Cyber Security Test Strategy for Non-safety Display System

Han Seong Son[a], Hee Eun Kim[b]
[a] *Department of Computer and Game Science, Joongbu University,*
201 Daehak-ro, Chubu-myeon, Geumsan-gun, Chungnam, 312-702,
[b] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,*
373-1 Guseong-dong,Yuseong-gu, Daejeon 305-701, South Korea
**Corresponding author: hsson@joongbu.ac.kr*

1. Introduction

Cyber security has been a big issue since the instrumentation and control (I&C) system of nuclear power plant (NPP) is digitalized. There were several cyber-attack attempts toward infrastructures including nuclear facilities; Davis-Besse worm infection on 2003, Browns Ferry shutdown on 2006, Stuxnet on 2010, and Black Energy on 2015, etc. A cyber-attack on NPP should be dealt with seriously because it might cause not only economic loss but also the radioactive material release.

Researches on the consequences of cyber-attack onto NPP from a safety point of view have been conducted. A previous study [1] shows the risk effect brought by initiation of event and deterioration of mitigation function by cyber terror. Although this study made conservative assumptions and simplifications, it gives an insight on the effect of cyber-attack. Another study shows that the error on a non-safety display system could cause wrong actions of operators [2]. According to this previous study, the failure of the operator action caused by a cyber-attack on a display system might threaten the safety of the NPP by limiting appropriate mitigation actions.

This study suggests a test strategy focusing on the cyber-attack on the information and display system, which might cause the failure of operator. The test strategy can be suggested to evaluate and complement security measures.

2. Operator error caused by a cyber-attack

2.1. Operator error caused by a cyber-attack on a display system

If an information and display system is attacked by a hacker, it might provide wrong information to the operator. The wrong information might cause the operator to diagnose the state of NPP incorrectly. In this study, it is assumed that the operator always follows the emergency operating procedure (EOP) for he is well trained enough. When incorrect information is provided, it is unavoidable for an operator to commit errors while following the EOP.

In the conventional NPP PSA, the errors of operators are included and also modeled in the FT model. The process of an operator can be divided into three steps; stimulus, organism, and response [3]. In the stimulus step, the operator cannot react properly unless the information is appropriately provided. It is considered in the diagnosis step in Korean standard human reliability assessment.

However, in case of a cyber-attack, the wrong actions are not related to the failure of operator during the cognition process. Furthermore, this kind of error is caused only in a specific situation. Therefore it should be separated from the conventional human error analysis. Conventional human errors are not considered in this study.

2.2. Possible failure caused by operator error caused by a cyber-attack

As it is different from the conventional human error, the cyber-attack-induced errors should be described in the FT model separately. The effect of the wrong actions can be represented as conventional basic events. Based on the conventional FT model, the corresponding basic events are additionally considered. Failure of valve opening is shown in the Fig.1, as an example. Those basic events do not need to be quantitatively assessed, because it is not easy to quantify the depth of cyber-attack and unavoidable operator errors.

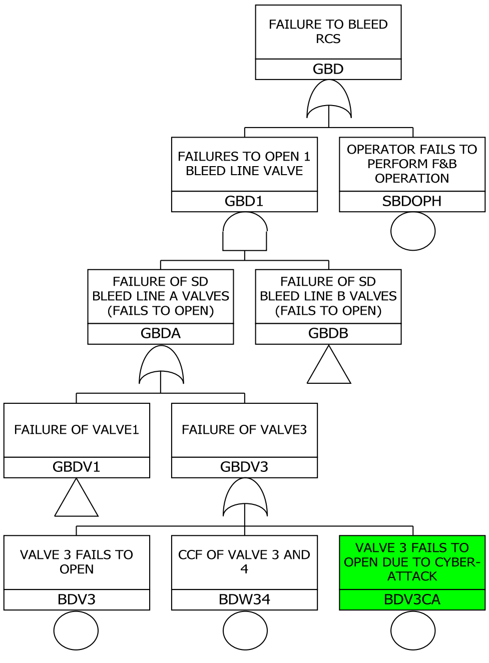
FAILURE TO BLEED RCS
GBD
FAILURES TO OPEN 1 BLEED LINE VALVE
GBD1
OPERATOR FAILS TO PERFORM F&B OPERATION
SBDOPH
FAILURE OF SD BLEED LINE A VALVES (FAILS TO OPEN)
GBDA
FAILURE OF SD BLEED LINE B VALVES (FAILS TO OPEN)
GBDB
FAILURE OF VALVE1
GBDV1
FAILURE OF VALVE3
GBDV3
VALVE 3 FAILS TO OPEN
BDV3
CCF OF VALVE 3 AND 4
BDW34
VALVE 3 FAILS TO OPEN DUE TO CYBER-ATTACK
BDV3CA

Fig.1. FT model with cyber-attack-induced basic event

2.3. Test target scenario

Considering cyber-attack-induced basic events, minimal cut sets (MCS) can be obtained. These MCSs imply the mitigation failure scenarios due to the cyber-attack, including random failure. Among them, the MCSs consisting of only cyber-attack-induced basic events represent the realistic attack scenario the hackers aims at.

Test should be performed focusing on these scenarios since they are closely related to the safety. The integrity of the data which are related to the conditions of each basic event need to be carefully tested.

3. Test strategy

3.1. Analyzing test targets

In this study, it is assumed that the operator concentrate on the LDP and operator console, because those displays provides comprehensive information. The data flow of non-safety information and display system is considered, so the information processing system (IPS) is selected as a test target. The test should be focused on the data which are the elements of the conditions the operators need to check.

There should be some considerations on testing IPS. First, the non-safety system has relatively many attack entry points. The second one is that there might be more known and unknown vulnerabilities, since the non-safety I&C is implemented on the common platform using commercial off-the-shelf. The IPS is a non-safety system and thus performing exhaustive penetration test, which means testing for all attack vectors and vulnerabilities, is not preferable. It is very expensive and time consuming, and moreover, testing should be performed whenever the system is upgraded.

Before testing the security measures applied in the system, the information which is easily detected when it is cyber-attacked needs to be identified first. Some cyber-attack might be detected during maintenance period. It is one of the important characteristics of testing IPS. By providing appropriate maintenance plan the threat from cyber-attack could be detected and reduced during the maintenance testing. However, some types of cyber-attack cannot be detected during the maintenance period because the system might be infected while it is operating. Thus, for the remaining information and attack type, which was not identified as free from cyber-attack, the effectiveness of cyber security measures needs to be tested. The objective of the test is similar to the one of the penetration test performed in the security field.

3.2. Adopting software failure modes

There are various types of cyber-attack, but its intermediate consequences can be described as software failures. Therefore failure modes of software [4] could be adopted for the test strategy development. For example, if the display system is stopped, then the operator could notice the failure. In this case, he can utilize another display in the main control room such as that of safety console. We do not have to consider this kind of cases because the accident could be mitigated by operator. On the other hand, the elaborate data manipulation or the delaying of information transfer should be carefully considered.

The failure modes could be applied to the subcomponent of the test target. The architecture of IPS could be simplified as shown in Fig.2. It consists of DB server, data processing unit and data display unit. DB server has several tables, which is filled with rows of time stamp and corresponding process parameters. It stores process parameters with time stamp, and transfer data by request. Data processing unit requests for data to DB server periodically, calculates and stores results, and transfers data by request. Data display unit requests for calculated results and displays the data periodically.

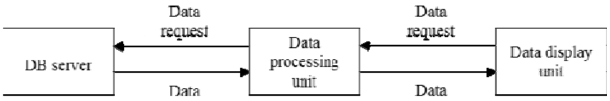

Fig. 2. Simplified architecture of IPS

The failure modes could be applied to each subcomponent of IPS, and need to be checked whether they affect the integrity of data. The test can be performed for the vulnerability which might cause the failure modes.

4. Summary and conclusions

Identifying whether a cyber-attack on the information and display system can affect the mitigation actions of operator, the strategy to obtain test scenarios is suggested. The failure of mitigation scenario is identified first. Then, for the test target in the scenario, software failure modes are applied to identify realistic failure scenarios. Testing should be performed for those scenarios to confirm the integrity of data and to assure effectiveness of security measures.

REFERENCES

[1] H.G. Kang, Risk Effect of Possible Cyber Terror to Nuclear Plants, The 18th Pacific Basin Nuclear Conference, BEXCO, Busan, Korea, March 18-23, 2012

[2] H.E. Kim, et al., An approach to Identify the Risk Induced by Cyber-Attack on the Non-safety NPP I&C System, Transactions of the Korean Nuclear Society Spring Meeting, Jeju, Korea, May 12-13, 2016

[3] Christopher D. Wickens, and Justin G. Hollands, Engineering Psychology and Human performance, Prentice-Hall, 2000.

[4] Bin Li, et al., integrating Software into PRA: A Software-Related Failure Mode Taxonomy, Risk Analysis, Vol 26, No.4, pp. 997-1012, 2006.