Research on Methodology to Prioritize Critical Digital Assets based on Nuclear Risk Assessment

Wonjik Kim, Kookheui Kwon, Hyundoo Kim
Korea Institute of Nuclear Nonproliferation and Control (KINAC), 1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea
kimwj2@kinac.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 for nuclear facilities to protect digital systems from cyber-attack in terms of safety operation and public health since cyber compromise of these systems could lead to unacceptable radiological consequences.

Based on KINAC/RS-015 which is a cyber security regulatory standard, regulatory activities for cyber security at nuclear facilities generally focus on critical digital assets (CDAs) which are safety, security, and emergency preparedness related digital assets.
Critical digital assets are estimated over 60% among all digital assets in a nuclear power plant.

Therefore, it was required to prioritize critical digital assets to improve efficiency of regulation and implementation. A regulatory body and nuclear licensees will be able to more focus on high prioritized critical digital assets which are based on the graded approach for cyber security.

In this paper, the research status on methodology development to prioritize critical digital assets based on nuclear risk assessment will be introduced.

2. Graded Approach for Critical Digital Assets

2.1 IAEA

▪ Implementing Guide for Computer Security at Nuclear Facilities (NST045) [1]

This IAEA guide requires that the risk informed, graded approach entails designing and implementing security measures commensurate with direct or indirect potential consequences of unauthorized acts, taking into account the current threat.

▪ Technical Guide for Computer Security of I&C Systems at Nuclear Facilities (NST036) [2]

This IAEA guide requires that the facility computer security risk assessment should include an identification of the I&C systems whose compromise by cyber attack could lead to potential consequences. These potential consequences include the Normal operation impeded, Anticipated operational occurrence (AOO), Design basis accident (DBA), and Beyond design basis accident (including severe accident and other design extension conditions)

2.2 U.S. NRC (Nuclear Regulatory Commission)

The NRC cooperates with the NEI [3] to develop a cyber security control assessment guide for CDAs based on direct/indirect impact assessment. This guidance is to streamline the application of cyber security to the large number of CDAs, and the goal is to minimize the burden on licensees of complying with their cyber security plan (CSP).

2.3 U.S. SNL (Sandia National Laboratory)

The SNL indicated current methods to protect CDAs based on the NRC Regulatory guide 5.71 may cause licensees to overprotect some digital assets and under-protect others. Additionally some critical CDAs could be completely overlooked. So the SNL analyzed existing hazard assessment methods and plant risk assessment models can be extended to address the challenges associated with identifying and prioritizing CDAs.

2.4 KINAC

The Regulatory standard for cyber security of nuclear facilities (KINAC/RS-015) [4] requires licensees to identify CDAs among critical assets. And KINAC/RS-019 [5] suggests more detail questions and methods for identification. And KINAC researches regulatory techniques of graded risk approach for cyber security, which granted financial resource from NSSC (Nuclear Safety and Security Commission)

This research focus on consequence based cyber security analysis based on existing PRA (probabilistic risk assessment) models.

3. PRA result analysis

3.1 Initiating Event analysis

To analyze digital assets that can occur Initiating Event (IE) by cyber-attack, PRA models of PWR [6] are analyzed. First, from the fault tree, components (pump, valve, and so on) which are controlled by digital I&C systems are selected. And a scenario in minimal cut set in which if these systems fails by cyber-attack, IE will happen or Core Damage (CD) will occur due to mitigation failure is analyzed. Among digital I&C systems that can affect the event initiation and

mitigation system, safety system (ESF-CCS) is analyzed. Furthermore, non-safety system (Process-CCS) is also analyzed.

The analysis sequence is core damage sequence #38 in Loss of Condenser Vacuum (LOCV) accident. LOCV Event Tree (ET) is shown in Fig. 1.

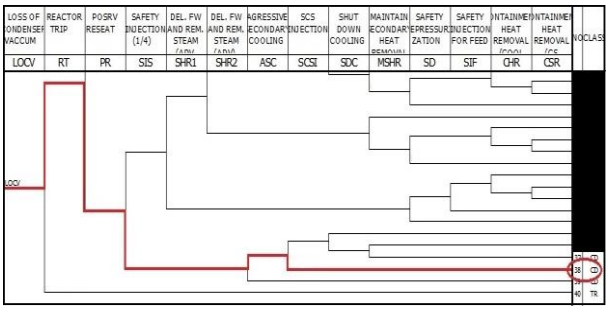

Fig. 1 Event tree model of LOCV

The initiating event LOCV can occur due to failure of condenser vacuum system or loss of circulating water or leakage of condenser. If circulating water is lost, Circulating Water System (CWS) will fail. CWS diagram is shown in Fig. 2.

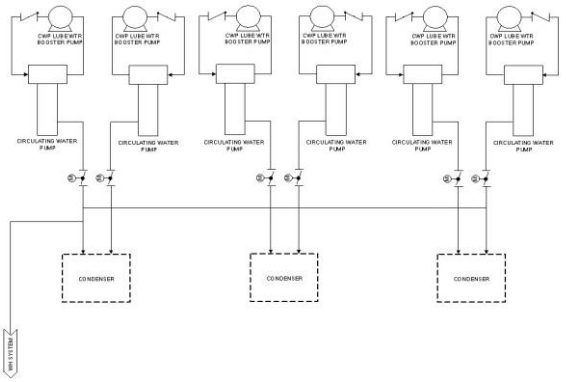

Fig. 2 Diagram of CWS

This analysis shows that some pumps in CWS which are controlled by Process-CCS digital systems could affects LOCV as an initiating event.

3.2 Accident sequence analysis

In accident sequence #38 of LOCV, minimal cut set which can occur CD by cyber-attack consists of failure of Pilot operated Safety Relief Valves (POSRVs) and failure of Safety Injection System (SIS) and Shutdown Cooling System Injection (SCSI) due to common cause failure (CCF) of digital system. POSRVs which are aimed to provide overpressure protection and Rapid Depressurization for RCS are controlled by ESF-CCS digital system.

After the IE happens, POSRVs open to try depressurization in RCS. If POSRVs fail to reseat or motor operated pilot valves which are controlled by digital system fails to open by cyber-attack, Small Loss of Coolant Accident (SLOCA) is occurred. If the SLOCA continues due to POSRVs fail open, SIS must supply coolant to RCS. If SIS does not work, Shutdown Cooling System (SCS) should be injected coolant into Reactor Vessel (RV) from In-containment Refueling Water Storage Tank (IRWST). But, if digital system in Component Cooling System (CCS) that commonly applied to SIS and SCS fails by cyber-attack, Motor Operated Valve (MOV) which is controlled by this system closes, and could causes core damage.

Digital control systems and related components that found out from result of analysis are given in Table. 1.

Table. 1 Digital systems related to component and Type

Digital system	Related Component	Type	Result from Cyber-attack
Process-Component Control System	Pumps	Non-Safety	Event Initiating
ESF-Component Control System	MOVs	Safety	Mitigation Fail
ESF-Component Control System	MOVs	Safety	Core Damage

4. Conclusions

In this paper, to derive digital asset directly affect accident, PRA results (ET, FT, and minimal cut set) are analyzed. According to result of analysis, digital systems related to CD are derived ESF-CCS (safety-related component control system) and Process-CCS (non-safety-related component control system) as well as Engineered Safety Features Actuation System (ESFAS). These digital assets can be identified Vital Digital Asset (VDA).

Hereafter, to develop general methodology which was identified VDA related to accident among CDAs, (1) method using result of minimal cut set in PRA model will be studied and (2) method quantifying result of Digital I&C PRA which is performed to reflect all digital cabinet related to system in FT will be studied.

It is expected that this research is reasonably finding methodology to identify digital assets and improving regulatory efficiency.

REFERENCES

[1] “Computer Security for Nuclear Security(NST045)”, IAEA, 2016.
[2] “Computer Security of Instrumentation and Control Systems at Nuclear Facilities(NST036)”, IAEA, 2014.
[3] “Cyber Security Control Assessments (NEI 13-10)”, NEI, 2015.
[4] “Regulatory Standard on Cyber Security for Nuclear facilities (KINAC/RS-015)”, KINAC, 2014.

[5] “Regulatory Standard on identification of critical digital assets for nuclear facilities (KINAC/RS-015)”, KINAC, 2014.
[6] “"WASH-1400 (NUREG-75/014), An assessment of accident risks in U.S. commercial NPP”, NRC, 1975.