Study on CDA Identification and Lesson Learned from the Result for the Cyber Security Regulation for Nuclear Facilities

Si Won Kim*
Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea 34054
**Corresponding author: swkim@kinac.re.kr*

1. Introduction

According to the trend that nuclear power plants (NPPs) are being digitalized, the number of digital systems in NPP is increasing steadily. The digital systems in NPP can have serious effects on NPP operation due to malicious cyber attacks. In addition, when they are used as terror attacks, they can create the radiological impact. Due to such impact, there is a growing emphasis on cybersecurity of NPPs.

It is the United States that shows the most enthusiastic preparation for the protection of NPPs from cyber threats. The United States has been trying to improve cybersecurity of NPPs since the 911 terror in 2001 [1]. In this process, the Nuclear Regulatory Commission (NRC) of the U.S. demanded the protection of the digital systems in NPPs to the licensee through 10 CFR 73.54 [2]. Moreover, RG 5.71 defined the assets, which should be protected from cyber threats, as Critical Digital Asset (CDA) [3]. Nuclear Energy Institute (NEI) provided the CDA identification guide through NEI 10-04 [4]. Meanwhile, International Electrotechnical Commission (IEC) presented the security program requirements of I&C computer in NPP [5], as well as category about systems and functions through IEC 61226 which is under revision.

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. And nuclear licensees has been applying it to facilities, after that, CDA identification has been done by each licensee except Korea Hydro & Nuclear Power (KHNP). KINAC has identified the validity of the results through the inspection about such licensee execution result, and this paper shows that the problems and solutions which have been identified during the CDA identification processes.

2. Result of CDA Identification

Nuclear licensees except KHNP identified CDAs on the basis of KINAC/RS-019. To identify CDA, the first thing to do is to identify Critical System (CS) out of the whole system in 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. The next thing to do is to identify CDAs among the whole digital assets in identified CS. A CDA is the digital asset which performs SSEP functions or could adversely affect SSEP functions or CSs. It also includes the digital asset that provide a pathway to a CS and/or CDA, or support a CS and/or CDA [6].

According to the process mentioned above, the final result from identifying CDA in each facility is as follows.

Table 1: Number of CS and CDA per Facility

	number of CSs	number of CSs include CDA	number of CDAs	number of CDA Types
Facility A	5	5	198	29
Facility B	22	15	274	70
Facility C	13	3	42	13
Facility D	12	4	47	9
Facility E	26	5	23	7
Total	78	32	584	128

The table 1 can make certain that on average 16 CSs are identified per facility. Besides, the number of CSs which include CDA is 40% on average, and about 20 to 270 CDAs are identified per facility. On average one facility has 120 CDAs, and the number of CDA types is average 26.

3. Lesson Learned from the Result

KINAC performed the inspection to check the validity of CDA identification results from each facility, and could identify that all the results were valid by checking identification processes and basis documentation as well as performing site inspection. However, there were several problems which were identified during the inspection. The identified problems are shared and the possible solutions are described in the below.

3.1 Connection between Different Networks

Unlike the NPPs that separate corporate network from control network and operation network, in other nuclear facilities, the considerable cases that various networks are connected each other were discovered. This can cause the result that unnecessary CSs are identified. For example, if Network includes a CS is connected with Network includes a non-CS, additionally that non-CS would be identified as a CS because it provides a pathway to the CS. To solve such a problem, the licensee should have designed system considering the connections between Networks.

3.2 Finding the Systems that are not on the list

The first step to identity CS is to list the whole systems in nuclear facilities. Since each process to identify CS is performed only for the systems in the whole systems list, the other systems that are not on the list cannot be identified as CS. In reality, there were several cases that missing systems were discovered in some facilities during inspection and that several steps for identifying CS were affected by adding the missing systems to the whole systems list. The licensees have to check whether the added systems perform SSEP function, provide a pathway to a CS, and support a CS. On the contrary, they also should make sure whether CS provides the access to the added systems, as well as whether there is any system that supports the added systems. The licensees should not perform such steps recursively to save valuable resource, so it will be crucial that there is no missing systems in the process of initially listing the whole systems.

3.3 Ambiguousness of Determining System Unit

To identify CS, the first thing to do is to list the whole systems, which gave difficulties about how licensee determine system unit. For instance, if there is one big system that contains several subsystems, the one big system can be seen as either 1 system. However, it also can be seen as several systems if the licensee considers each subsystem as an individual system. When dividing systems largely, the number of the systems decreases, but the number of assets per system increases. Dividing systems small produces the opposite result. Both of them have the pros and cons in management, so the licensee should set up the optimal system unit considering each facility's characteristics and trade-off.

3.4 Difference in Understanding of Cybersecurity between Cybersecurity Team and Operation Team

There were the cases that some problems were encountered during the identification processes, due to the difference in understanding of cybersecurity between cybersecurity team and operation team. The most representative case was that in Facility A, some power system and Heating, Ventilating, and Air Conditioning (HVAC) system were missing out of the whole systems list to identify CS. It was because the operation team did not understand exactly the standard related to cybersecurity. To solve such problems, it seems to be necessary that the cybersecurity teams not only support the operation teams during the identification processes, but also perform the continuous review about the identification results. Such activities could surely decrease the problems resulted from the low degree of understanding of the operation teams.

4. Conclusions

As time goes by, the digital systems in NPPs increase and the possibilities of cyber threats becomes greater. To protect these systems from cyber attacks, it is important to identify CDA, which is the target to be protect. For that, the standards to identify CDA were established, and according to the standards, the licensees could perform identification works and draw many CDAs. During the inspection processes for this, KINAC could find several problems and has been tried to look for the solutions.

It is desired that such solutions will be actively used when identifying CDAs in NPPs, and also they should be applied to the systems which are added or changed during the whole facility life cycle. Through this, whole CDAs could be identified perfectly during the whole facility life cycle, and then the licensees could manage CDAs more efficiently. Moreover, since the licensees could apply the security controls for clearly identified CDA, they will be able to strengthen cyber security. Finally, as the identification of target to be protected could be done more fitly, it is expected that the waste of effort to apply the security controls and conduct inspection will be certainly reduced.

REFERENCES

[1] K. Kwon, I. Shin, J. Lee, S. Jo, Safety-Security Interface Method for Protection of Digital Safety System at Nuclear Facilities, 2014 Conference on Information Security and Cryptology.

[2] 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks, U.S. NRC, Nov. 2, 2015.

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

[4] NEI 10-04 Rev.2, Identifying Systems and Assets Subject to the Cyber Security Rule, Nuclear Energy Institute, Jul. 2012.

[5] IEC 62645, Nuclear Power Plants - Instrumentation and Control Systems - Requirements for Security Programmes for Computer-based Systems, International Electrotechnical Commission, Aug. 2014.

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