Identification of the Risk Induced by Cyber-Attack on the Non-safety NPP I&C System

Hee Eun Kim[1], Han Seong Son[2], Jonghyun Kim[3], and Hyun Gook Kang [4, 5]

[1] Department of Nuclear Engineering, Korea Advanced Institute of Science and Technology: KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, heeeun.kim@kaist.ac.kr
[2] Department of Game Engineering, Joongbu University: 201 Daehak-ro, Chubu-myeon, Geumsan-gun, Chungnam, 312-702, hsson@joongbu.ac.kr
[3] Department of Nuclear Energy Engineering, Chosun University, 309 Pilmun-daero, Dong-gu, Gwangju, 61452, jonghyun.kim@Chosun.ac.kr
[4] Department of Nuclear Engineering, Korea Advanced Institute of Science and Technology: KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, hyungook@kaist.ac.kr
[5] Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute: Troy, New York, 12180, hyungook@kaist.ac.kr

Nowadays, the cyber-attack on the infrastructure including nuclear power plant (NPP) is one of the important issue. The risk from cyber-attack on the non-safety system of instrumentation and control system, along with the actions of human operator was studied in this study. The cyber-attack-induced initiating events and failure of mitigation is related to the failure of information display system and failure of operator. In this study, the wrong actions of human operator during mitigation is considered, so the failure of safety functions or safety components were identified from the probabilistic safety assessment result. The scenarios can be suggested by using minimal cut sets. The feed and bleed operation is chosen as a target operation. By analyzing those operation steps, the example scenarios were obtained.

I. INTRODUCTION

Cyber security is considered as one of the important issue of risk assessment of digital instrumentation and control (I&C) system of nuclear power plant (NPP). The digitalization of I&C systems of NPP increased the threat from cyber-attack. There have been several cyber security related accident at the nuclear facilities, including Davis-Besse worm infection in 2003, Browns Ferry shutdown in 2006, Hatch automatic shutdown in 2008, and Stuxnet attack in 2010. Those cases did not caused the release of radioactive materials, but they called the attention to the cyber security issue in the nuclear filed. In Korea, there was a cyber-attack on KHNP on 2014. Even though the critical safety functions were not affected, it shows that the NPP need to be provided for an organized and persistent cyber-attack. For licensee's cyber security plan, US NRC provides regulation guides 10 CFR 73.54.

Kang et al. pointed out that digital system induced initiating events including human errors should be considered in the risk assessment (Ref.1). Furthermore, Kang studied the risk effect of the initiation of accident by cyber-attack and deterioration of mitigation function including human failure by sensitivity study (Ref. 2). Those previous studies implies the importance of the cyber-attack induced initiating events and mitigation failure including the operator action. Song, et al., suggested methods and considerations to define attack vectors for plant protection system (PPS) model (Ref. 3). It shows the possibility of cyber-attack on the critical digital assets of the model PPS through the maintenance devices. In this study, the consequences of malicious attack on the non-safety I&C system will be covered. To identify the risk from cyber-attack the result of PSA will be applied.

In this study, the probabilistic concept will be adopted rather than deterministic approach. In a probabilistic approach, the scenario is developed and mitigation of initiating event is modeled in detail. Multiple failures are considered in the important events, and human reliability assessment is considered in detail. The Sandia National Laboratories (Ref. 4, 5) suggested to adopt FT model for vital area identification. Although this study was done for the physical protection of NPP, it gives insight for the risk induced by the cyber-attack. By identification of MCSs related to the cyber-attack, the way to core damage by cyber-attack can be identified.

II. FAILURE OF HUMAN ACTION UNDER THE CYBER-ATTACK ON THE INFORMATION SYSTEM OF NPP

The failure of human action should be considered carefully in the safety assessment of NPP. It is known that some human error might initiate an anticipated transient, so the possibility of human error due to the cyber-attack also need to be considered. Furthermore, the failure of mitigation by the operator also need to be considered. In the NPP, important safety functions such as the reactor trip and heat removal functions are automated to ensure safety in case of the accident. However, checking the status of operation including backup and maintaining the operation is performed by the operator and operator's actions have priority over the automatically generated signals, so the failure of maintaining the safety functions also might be threaten the safety of NPP. The operator get the information from the information display systems which are generally implemented on the non-safety platform. A previous study also implies that a cyber-attack on information display system might lead an operator to judge the plant state incorrectly (Ref. 3).

II.A. Initiating event induced by cyber-attack

The initiating event can be classified as internal events and external events. Internal events includes plant component failure and failure of operator. Therefore the cyber-attack-induced initiating events need to be considered from both perspectives.

II.A.1. Initiating events caused by direct attack on the plant component

Digitalized equipment have known and unknown vulnerabilities. The failure of each component or system might be caused by an attack on those vulnerabilities. There are several cases which shows that some components of NPP are susceptible for a cyber-attack. The Browns Ferry shutdown is one of the example for possibility of component hacking. High traffic caused failure of both recirculation pumps and condensate demineralizer controller so the plant was manually shutdown. Another example is Hatch automatic shutdown, in which a mistake during software update caused the initiation of safety functions (Ref. 6). Those examples shows possible failure modes and components caused by cyber-attack, and they should be studied more in the security filed. The target components can be selected based on the initiating event.

II.A.2. Initiating events induced by the human action

It is known that human error, so-called category B, can also initiate an unanticipated transient. Therefore an error of operator induced by cyber-attack on the information system need to be considered. A previous study (Ref. 7) shows systematic procedure for identification of human-induced initiating events during low power and shutdown operation. Same procedures can be applied for selecting human errors. Those errors should be examined whether it is related to the failure of information system.

II.B. Failure of mitigation

Although the initiating events were occurred, they can be mitigated by safety functions and operator actions. However, during mitigation, human errors can be induced by cyber-attack on the information system. Davis-Besse Slammer worm infection is an example of cyber-attack on the information system. The information system of the plant was not available for several hours due to the worm. If that kind of attack is combined with the cyber-attack-induced initiating events, the safety of NPP might be threatened.

The failure of operator during mitigation can be identified by analyzing the emergency operating procedure (EOP), and conventional fault tree (FT) model. The FT model includes the failure of safety components which are used for the mitigation of accident. In other words, the failure of components which are not included in the FT are not strictly related to the safety. In this study, the steps are focused on the failure of mitigation.

III. METHODOLOGY DEVELOPMENT

III.A Procedure

The action of human operator can be reviewed based on the EOP. The failures of operator can be represented as basic events. Some errors can be replaced with basic events which is already modeled. However the error-of-commission is not generally modeled in the conventional PSA model, so it could be a new failure mode introduced by cyber-attack. The steps

for identifying instructions of EOP in which the operator would commit error due to the cyber-attack on the information and display system is described in the Fig. 1.

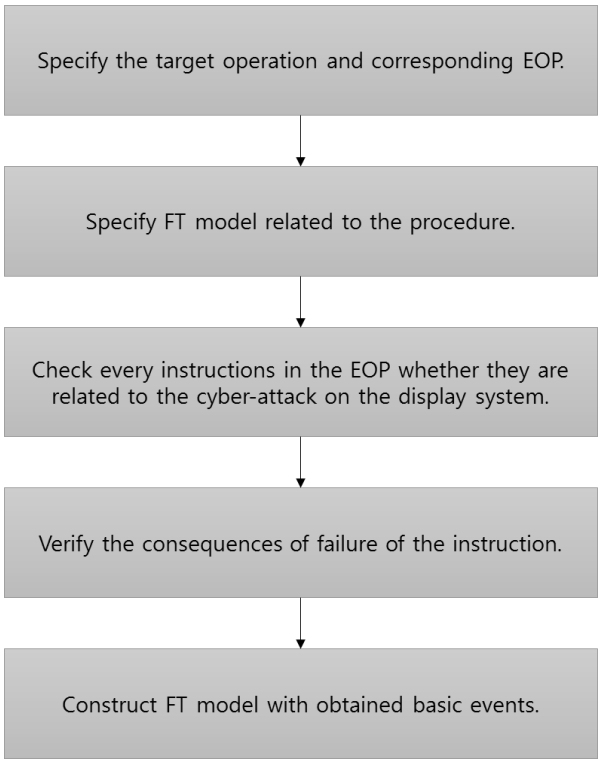

Fig.1. The steps for identifying instructions related to the cyber-attack

III.B Obtaining basic events

By following the steps described in the Fig. 1, the wrong actions can be obtained. The basic event induced by wrong action can be classified as below.

III.B.1. Failure of performing specific EOP

Checking the entry condition of target EOP is the first step of the EOP. The condition should include the plant condition and the status of the corresponding safety component. If the display shows manipulated information that the plant condition does not satisfy the entry condition, the operator has to terminate the procedure and perform other procedures.

III.B.2. Failure of performing specific manual step

Some EOPs include manually started steps. If the conditions for the steps are not satisfied, the operator commit EOO and the effect is same as ‘fails to start’ event of the corresponding component or the signal generation in FT model.

III.B.3. Inappropriate termination of specific steps

A specific step might not be inappropriately terminated by the manipulated information. This type of failure could be represented as ‘fails to run’ event of running component in the FT model.

III.B.4. Inappropriate termination of EOP

EOPs also have the exit conditions and the conditions are presented between the steps or the end of the EOP. The effect might be the failure of several steps.

IV. Example development

The target is F&B operation in case of loss of all feed water (LOAF). The F&B operation directly cools down the reactor coolant system (RCS) when adequate residual heat removal by the secondary cooling system is not available (Fig.2.). The failure of bleeding RCS, failure of SI into the primary system, and failure of recirculation to continue SI are modeled in the conventional PSA model.

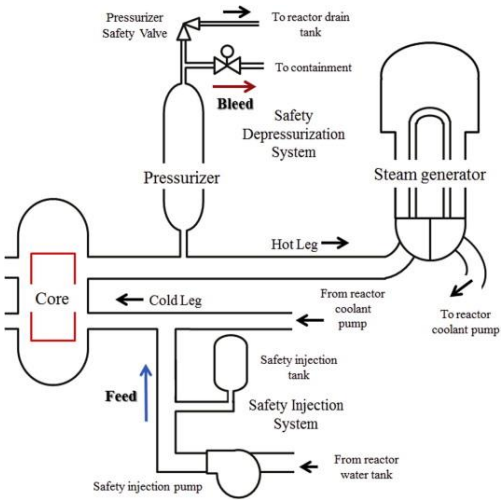

Fig.2. A schematic diagram of the F&B operation (Ref. 7)

An example FT model is shown in the Fig.3. Some example scenarios are described below.

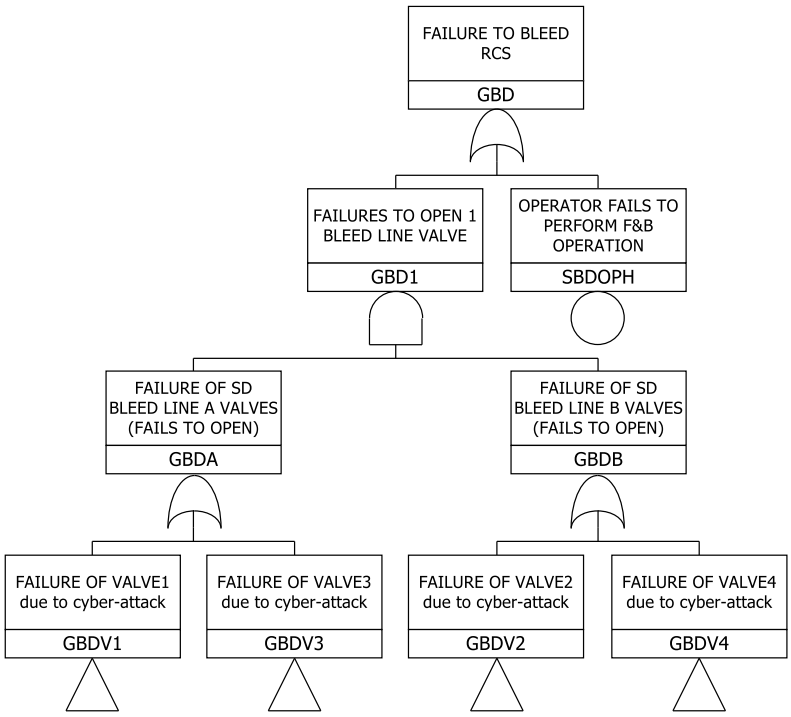

Fig.3. A FT which describes failure of F&B operation due to cyber-attack

- Failure of starting F&B operation procedure: If the display shows that one of the entry conditions are not satisfied, which means the heat removal using SG is available, the operator cannot start F&B operation for RCS heat removal. Then the operator should terminate this procedure and tries to remove heat by using SG. It can be represented as basic event "operator fails to perform F&B operation" of failure of bleeding RCS gate in the conventional FT model.

- Failure of bleeding by opening SDS valve: The F&B operation is started with manual opening of SDS valve. If the display shows the conditions are not satisfied, the operator cannot open the SDS valve. The effect is the same as existing basic event "valve fails to open".

V. Conclusion

A cyber-attack might cause the initiating event including failure of hardware or failure of operator. This initiating event could to be mitigated by safety functions and operator actions, but it also might be disrupted by cyber-attack. The scenario for failure of mitigation was obtained by analyzing EOP and FT model. More realistic result can be obtained if the operational environment, such as diverse display, or use of computerized procedure system, is considered together. Those system can assist the operator's clear judgement.

It is shown that a cyber-attack on the non-safety system might threaten the safety of the NPP. Therefore the security solution on the non-safety information display system also need to be considered carefully.

This study could be reinforced in a more realistic way if the information on the maintenance is considered, because certain type of cyber-attack could be detected during the maintenance.

REFERENCES

1. H. G. Kang and T. Sung, "An analysis of safety-critical digital systems for risk-informed design," *Reliability Engineering & System Safety*, 78, 307–314 (2002)
2. 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)
3. J. G. Song, et. al., "An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants," *Nuclear Engineering and Technology*, **45,** 637-652 (2013)
4. Varnado GB, Ortiz NR, "Fault tree analysis for vital area identification," NUREG/CR-0809 (1979)
5. Stack DW, Francis KA. "Vital area analysis using SETS," NUREG/CR-1487 (1980)
6. Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights*, **10** (2011)
7. Y. Kim and J. Kim, "Identification of human-induced initiating events in the low power and shutdown operation using the Commission Error Search and Assessment method," Nuclear Engineering and Technology, 47, 187–195 (2015)