Consequence-Based Cyber Security Graded Approach for CDA Identification

Ickhyun Shin[*], Sangcheol Hyung
Nuclear Control Policy Center, Korea Institute of Nuclear Non-proliferation And Control, 1418 Yuseong-daero, Yuseong-gu, Daejeon City, 34101
[*]Corresponding author: ihshin@kinac.re.kr

1. Introduction

The instrumentation and control systems of nuclear power plants have been converted from analog to digital, from proprietary system to commercial system, from stand-alone system to multi-connected system such as SCADA. This means that cyber attacker can have more chance to conduct cyberattack using variety of attack vectors while cybersecurity personnel need to take more efforts on implementing cyber security measures. This will lead to increased fatigue and reduced efficiency of the work, resulting in poor quality of security measures, which can make computer systems more vulnerable to cyberattack.

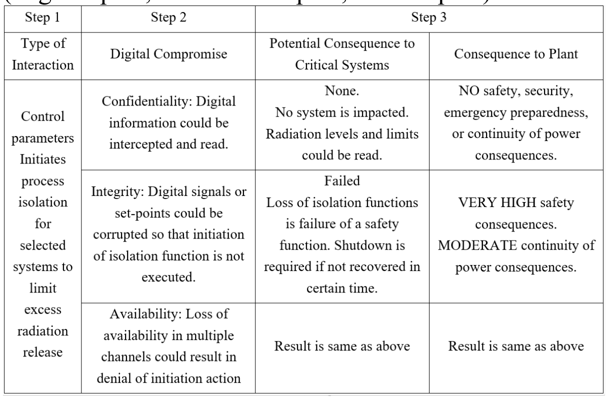
Therefore, effective cybersecurity measures need to be established. The IAEA's INFCIRC 225_Rev5 recommends that security measures should be applied proportionately to the degree of risk [1]. From a traditional safety perspective, the degree of risk can be assessed by assessing the probabilities of safety events, such as machine failure, human error, and natural disasters, and the degree of consequence resulting from the occurrence of the event. However, in cybersecurity, the probability of occurrence is set at 1, not as a variable, but as a fixed constant, and only a consequence assessment is performed when considering cyber risk. This is because it is not possible to quantify how often cyberattack actors will carry out cyberattacks.

Currently, the nuclear power plant licensees in U.S. and ROK need to classify CDAs as direct CDAs and non-direct CDAs according to the importance of functions as a Consequence-Based Approaches. And only baseline security measures are applied to the non-direct CDAs, while all the security measures need be applied to the direct CDS [4,5,6]. Some improvements in the method is needed. First, the CDAs need to be further subdivided to apply security measures in more efficient manner. Second, the CDA need to be classified according to the consequence.

In this paper, the consequence assessment methodologies presented by the US NRC's research report and the IAEA's cybersecurity guide are reviewed. And a more optimized CDA consequence assessment methodology is presented.

2. Cyber Security Self-Assessment Method

U.S. NRC NUREG/CR-6847 provides a consequence assessment method for CDAs. The consequence level on each of the SSEP systems (Safety System, Safety Support System, Plant Security, EP System, Continuity of Power Impact) is presented when the interaction between the CDA and the Critical System is compromised. Also, the consequence level on the plant as a whole is presented in three phases, as shown in Figure.1. [3]
- Step 1: Categorize into 7 types of information that is interacted between CDA and Critical System
- Step 2: Classify 3 types of compromise (Confidentiality, Integrity and Availability)
- Step 3: Categorize the main consequence on the system into three types (None, Degraded, Failed) and the ultimate consequence on the plant as a result of the compromise of interaction information into three classes (High Impact, Moderate Impact, Low Impact)



Step 1	Step 2	Step 3	
Type of Interaction	Digital Compromise	Potential Consequence to Critical Systems	Consequence to Plant
Control parameters Initiates process isolation for selected systems to limit excess radiation release	Confidentiality: Digital information could be intercepted and read.	None. No system is impacted. Radiation levels and limits could be read.	NO safety, security, emergency preparedness, or continuity of power consequences.
	Integrity: Digital signals or set-points could be corrupted so that initiation of isolation function is not executed.	Failed Loss of isolation functions is failure of a safety function. Shutdown is required if not recovered in certain time.	VERY HIGH safety consequences. MODERATE continuity of power consequences.
	Availability: Loss of availability in multiple channels could result in denial of initiation action	Result is same as above	Result is same as above

Fig. 1. Sample consequence analysis for the Radiation Monitoring System

This methodology focuses on the compromise of the CDA function and divides the CDA into three classes depending on the degree of consequence on the plant, which is a suitable methodology for the Graded Approach. But some improvements are needed. The first would be to classify the classes into system units rather than dividing the consequence classes by CDA of the functional units. This is because each CDAs in a system is connected together, which can affect other CDAs in the system if one CDA is compromised.

Second, the confidentiality, availability and integrity presented by the type of digital compromise are classified according to the intention of the attacker. Therefore, the changes should be made to each type of compromise that CDA will receive. Therefore, this step should be replaced by the type of consequence observed in the event of a compromise of functions presented in IAEA NSS No. 33-T, as discussed in the following chapters.

3. Risk-Informed Graded Approach

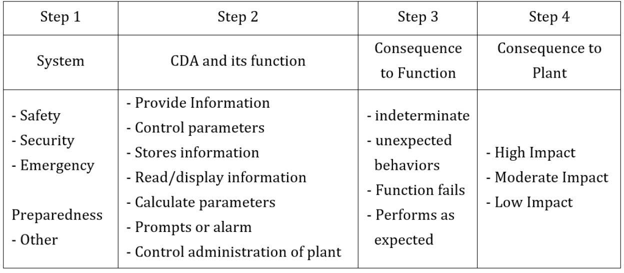
The IAEA NSS No. 33-T (Computer Security of I&C Systems at NFs) recommends that cybersecurity requirements should be defined in accordance with Risk-Informed Graded Approaches, and in particular, Graded Approaches can be achieved by assessing the degree of consequence from cyberattacks. As a specific method of consequence assessment, the level of symptoms that can be witnessed when a CDA function is compromised by a cyberattack is presented in four types as follows: [2]

- The function is indeterminate: cyber compromise has occurred but this incident cannot be recognized.
- The function has unexpected behaviors: Cyber compromise will cause the system to function abnormally and this incident can be recognized.
- The function fails: Cyber compromise prevents the system from functioning
- The function performs as expected: A situation in which a cyberattack was attempted but had no adverse effect on the system's function

The consequence type presented in this methodology is a rather narrow approach. This is because the types of consequence presented correspond to symptoms that can be observed intuitively when a CDA's function is compromised. Therefore, the consequence that could ultimately occur at the plant level should be suggested as a result of the symptoms. This may be complemented by referring to the methods for assessing the consequence previously presented in NRC NUREG/CR-6847**.**

4. Suggestion: New Approach for Consequence Assessment

This chapter presents a new approach for the consequence assessment, shown in Fig.2, which took advantage of and complement to the NRC and IAEA methodologies.



Step 1	Step 2	Step 3	Step 4
System	CDA and its function	Consequence to Function	Consequence to Plant
- Safety - Security - Emergency Preparedness - Other	- Provide Information - Control parameters - Stores information - Read/display information - Calculate parameters - Prompts or alarm - Control administration of plant	- indeterminate - unexpected behaviors - Function fails - Performs as expected	- High Impact - Moderate Impact - Low Impact

Fig. 2. Sample consequence analysis for the Radiation Monitoring System

In step 1, the system is classified into 4 different types of system. In step 2, the system is classified as a CDA of the functional unit within the system. Ultimately, this is to classify the consequence classes according to system unit rather than CDA units. In step 3, four different types of consequence to function is presented based on the IAEA NSS No. 33-T. Finally, step 4 classifies the consequence to plant into three categories (High Impact, Moderate Impact, Low Impact).

This method of consequence assessment focuses on CDA's functions and classifies CDAs according to the level of plant consequence caused by compromise of such functions. This methodology could be used to establish cyber security strategy toward to the risk-informed graded approach.

5. Conclusions

In this paper, the method of classifying consequence level for applying proportional security measures to CDA was studied. To this end, the advantages and disadvantages of the consequence assessment methodologies presented in the U.S. NRC's NUREG/CR-6847 and IAEA NSS No. 33-T were compared. New approach for consequence assessment which categorizes system into 3 different level of consequences is also presented. Further research is needed to assess whether the methodology is actually applicable.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018)

[3] U.S. Nuclear Regulatory Commission, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants, NUREG/CR-6847, Washington, D.C., 2004

[4] Nuclear Energy Institute, Cyber Security Control Assessments, NEI 13-10 Revision 5, Washington D.C., 2017

[5] U.S. Nuclear Regulatory Commission, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, Washington, D.C., 2010

[6] Korea Institute of Nuclear Non-proliferation And Control, Information and Cyber Security for Nuclear Facilities, Regulatory Standard 015, Daejeon, 2016