DEVELOPMENT OF CYBER SECURITY TEST SCENARIO FOR NON-SAFETY DISPLAY SYSTEM

Hee Eun Kim*
Department of Nuclear and Quantum Engineering
Korea Advanced Institute of Science and Technology
373-1 Guseong-dong,Yuseong-gu, Daejeon 305-701, Republic of Korea
heeeun.kim@kaist.ac.kr

Han Seong Son
Department of Computer and Game Science
Joongbu University
201 Daehak-ro, Chubu-myeon, Geumsan-gun, Chungnam, 312-702, Republic of Korea
hsson@joongbu.ac.kr

Jonghyun Kim
Department of Nuclear Engineering
Chosun University
309 Pilmun-daero, Dong-gu, Gwangju, 61452, Republic of Korea
Jonghyun.kim@chosun.ac.kr

Hyun Gook Kang
Department of Mechanical, Aerospace, and Nuclear Engineering
Rensselaer Polytechnic Institute
Troy, New York, 12180
Kangh6@rpi.edu

ABSTRACT

In order to test the cyber security of NPP related to safety, the results of probabilistic safety assessment were used. The fault tree (FT) is used to reflect the impact of the cyber-attack on the operator. The cyber security test should be performed focusing on the scenario derived from the FT. The concept of a security case has been introduced.

Key Words: cyber security, human error, failure mode

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 have been several cyber-attack attempts toward infrastructures including nuclear facilities. A cyber-attack on NPP should be dealt with seriously because it might cause not only economic loss but also the radioactive material release. A cyber-attack not only can fail a safety component but also can deteriorate the mitigation actions of operators during an accident. The operators judge the status of the NPP by referring displays of the main control room. Therefore the failure of display might cause failure of operator actions threatening the safety of the NPP. This kind of problem has been brought out several times [1, 2]. Display system could be tested to ensure the integrity of information provided to the operator. An intrusion can occur by a malicious hacker from outside or inside worker. In

2003, the Davis-Besse NPP was infected by a Slammer worm which propagated through the corporate network. A certain type of intrusion can be adopted from an attack on the supply chain. There are several studies on the supply chain attack [3, 4]. Most NPP I&C system is isolated from outside, but an inside worker can incapacitate the isolation.

The objective of this study is to suggest cyber security test scenario for a non-safety display system. The scenario is developed based on the possible core damage scenario, so this scenario is related to the safety. By testing the I&C system according to the scenario, the level of security and the safety of NPP can be assured.

2 DEVELOPMENT OF TEST SCENARIO

2.1 Failure of Human Action

As mentioned in the introduction, failure of the display system can cause failure of an operator. The operators refer to the emergency operating procedure (EOP) to perform a specific operation. There are conditions in the steps, and the operator performs a step when the conditions are satisfied. Therefore a cyber-attack on display which shows the conditions will affect the actions of an operator. If the display deliberately shows manipulated conditions that some conditions are not satisfied, the operator has to wait. In that case, the operator cannot perform required actions properly, so the effect is the same as a component fails to run. If the display shows that conditions for component termination are satisfied, operators need to stop the component. The effect is the same as component fails to run. If the display does not show the status of safety signals or failure of components, the operator cannot perform backup properly.

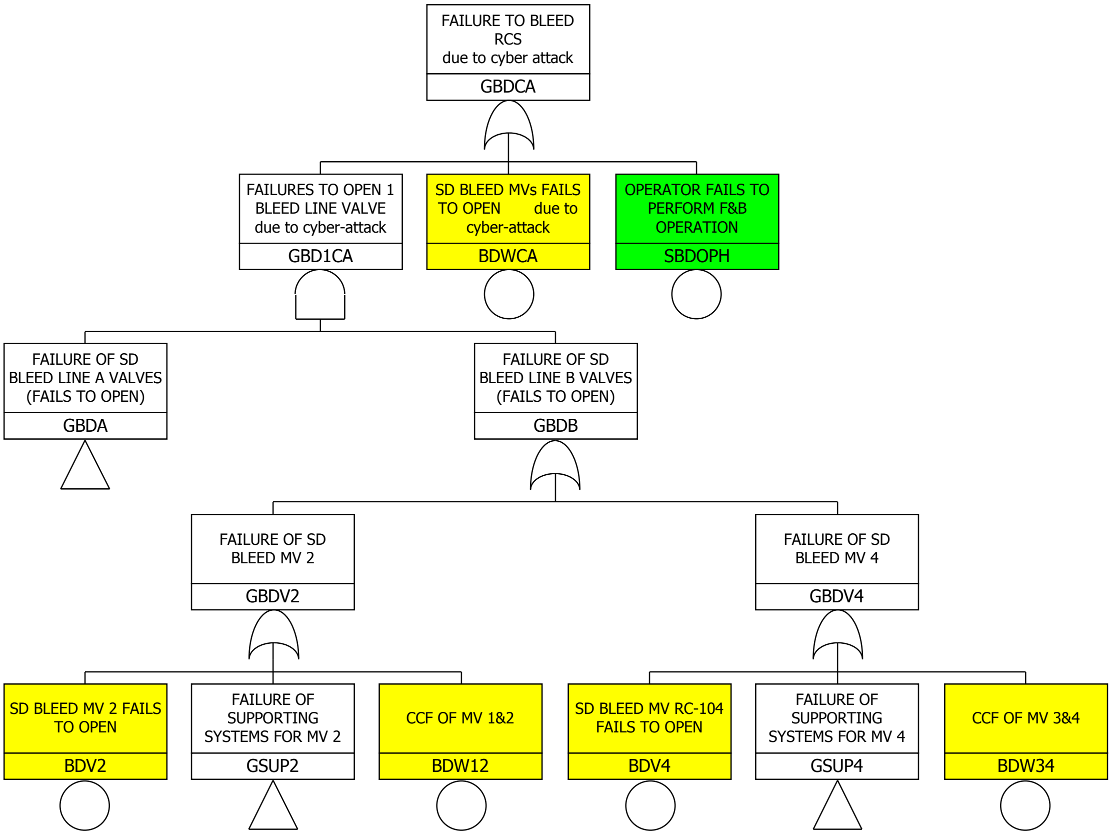
FAILURE TO BLEED RCS due to cyber attack
GBDCA
FAILURES TO OPEN 1 BLEED LINE VALVE due to cyber-attack
GBD1CA
SD BLEED MVs FAILS TO OPEN due to cyber-attack
BDWCA
OPERATOR FAILS TO PERFORM F&B OPERATION
SBDOPH
FAILURE OF SD BLEED LINE A VALVES (FAILS TO OPEN)
GBDA
FAILURE OF SD BLEED LINE B VALVES (FAILS TO OPEN)
GBDB
FAILURE OF SD BLEED MV 2
GBDV2
FAILURE OF SD BLEED MV 4
GBDV4
SD BLEED MV 2 FAILS TO OPEN
BDV2
FAILURE OF SUPPORTING SYSTEMS FOR MV 2
GSUP2
CCF OF MV 1&2
BDW12
SD BLEED MV RC-104 FAILS TO OPEN
BDV4
FAILURE OF SUPPORTING SYSTEMS FOR MV 4
GSUP4
CCF OF MV 3&4
BDW34

Figure 1. FT model which reflects the effect of cyber-attack-induced operator failures

Fig. 1 shows a cyber-attack-induced basic event representing operator fails to open safety depressurization system (SDS) valve. In the conventional NPP PSA, the errors of operators are included and also modeled in the FT model. However, the aspect of operator failure caused by cyber-attack is different from conventional human error. Furthermore, this kind of error is caused only in a specific situation. Therefore, in the previous study of authors [5], these actions were defined as the new failure mode of safety component. The basic event representing these new failure modes can be defined and added in the conventional fault tree (FT) model to reflect the effect of cyber-attack-induced operator failures. Minimal cut sets (MCS) can be obtained considering cyber-attack-induced basic events. 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 hacker aims at. The test should be performed focusing on these scenarios since they are closely related to the safety.

2.2 Failure Mode

As described above, operators refer to display and perform as described in the EOP. Therefore a cyber-attack to display is an effective way of disturbing proper action of operators. However, not every type of cyber-attack can affect the actions of operators. For example, a hacker can attack human-machine interface system to stop the system. In this case, operators would not be deceived, because they can notice the system is attacked. They can continue the operation by referring redundant display such as safety console. On the other hand, the elaborate data manipulation or the delaying of information transfer should be carefully considered. That is to say, the failure mode of display caused by cyber-attack needs to be identified, to illustrate whether a certain type of cyber-attack can affect an operator. Observable failure mode from the view of operators needs to be considered.

Since the effect of a cyber-attack is a failure of some functions, software failure mode can be adopted to illustrate the effect of cyber-attack on display. 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. There are various types of software such as developed by A. M. Neufelder [6], and this failure mode could be adopted for the test strategy development.

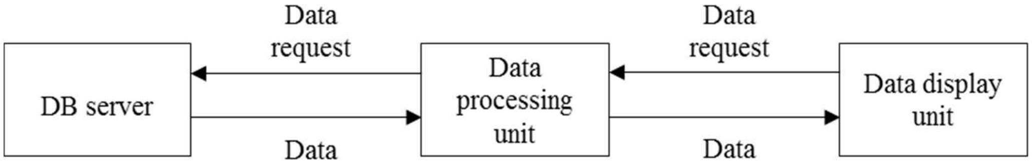

Fig. 2. Simplified architecture of IPS

The failure modes could be applied to each subcomponent of a target system, 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.

3 TEST OF SECURITY CASES

In this study, the penetration test for the security cases is suggested. Description of security case and test target selection based on the security case is described in this section.

3.1 Security Case

A safety case is defined as “A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment” [7]. Similarly, security case is defined as a comprehensive set of test cases to demonstrate that the system is safe from a cyber-attack for a specific application and situation, by referring safety case. Security case can be drawn from core damage scenarios developed from the FT above, since it needs to demonstrate that the system is safe. In case of a cyber-attack on information and display system, the security case includes the components or specific information.

Test can be performed based on the security case. By performing tests and reinforce preventive measures for the security cases, it can be assured that the system is safer from a cyber-attack-induced human error. However, unlike safety cases, security cases need to be verified consistently because the technology of cyber-attack evolves.

3.2 Target Selection for Test

Penetration test is a type of security testing to evaluate a system’s ability to protect the system. Penetration test usually is required when the system is updated or new threats or vulnerabilities are discovered. Since the I&C system of NPP does not change frequently, penetration test needs to be performed when the system is installed, and periodically. Penetration test needs to be performed focusing on the security cases. If a penetration tester can access a data which is included in the security cases, then the behavior of operator can be affected by this attack.

In this study, it is assumed that the operator concentrates on the LDP and operator console, because those displays provide 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. 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.

The security cases are the data which are the elements of the conditions the operators need to check. The test should be focused on these data. Since not every failure of display causes wrong human action, not all vulnerability needs to be tested. For example, among the scenarios, operator failure of opening SDS valve can be caused because of misleading information. Then the security case for this scenario includes the conditions of opening SDS valves, and failure mode to deceive operator. Faulty data [7] is one of the possible software failure modes. The penetration test needs to be performed focusing on this security case. That is to say, if the data representing the SDS valve opening conditions can be manipulated by the effort to penetrate the system, the operator action can be affected, and ultimately the plant can be in a dangerous state. While considering the software failure mode of faulty data, the availability of plant data should be considered. Since the operators are well-trained, they might notice the cyber-attack when the unfamiliar data trend is provided. Therefore the quality of plant data is one of the crucial factors for this failure mode.

4 CONCLUSIONS

By following the suggested method, the test scenarios can be suggested. The failure of mitigation scenario is identified first. Then, for the test target in the scenario, software failure modes can be applied to identify realistic failure scenarios. Testing could be performed for those scenarios to confirm the integrity of data and to assure the effectiveness of security measures. Since the MCSs and corresponding scenarios obtained in this study thoroughly represent the possible scenarios, the result of the testing also can be assured.

By identifying security cases, efficient testing can be performed. The security cases are also directly related to the safety of NPP. The I&C system of NPP usually does not be changed easily because of the regulations. However, security testing should be repeated because the information technology evolves. Therefore identifying the safety cases will be very helpful for periodic security testing. The security cases can also be utilized for training of operators.

5 REFERENCES

1. J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D. Y. Lee, C. K. Lee, "An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants," *Nuclear Engineering Technology*, **45**, pp.637-652 (2013)
2. R. Masood, "Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives," (2016)
3. J. F. Miller, *Supply Chain Attack Framework and Attack Patterns*, MITRE corporation MCLEAN VA, (2013)
4. D. Waalewijin, *Cyber security in the supply chain of industrial embedded devices*, MS thesis, university of Twente (2014)
5. H. E. Kim, H. S. Son, J. Kim, H. G. Kang, "Identification of the Risk Induced by Cyber-attack on Non-safety NPP I&C system,"*13th international conference on Probabilistic Safety Assessment and Management,* Seoul, 10/2-7 (2016)
6. A. M. Neufelder, *Effective Application of Software Failure Mode Effects Analysis*, Quanterion Solutions Incorporated, USA (2014)
7. UK Def, *Safety Management Requirements for Defence Systems*, UK Ministry of Defence (1996)