Development of an Identification Method for Vital Digital Assets Selection on Nuclear Cyber Security

Meejeong Hwang[a], Kookheui Kwon[b]

[a]*Korea Atomic Energy Research Institute, 989-111, Daedeok-daero, Youseong-Gu, Daejeon*
[b]*Korea Institute of Nuclear nonproliferation And Control, 1418, Youseong-daero, Youseong-Gu, Daejeon*

** Corresponding author: mjhwang@kaeri.re.kr*

1. Introduction

Digital systems are used in nuclear facilities to monitor and control various types of field devices, as well as to obtain and store vital information. Therefore, it is getting important to protect digital systems for nuclear facilities which could lead to unacceptable radiological consequences through cyber-attack. Regulatory activities for cyber security of nuclear facilities assist licensees to effectively establish the system to prevent, detect, and respond against the unauthorized removal and sabotage, which could lead to radiological impact, and to minimize the impact of cyber-attack. The KINAC (Korea Institute of Nuclear nonproliferation And Control) which is an affiliated regulatory body of ROK government has published regulatory standard, RS-015, to support Korean nuclear facilities establishing the cyber security system [1, 5]. Though the KINAC has helped nuclear facilities to identify sites' specific CDA (critical digital assets), nuclear facilities are spending much time to make cyber security system since there are lots of critical digital assets. Generally, critical digital assets are estimated over 70% of all digital assets in a nuclear power plant [6, 8]. Thus, it is necessary to identify VDAs (vital digital assets) to improve an efficiency of cyber security regulation and implementation.

In this paper, we developed a methodology identifying vital digital assets based on PRA (Probabilistic Risk Assessment) and applied the method to a nuclear power plant model. At this point, we considered only mitigating systems except IEs (Initiating Events) to identify the VDAs since IEs are not fully developed as fault tree models.

2. Identification of Critical Digital Assets

The KINAC/RS-015 provides an identification methodology for CDAs for nuclear cyber security as shown in Figure 1, which is provided in the US NRC (Nuclear Regulatory Commission) regulatory guide 5.71 [5, 8]. The critical systems which include CDAs are those systems that (1) perform or are relied upon for safety, SSEP (security and emergency preparedness) functions, (2) affect SSEP functions or affect CS (critical systems) and/or CDAs that perform SSEP functions, (3) provide a pathway to a critical system and/or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS and/or CDA, or (5) protect any of the above from cyber-attack up to and including the DBT (design basis threat) [6].

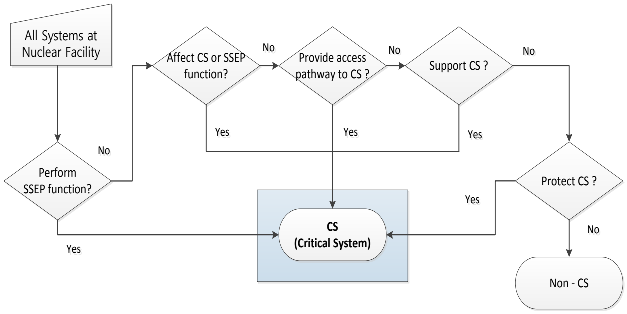

Fig.1 Identification Method for Critical System which includes Critical Digital Assets

3. PSA-based Vital Digital Assets Identification

3.1 General Concept

The methodology basically assumes that a system composed of digital devices causing physical operation and impact. The industrial control systems have been converted from analog systems to digital systems, and the digital systems called SCADA (supervisory control and data acquisition), PLC (programmable logic controller), and DCS (distributed control system) etc. measure the states of the power plant and operate the equipment. Figure 2 shows a general concept how a digital system is operated physically. Hence cyber security measures must be applied, if a required system is digitally configured to perform SSEP functions that are critical to the plant.

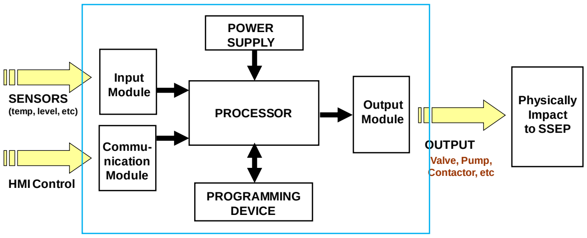

Fig.2 General Concept of Industrial Control System

As the CDAs performing the SSEP function are widespread in a plant, it is not easy to protect them from cyber-attack. In this paper, we proposes a method to identify VDAs preventing core damage accidents. Therefore, the VDAs consist of CDAs. The process identifying CDAs does not take into account the diversity and redundancy of the system, but the VDA takes these realities into account. The form of the VDA may be a digital control system that physically operates the device or a cabinet that includes such a digital system. A cyber-attack to the sets of CDAs can lead to the plant shutdown and mitigation failure. But we can prevent occurrence of the sets of CDAs leading to core damage accident by protecting a set of VDAs. The following Fig. 3 shows the concept of for identification method of target sets of digital assets. In this paper, we did not consider the target sets of digital assets provoking IEs.

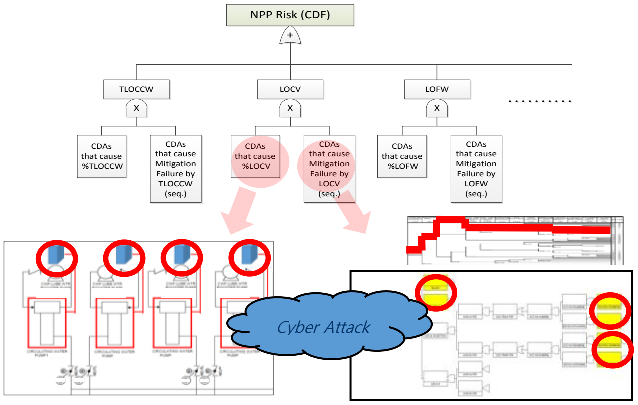
NPP Risk (CDF)
TLOCCW
LOCV
LOFW
....
CDAs that cause %TLOCCW
CDAs that cause Mitigation Failure by TLOCCW (seq.)
CDAs that cause %LOCV
CDAs that cause Mitigation Failure by LOCV (seq.)
CDAs that cause %LOFW
CDAs that cause Mitigation Failure by LOFW (seq.)
Cyber Attack

Fig.3 Concept of target set of digital assets identification method

3.2 PSA-based VDAs Identification

After an IE has occurred, related systems are operated to mitigate the event. In this step, we analyze whether the failure of event mitigation can be caused by a failure of digital assets due to cyber-attack. The analysis of the MCS (minimal cut set), which can induce reactor core damage, has already been carried out for a long time in the PRA model, and the results are used in this study. The process of identifying vital digital assets that prevent a failure of accident mitigation is as follows; 1) Mapping events to cabinet failures, 2) replace events with cabinet failures, 3) Calculate MCSs (target sets) consisting of combination of digital assets (cabinets) through an event tree (ET) and a fault tree (FT) analysis for the corresponding initiating event, 4) Calculate prevention sets (digital assets sets), 5) Select the most effective prevention set which can be VDAs. Table 1, 2, and 3 shows the example of the VDAs identification results.

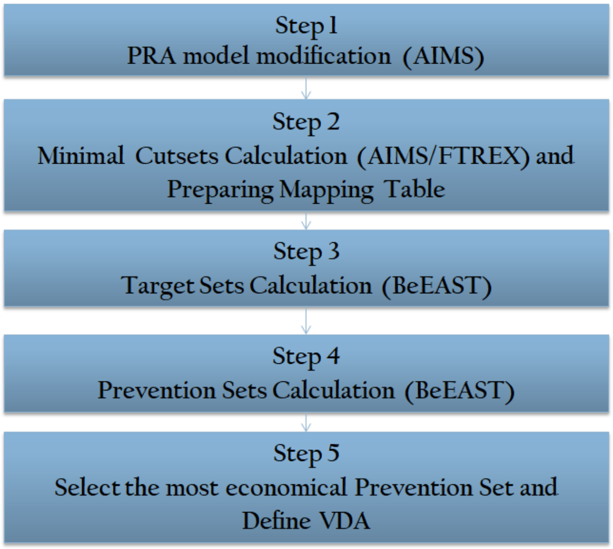
Step 1
PRA model modification (AIMS)
Step 2
Minimal Cutsets Calculation (AIMS/FTREX) and Preparing Mapping Table
Step 3
Target Sets Calculation (BeEAST)
Step 4
Prevention Sets Calculation (BeEAST)
Step 5
Select the most economical Prevention Set and Define VDA

Fig.4 PSA-based VDA Identification Process

Table 1. Mapping of digital asset event to cabinet

Digital Asset Failures Events	Cabinets	MCS
A, B, D	C1	AB
C	C2	AC
E, G	C3	AEI
H, I, J	C4	EJ
		GIJ
		CEG
		DH
		BCEI

Table 2. Target sets (Mapping cabinet information to MCSs)

No.	Event1	Event2	Event3	Event4	Minimal Target Sets
1	C1				C1
2	C1	C2			C3, C4
3	C1	C3	C4		C2, C3
4	C3	C4			
5	C2	C3			
6	C2	C3	C4		
7	C1	C4			
8	C1	C2	C3	C4	

Table 3. MPS (Prevention sets)

No.	Event1	Event2	Event3
1	C1	C3	
2	C1	C2	C4

Table 4. Comparison of the Result according to Initiating Events

	No.	No.
Initiating Event	11	20 (Including All IEs)
Mapped Basic Events	576	576
Mapped Cabinets	95	95
Minimal Cutsets	6,937	16,781
Target Sets	160 (3~6)*	165 (2~6)*
Prevention Sets	513 (6~12)*	1,304 (9~19)*

*The length of the set

4. Conclusions

As cyber threats increase, cyber security needs to be strengthened. Cyber threats to nuclear power plants have become a reality, and many cases have been reported that cyber-attack can have a physical impact. While there have been many concerns over the impact of the nuclear power plant on cyber-attack, there has not been much research on quantitative or systematic impact assessment. Through this study, we have conceptually confirmed that the failure of controlling digital assets due to cyber-attack affect the system and can affect initiating events of nuclear power plants and failure of accident mitigation. The vital digital assets are defined as sets of digital assets that can prevent failure of mitigation for accidents inducing a core damage of a nuclear power plant. The general concept of VDAs identification was described in this paper. This study will be conducted in more detail through a variety of operating modes and practical models of nuclear power plants for a couple of years.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KoFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea. (No.1605007).

REFERENCES

1. IAEA, Technical Guidance “Computer security at nuclear facilities”, NSS-17, Vienna, 2011.
2. IAEA, Technical Guidance “Computer Security of I&C System at Nuclear Facilities”, NST036, Vienna, 2017.
3. IAEA, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Safety Standards, Vienna, 2010.
4. IAEA, Defining initiating events for purposes of probabilistic safety assessment, Tecdoc-719, Vienna, 1993.
5. KINAC, Regulatory Standard on Computer Security of Nuclear Facilities, RS-015, the Republic of Korea, 2014.
6. KINAC, Regulatory Standard on Identifying Critical Digital Assets, RS-019, the Republic of Korea, 2014.
7. KAERI, Procedure for Conducting Probabilistic Safety Assessment, KAERI/TR-2548/2003, the Republic of Korea, 2003.
8. U.S. NRC, Computer Security Programs for Nuclear Facilities, R.G. 5.71, U.S., 2010.
9. K. Kwon and W. Kim, “Research on Methodology to Prioritize Critical Digital Assets based on Nuclear Risk Assessment”, IAEA International Conference on Nuclear Security, 2016
10. W.S. Jung, “Development of High-Performance Minimal Cut Set Analyzer for Nuclear Safety Regulation”, R&D Report, Nuclear Safety and Security Commission, 2017