data transmission test

6. Conclusion

In accordance with the NSSC(Nuclear Safety and Security Commission) Notice of 2022, nuclear power facilities are required to provide safety information digitally to NSSC and KINS. To comply with this mandate, HANARO developed the HDTS to securely transmit safety data from the control system to the KINS data collection server.

HANARO's cybersecurity framework, established under RS-015, provides a robust defense against cyber threats. The newly developed HDTS adheres to these cybersecurity regulations, incorporating enhanced security measures to mitigate external threats. The design process, communication tests, and transmission tests confirm that the HDTS effectively and securely transmits data, fully meeting KINS requirements.

REFERENCES

[1] KINAC/RS-015, Cybersecurity for Computer and Information Systems

[2] Guidelines for Cybersecurity Management of Nuclear Facilities at the Korea Atomic Energy Research Institute

[3] Guidelines for Identifying Essential Digital Assets of Nuclear Facilities at the Korea Atomic Energy Research Institute