Identification of Critical Digital Assets for Nuclear Instrumentation System in Research Reactor

Sungmoon JOO[1], Sang Mun SEO[2], and Yong–Suk SUH[3]

1. Decommissioning Technology Research Division, Korea Atomic Energy Research Institute, 111 Daedeok-daero 989Beon-gil, Daejeon 34057, Korea (smjoo@kaeri.re.kr)
2. Research Reactor System Design Division, Korea Atomic Energy Research Institute, 111 Daedeok-daero 989Beon-gil, Daejeon 34057, Korea (smsuh@kaeri.re.kr)
3. Research Reactor System Design Division, Korea Atomic Energy Research Institute, 111 Daedeok-daero 989Beon-gil, Daejeon 34057, Korea (yssuh@kaeri.re.kr)

Abstract: Identification of critical digital assets is the first step for cyber security in nuclear facilities. Among many systems in nuclear reactor instrumentation and control system, nuclear instrumentation system is unique in the sense that it can be considered as a single system or a collection of several sub-systems. This paper presents a preliminary result of the identification of critical digital assets in an open-pool type research reactor.
Keyword: Cyber Security, Critical Digital Assets, Nuclear Instrumentation System, Research Reactor

1 Introduction

In recent years, the nuclear instrumentation system in research reactors has been digitalized as it has the potential to improve safety and operational performance. This digitalization, however, comes with a caveat that the digital system is vulnerable to cyber security issues. KINAC RS-015[1] and KINAC RS-015[2] provide regulatory guidelines for the implementation of cyber security measures for nuclear facilities in Korea. In essence, all the nuclear facilities need to be designed and operated in accordance with its own cyber security plan (CSP), and the identification of critical digital assets (CDAs) is the first step towards defining the scope of application for cyber security measures within the nuclear facilities[1][2][3].

Critical system (CS) for nuclear facilities is defined as systems and networks associated with safety, security, emergency preparedness (SSEP) systems, and their support systems[1][2][3]. Components and equipment within a CS that contain digital electronics such as microprocessors, FPGAs, or SoCs are considered as CDAs[1][2][3]. The results of CDA identification are documented in the cyber security plan (CSP), and used as reference data for all CSP related activities[1][3]. The details of CDA identification procedure for nuclear facilities in Korea is provided in [2].

Nuclear instrumentation system (NIS) is different from usual field instrument systems in the sense that NIS itself is not a single system within the instrumentation and control system, but is a collection of independent sub-systems providing radiation signals necessary for safe reactor operation. Each radiation measuring system included in NIS functions as a field instrument but it is more than that; a typical radiation measuring channel consist of three components: detector, signal conditioning unit (SCU), and signal processing unit (SPU). This unique nature of NIS requires attention in the implementation of cyber security.

This study presents the experience in the implementation of NIS CDA identification procedure, and the preliminary result for a research reactor, Kijang Research Reactor (KJRR).

2 CDA Identification

In this section, we present the preliminary results of the CDA identification for KJRR. The result is preliminary as the CDA identification has not been finalized yet.

2.1 Kijang Research Reactor

KJRR project launched in April 2012. Korea Atomic Energy Research Institute (KAERI) is the owner of KJRR project. The primary purpose of KJRR operation is fission molybdenum production. The nominal thermal power of the reactor is 15MW. The reactor is open-pool type, and adopts LEU U-Mo plate type fuel. The reactor core is cooled by light water. As of writing the paper, KAERI has been

finalizing the design, and waiting for the approval of construction permit.

2.2 KJRR Nuclear Instrumentation System

The nuclear instrumentation system of KJRR includes following sub-systems:

1) NMS (Neutron Measurement System)
2) PNMS (Neutron Monitoring System for Primary Cooling System)
3) PGMS (Gamma Monitoring System for Primary Cooling System)
4) PRMS (Pool Surface Radiation Monitoring System)

Radiation monitoring system for fission molybdenum production facility is not considered in this study.

Table 1 summarizes the configuration and functions of the nuclear instrumentation system.

Table 1 KJRR Nuclear Instrumentation System

	Detector Type/Signal Destination
NMS	Wide Range Fission Chamber - Safety Channel: Reactor Protection System (RPS) - Non-Safety Channel: Reactor Regulating System (RRS), Alternate Protection System (APS)
	Compensated Ionization Chamber - Safety Channel: RPS, Accident Monitoring System (AMS)
PNMS	Proportional Counter - Safety Channel: RPS, AMS - Non-Safety Channel: APS
PGMS	Gamma Ionization Chamber - Safety Channel: RPS
PRMS	Gamma Ionization Chamber - Safety Channel: RPS, AMS

2.3 CDA Identification

Critical digital assets are identified following the guideline from [2]; critical systems (CSs) are identified first, then critical digital assets (CDAs) are identified. Fig. 1 and 2 show the identification process for CS and CDA, respectively.

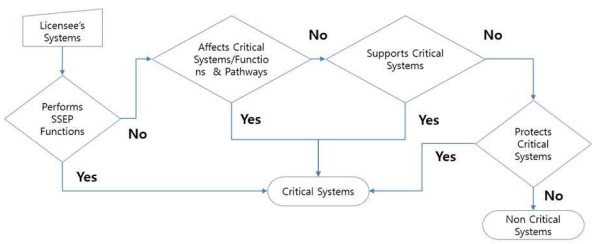

Fig.1 Identification Process for Critical Systems

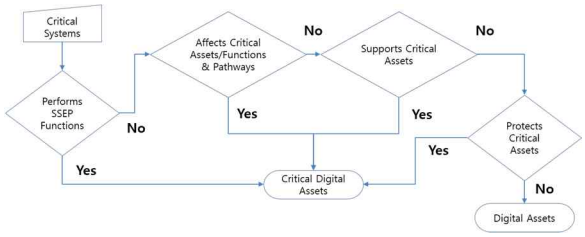

Fig. 2 Identification Process for Critical Digital Assets

The identification of CSs illustrated in Fig. 1 can be performed by a check list that asks whether a system (i) performs or is relied upon for SSEP functions, (ii) affects SSEP functions, (iii) provides a pathway to a CS that could be used to compromise, attach, or degrade an SSEP function, (iv) supports a CS, or (v) protects any of the above from cyber-attack up to and including the design bases threat. As NIS provides critical radiation measurement information to instrumentation and control system, all of the sub-systems in KJRR NIS is identified as CS (Table 2).

Table 2 Critical System Identification for KJRR NIS

	System	CS (×/O)
NMS	Wide Range Fission Chamber - Safety Channel RPS	O
	Wide Range Fission Chamber - Non-Safety Channel RRS, APS	O
	Compensated Ionization Chamber - Safety Channel RPS, AMS	O
PNMS	Proportional Counter - Safety Channel RPS, AMS	O
	Proportional Counter - Non-Safety Channel: APS	O
PGMS	Gamma Ionization Chamber - Safety Channel RPS	O
PRMS	Gamma Ionization Chamber - Safety Channel RPS, AMS	O

As mentioned earlier, typical digital nuclear instrument channel consists of three components: detector, SCU, and SPU. Table 3 shows three scenarios that a licensee can consider in CDA identification process. Case1 is the case in which a channel itself is considered as a unit for CDA identification, while, in Case2 and Case3, each component in a channel is considered as a unit for CDA identification. Thus, in Case1, if any of the three components in a channel is a digital equipment, the channel is identified as a CDA. In most cases, neutron or gamma radiation detectors are analog.

Thus detector is assumed to be analog. The difference between Case2 and Case3 is the type of SCU. Case2 represent the scenario with analog SCU, while Case3 represents the scenario with digital SCU. Some NIS vendors provide products with analog SCU, and other vendors provide digital equipment.

Table 3 CDA Identification Scenario for Digital NIS

	Case1	Case2	Case3
Detector	Digital System	Analog Component	Analog Component
Signal Conditioning Unit (e.g., preamplifier, current-to-frequency converter)		Analog Component	Digital Component
Signal Processing Unit		Digital Component	Digital Component

The results of CDA identification for three cases are summarized in Table 4 which shows that how we define a unit for CDA identification affects the number of CDAs.

Table 4 CDA Identification for Digital NIS in KJRR

CDA (×/O)			
Component	Case1	Case2	Case3
Detector	O	×	×
SCU		×	O
SPU		O	O

3 Concluding Remarks

In this paper, preliminary result of CDA identification for KJRR NIS was presented. The primary observation is the effect of the unit of CDA identification. If we see NIS in component level, there are chances that the number of CDAs increases but we can prepare very detailed cyber security plan. At the other end of the spectrum, if we see NIS in channel level, there are chances that we miss some cyber-attack paths which are unobservable. There must be a trade-off in determining the CDA level.

There are also some other factors to be considered in CDA identification for research reactors. Among others, the difference between research reactors (RRs) and nuclear power plants (NPPs) must be considered. Table 5 shows a comparison between the two. It can be implied that RRs are much safer than NPPs. Thus the significance of critical systems in NPP cyber security may not have the same significance in RR cyber security.

Table 5 Comparison of RR and NPP

	Research Reactor	Nuclear Power Plant
Type	Open-pool	Pressurized Reactor Vessel
Nominal Power	~15 MWth (KJRR)	~3000 MWth (OPR)
Core Size	Small - Radius: ~ 50 cm - Height: ~ 70 cm	Large - Radius: ~ 300 cm - Height: ~ 450 cm
Operating Condition	Low pressure (~ 10 atm) Low temperature (~ 50℃)	High pressure (~ 150 atm) High temperature (~ 300℃)
Reactor Building	Confinement	Containment

Once a system or component is identified as a CDA, it should be controlled by CPS, which means (potential) increase in cost and complexity in design, fabrication, operation and maintenance of the system or component. Thus it is beneficial for licensee to minimize the number of CDAs in general. Similar to the defense-in-depth protective strategies[3], we may define levels of 'criticality' among CSs in RRs, which potentially reduces the number of CDAs and associated cyber security tasks for licensee without compromising the safety of RRs.

References

[1] KINAC/RS-015, Regulatory Standard on Security of Computer and Information System for Nuclear Facilities, KINAC, Dec. 2015.

[2] KINAC/RS-019, Regulatory Standard on Identification of Critical Digital Assets for Nuclear Facilities, KINAC, Dec. 2015.

[3] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. NRC, Jan. 2010.

[4] S. W. Kim, "Study on CDA Identification and Lesson Learned from the Result for the Cyber Security Regulation for Nuclear Facilities", Transactions of the Korean Nuclear Society Autumn Meeting, Gyeongju, Korea, Oct. 27-28, 2016.