A Study on the method for identification of Critical Digital Asset at the Nuclear Power Plant

Seo Bin Oh [a*], Soon Il Chung [a], Soon Ho Park [a]
[a]*FNC Technology Co., Ltd.,32 Fl., 13 Heungdeok 1-ro, Giheung-gu, Yongin-si, Gyeonggi-do, Korea*
**Corresponding author: ohsb0226@fnctech.com*

1. Introduction

Recently, there is growing concern about cyber threats targeting Nuclear Power Plants (NPPs). Accordingly, "Korea Hydro & Nuclear Power" (KHNP) are regulating the cyber security plans of the nuclear facilities in order to ensure that the computer and information systems are adequately protected against Cyber Attacks.

To secure the security of nuclear facilities, the United States follow the 10 CFR 73.54. Identify Critical Digital Assets (CDA) to perform nuclear facilities Safety, Security and Emergency Preparedness (SSEP) functions and support system functions. It is also required that digital computers, telecommunication systems, and network of nuclear facilities including Design Basis Threat (DBT) from Cyber Attacks.

In Korea, Korea Institute of "Nuclear Nonproliferation and Control" (KINAC) established KINAC/RS-019, which is based upon NEI 10-04 and adapted to Korean circumstances. KHNP should carry out Cyber Security Plans (CSP) to establish cyber security measures according to the technical standards. The adequacy of the implementation results has been evaluated and examined in KINAC[1].

In this study, the methods of identifying Critical Systems (CS) and CDA of nuclear facilities have been performed accordingly.

2. Identification of Critical System and Critical Digital Assets

2.1 Critical System (CS) Identification Method

To identify CDA, the first thing to do is to identify Critical System (CS) out of the whole system from the facility. A CS is the system which performs or affects SSEP functions, and it also includes the system which provides a pathway to a CS or supports a CS.

A system that is associated with or provides safety-related functions; important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; or support systems and equipment which, if compromised, would adverse impact safety, security, or emergency preparedness functions[4].

In accordance with the regulations, the Safety-Related systems shall be defined as follows:

a. The integrity of the reactor coolant pressure boundary
b. The capability to shut down the reactor and maintain it in a safe shutdown condition
c. The capability to prevent or mitigate the consequences of external leakage accidents of radioactive material

In accordance with the regulations, other systems except safety-related systems are referred to as Important-to-Safety systems. Systems that perform important-to-safety functions should include those that are required to maintain diversity and defense-in-depth for safety functions.

References to help in identifying safety-related and important-to-safety systems include:

a. Safety Analysis Report (SAR)
b. Design Basis Documents
c. Technical Specifications (TS)
d. Licensee commitments with respect to RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants"

The emergency preparedness systems within the scope of the cyber-security rule include digital computer, and communication systems and networks associated with measures needed for the protection of the public in the event of a radiological emergency.

The ability to perform emergency preparedness should be demonstrated in consideration of the following:

a. Systems for both onsite and offsite communications
b. Backup capabilities
c. Alert and Notification System (ANS) for their EPZs
d. Maintain emergency preparedness capabilities
e. Consider self-imposed requirements

Support systems as equipment to be protected include those required to provide a stable environment conducive to the operational requirements of systems associated with SSEP functions or that, if compromised, would adverse impact system performing SSEP functions.

For example, support systems and equipment may include the following:

a. Electrical Power systems whether primary or backup
b. HVAC systems

c. Fire protection systems
d. Secondary Power supply for Detection and Assessment Equipment
e. Support systems and equipment that are required to maintain diversity and defense-in-depth for safety functions (e.g., the diverse actuation system and credited diverse display systems).

These essential systems can be controlled digitally or electronically and are not included or included within the scope of cyber security planning. Thus nuclear operators perform an initial consequence analysis of all operating system, devices, communications systems, network and support systems in nuclear installations. Also, one should determine whether the SSEP functions of the nuclear facility and classify them as essential systems could be damaged or not. For support systems and supporting devices that are not directly related to SSEP function, the nuclear operators perform a dependency analysis of the SSEP functions and are classified as required if they have a detrimental effect upon the SSEP function.

The following systems belong to the CS:

a. System which performs or affects SSEP functions
b. System which performs SSEP functions or could adversely affect SSEP functions or CSs
c. System that provide a pathway to a CS and/or CDA
d. System which CS or supports a CS

Figure 1 shows schematically critical system identification procedure[2].

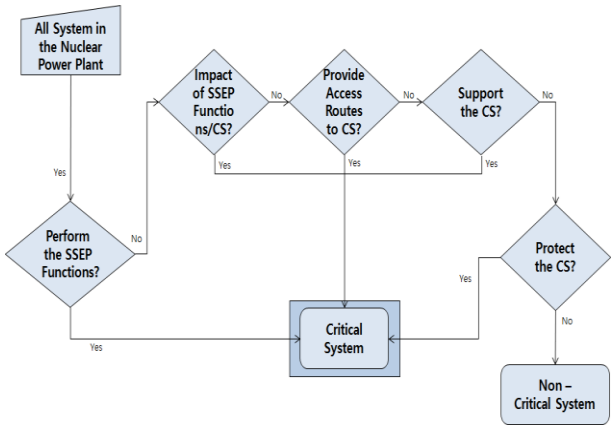

Fig. 1. Critical System Identification Procedure

2.2 Critical Digital Asset (CDA) Classification Method

A CDA is a computer and information system that performs SSEP functions or influences among the CS. It is a device that must be protected against Cyber Attacks. Also, it is a device that adverse impact functions on public safety. Nuclear operators should ensure that the computer and information system of the nuclear facility are protected against Cyber Attacks contained in Design Basis Threat (DBT).

In particular, the CDA that perform the following functions should be protected against Cyber Attacks.

▪Safety-related and Important-to-safety functions
▪Security functions
▪Emergency preparedness functions, including offsite communications
▪Support systems and equipment which, if compromised, would adverse impact safety, security or emergency preparedness functions

Based on the procedure in figure 1, classify and define assets according to the following:

▪Safety functions assets classification and definition
▪Security functions system classification and definition
▪Emergency response functions system classification and definition

Assets classified according to the above procedure are selected as CDA if one or more of the identified criteria.

The following digital assets belong to the CDA:

a. The digital asset which performs SSEP functions
b. The digital asset which adversely affect SSEP functions or CS and/or CDA
c. The digital asset that provide a pathway to a CS and/or CDA
d. The digital asset which CS or supports a CDA

Figure 2 shows schematically critical digital asset identification procedure[2].

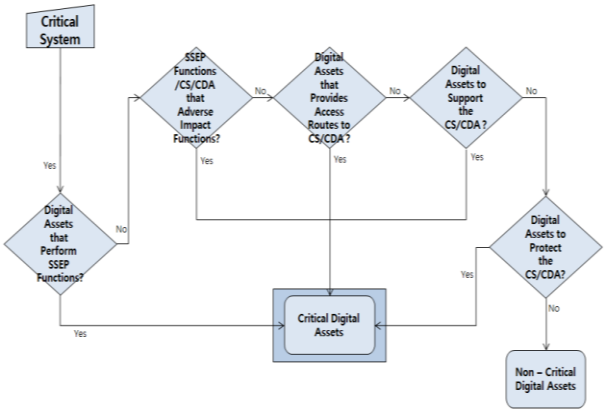

Fig. 2. Critical Digital Asset Identification Procedure

3. Conclusions

In this study, the method of identifying the critical digital assets has been reviewed based on the RS-019 technical standard established by the KINAC. It has examined how to identify the critical digital assets that can be contravened to respond to these Cyber Attacks. Examples of identified CDA include hart communication recorder, smart transmitters, etc.

In the future, it will likely need ongoing management and evaluation of critical digital assets and devices that are design changes or newly installed devices.

REFERENCES

[1] KINAC RS-019, Regulatory Standard on Identification of Critical Digital Assets for Nuclear Facilities, Rev. 0, 2015
[2] KINAC RS-015, Computer and Information System Security Technology Standards for Nuclear Facilities, Rev. 0, 2015
[3] NEI 13-10, Cyber Security Control Assessments, Rev. 0, 2013
[4] NEI 10-04, Identifying Systems and Assets Subject to the Cyber Security Rule, Rev. 2, 2012