Identification of the risk induced by malicious attack on the NPP HMI system

KIM Heeeun[1], SON Hanseong[2], KIM Jonghyun[3], and KANG Hyungook[4]

1. Department of Nuclear Engineering, Korea Advanced Institute of Science and Technology, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141 , Republic of Korea (heeeun.kim@kaist.ac.kr)
2. Department of Game Engineering, Joongbu University, 201 Daehak-ro, Chubu-myeon, Geumsan-gun, Chungnam, 312-702, Republic of Korea (hsson@joongbu.ac.kr)
3. Department of Nuclear Energy Engineering, Chosun University, 309 Pilmun-daero, Dong-gu, Gwangju 61452, Republic of Korea (jonghyun.kim@Chosun.ac.kr)
4. Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute, Troy, New York, 12180, United States of America (Kangh6@rpi.edu)

Abstract: The cyber security is one of the important issues in nuclear safety. This study deals with the cyber-attack on the non-safety system of instrumentation and control system, along with the actions of human operator. In this study, the failure of safety functions or safety components were identified from the probabilistic safety assessment result. The failure of safety functions or safety components could be caused by the cyber-attack on the non-safety system. The wrong actions of human operator under the cyber-attack were analyzed based on the emergency operating procedures. The scenarios can be suggested by using those analysis results. The feed and bleed operation is chosen as a target operation. By analyzing those operation steps, we can obtain the list of wrong actions of operator. The type of wrong actions differs from each other according to the step.

Keyword: HMI; cyber security; risk Identification; malicious attack

1 Introduction

Nowadays, the cyber-attack on the infrastructure including nuclear power plant (NPP) is one of the important issue. The threat from cyber-attack has been increased since the instrumentation and control (I&C) systems are digitalized. NPP should be secured from those kind of attacks, because it might cause not only the lack of national energy supply but also the release of radioactive material to the environment.

There are several cyber-attack vulnerabilities in nuclear facilities [1]. For example, on 2003, Davis-Besse NPP was infected by Slammer worm through corporate network, which was not a cyber-attack aimed at the specific target. It resulted malfunction of safety parameter display system. Hatch automatic shutdown shows one of the vulnerability of NPP digital I&C system. In this case, a mistake of a worker during software update caused automatic shutdown. It shows the potential for exploiting system vulnerabilities and the insider. In Korea, there was a cyber-attack on KHNP on 2014. Even though only non-critical information has been leaked, it shows that NPPs could be a target of cyber-attack again. Therefore in this study, malicious attack will be considered as main threat.

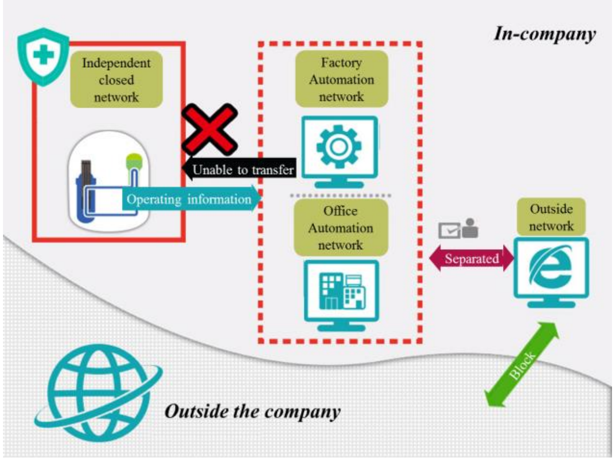

Fig. 1 The network system of KHNP [2].

Another example is Stuxnet, which is considered as advanced persistent threat (APT). Control system of Natanz uranium enrichment facility was isolated from outside network, but Stuxnet was carried by a worker and targeted specific component of the

Received date: November 16, 2016
(Revised date: November 28, 2016)

system. Since the control network of NPP in Korea is isolated from external network (Fig.1.), it has been considered that the cyber-attack on NPP is impossible. However, Stuxnet revealed that the isolated network can be also attacked by hackers. Song *et al*. suggested that cyber-attack can be introduced during maintenance [3]. It is described in the section 2.2 of this paper.

As revealed in the TMI-2 accident, the wrong information lead to the misunderstanding and wrong action of human operator and core damage. Therefore a cyber-attack on display system should be seriously considered. In this study, we assume APT, so the hackers can intrude into the NPP I&C system, especially into the non-safety display system. The consequences of wrong action due to the cyber-attack is the main concern of this paper.

2 Failure of human action under the cyber-attack on the information system of NPP

2.1 Considerations of wrong actions of the human operator

There are several manual backups for safety functions of the NPP. Manual backup is diverse and redundant means for the safety functions. Human operator can affect the safety function, roughly speaking, in two ways. The operator can fail to perform the backup of safety function, or he or she can undo the safety actions. Those two actions are caused by the wrong judgement of operator. The actions are described in detail in the emergency operation procedure (EOP).

Table 1 Description of influence of cyber-attack

	The occurrence of initiating event	Failure of mitigation
Direct cyber-attack on plant component	1st paragraph of 2.1.1	1st paragraph of 2.1.2
Failure of operator due to cyber-attack on display system	2nd paragraph of 2.1.1	2nd paragraph of 2.1.2

The risk effect of cyber-attack can be considered as the initiation of accident and deterioration of mitigation function [4]. Plant component also can be damaged by direct attack. Therefore the influence of cyber-attack can be categorized into four types (Table. 1). Failure of mitigation due to the cyber-attack on display system is considered in this paper.

2.1.1 Initiating event induced by cyber-attack

First, initiating events can be 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 show 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. Those examples show possible failure modes and components caused by cyber-attack, and they should be studied more in the security filed.

Second, initiating events also can be induced by the human action. It is similar to the category B human error, which involves errors that can initiate an unanticipated transient. [5] Therefore an error of operator induced by cyber-attack on the information system need to be considered. A previous study [6] 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.

This initiating event is not that harmful, because it can be managed by the safety system and operator. However, if several NPPs are attacked at the same time, it might cause national power outage.

2.2.2 Failure of mitigation caused by cyber-attack

Although the initiating events have been occurred, they can be mitigated by safety functions and operator actions. In the NPP, important safety functions are automatically initiated by actuation signals from plant protection system. Therefore the cyber-attack on the signal generation component or the control component of safety function will cause the failure of mitigation. The cyber-attacks on the control component of valves, motor *etc*. are frequently reported from industry. This kind of attack cannot be proceeded without insider. However the security level of NPP is very high, so it is quite not to be a probable attack.

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. In that case the operator cannot manage the accident appropriately, because they cannot obtain detailed information about the status of NPP. 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 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.

2.2 Wrong actions caused by wrong information on display by cyber-attack

Human-machine interface (HMI) system of nuclear power plant (NPP) is one of the critical element of NPP risk modeling. Several models which can be applied to the HMI of NPP have been developed. Those models include the information gathering process of operator, and the errors in this process are considered to be important. For example, information gathering process is considered as the first step of the Information – decision - action (IDA) model [7]. According to this model, the errors in the collected information are caused by the erroneous or incomplete information from the source, external filter and internal filter. Among those causes, incomplete, or wrong information might be caused by the malicious attack toward the HMI system.

Song, *et al.* [3] suggested potential malicious attack and corresponding attack vector. Figure 2 shows derived attack vectors during maintenance. A malicious user can access the information processing system (IPS) directly, or through engineering work station (EWS) external and media. Infection can be expanded through other critical digital assets (CDAs) connected to the IPS. Infection can be expanded from safety network through maintenance and test panel (MTP). If IPS is infected, wrong information might be displayed on large display panel (LDP).

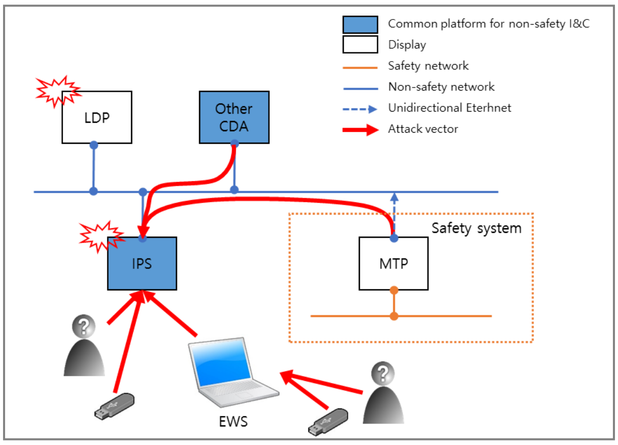

Fig. 2 Possible attack vectors.

2.3 Assumptions of the study

In this study, it is assumed that NPP risk model is perfect that it includes every safety-related human failure. The action of operator in the NPP is prescribed and he has to follow the steps, so it is not allowed for the operator to perform any arbitrary action. Therefore it is assumed that an operator does not make his own decision, and cannot perform arbitrary action. Also, a mistake of an operator is not considered, which means that the operator is guided by the wrong information and decides what he has to do. The failure of the operator is already modeled in the NPP risk model. It is also assumed that the operator concentrates on the operator console, since the operator console provides the essential information.

3 Methods

3.1 Failure of safety action

The errors of human operator are generally classified as error of omission (EOO) or error of commission (EOC). EOO under cyber-attack on the display system can be identified by following EOP steps and checking operator actions. The result of EOO is missing corresponding step. EOCs are not usually modeled in the PSA, however, inappropriate termination of equipment or specific operation could be induced under the intentional cyber-attack on the display system. Inappropriate termination of equipment or specific operation have been considered as EOCs in the previous studies [8, 9]. As we assumed that the operator always follows the EOP and he does not perform arbitrary actions, only this kind of EOC need to be considered. Furthermore, this kind of operator failure occurs only when the termination of equipment is described in the EOP.

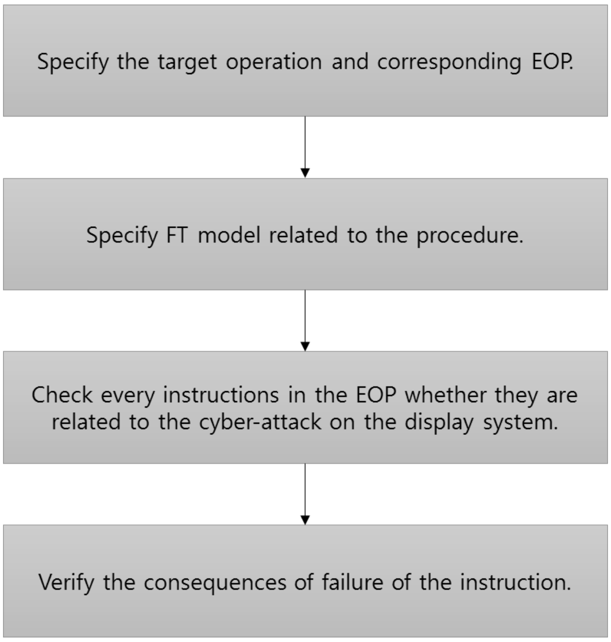
Specify the target operation and corresponding EOP.
Specify FT model related to the procedure.
Check every instructions in the EOP whether they are related to the cyber-attack on the display system.
Verify the consequences of failure of the instruction.

Fig. 4 The steps for identifying instructions related to the cyber-attack.

When the hacker attacked the information and display system, the operator commits errors at the instructions which consist of information acquisition and following conditional instruction. If the instruction step does not include the condition checking process, the operator agent performs the required action without doubt. The steps for identifying instructions in which the operator would commit error due to the cyber-attack on the information and display system is shown in Fig. 4.

If the consequences of failure of the instruction can cause the same effect of conventional basic event, this operator failure should be modeled. This new basic events are added to the conventional FT model, in the same level.

3.2 Identifying core damage scenario by wrong actions caused by cyber-attack

The consequences of failure of the instruction is the failure of equipment or failure of entire procedure. Those failures are the new basic events induced by cyber-attack.

The minimal cut set (MCS) should be identified to verify whether those failures can cause the core damage. If there are MCS with those new basic events, it might be lead to core damage. However, the existence of MCS does not ensure core damage, since the operator can notice the cyber-attack.

4 Results

4.1 Reference operation

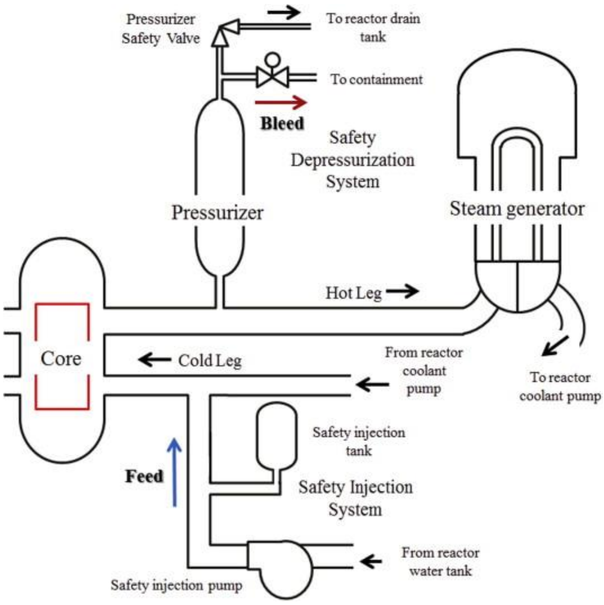

Fig. 5 A schematic diagram of the F&B operation. [10]

Feed and bleed (F&B) operation has been selected as a target operation. F&B operation includes depressurization and injecting water into the primary system, and recirculation to continue HPSI. It was selected because this operation is composed of several steps, and the failure of F&B operation is caused by the failure of the component and the human operator. In this operation, operators may hesitate to initiate an F&B operation if a clear cue is not provided because its initiation will result in the release of radioactive coolant into the containment structure. [10]

4.2 Scenarios

Failure of some components and operator actions can be induced by cyber-attack. Those failures can be represented in the FT model as and they might eventually cause the core damage. Cyber-attack might introduce different consequences in each instruction steps.

It might cause failure of entire F&B operation steps, failure to start or continue operation, or inappropriate termination of F&B operation. The wrong action of operator in each instruction steps causes different result according to the step.

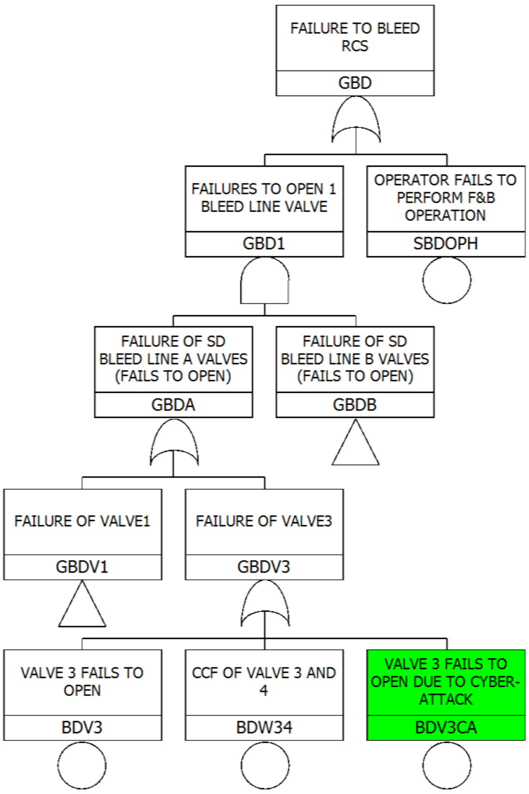
FAILURE TO BLEED RCS
GBD
FAILURES TO OPEN 1 BLEED LINE VALVE
GBD1
OPERATOR FAILS TO PERFORM F&B OPERATION
SBDOPH
FAILURE OF SD BLEED LINE A VALVES (FAILS TO OPEN)
GBDA
FAILURE OF SD BLEED LINE B VALVES (FAILS TO OPEN)
GBDB
FAILURE OF VALVE1
GBDV1
FAILURE OF VALVE3
GBDV3
VALVE 3 FAILS TO OPEN
BDV3
CCF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

Fig. 6 FT model with cyber-attack-induced basic event.

One of the scenario is 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”. This effect can be modeled as “valve fails to open due to cyber-attack”, which is described in Fig. 6. The time limit of this operation is very short, so delay of information can be also an effective way to induce the basic events and core damage.

5 Conclusions

A cyber-attack can cause initiating event by attacking safety or non-safety components, and it also can deteriorate mitigation by attacking safety or non-safety components. In this study, it is shown that a cyber-attack on the non-safety system might threaten the safety of the NPP. More realistic result can be obtained if the operational environment, such as diverse display, or use of computerized procedure system, is considered together. Those systems can assist the operator’s clear judgement.

The risk induced by cyber-attack can be identified by using PSA result. Cyber-attack may cause other risks except for the core damage. Those risks also can be identified by applying this method. 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.

Also, possible set of wrong actions need to be selected, based on the knowledge of I&C system and its vulnerabilities because the hacker might not attack every information. To obtain the realistic result information that can be manipulated need to be listed, because the hacker may not attack certain information, not to be detected during the maintenance.

This study was performed on the assumption that an initiating event already has been occurred, and the analysis was focused on the operator action. Therefore the generation of initiating event should be discussed more. An initiating event might be triggered by operator action during normal operation, in the similar way. It might also occur by the cyber-attack targeting the safety or control system.

In addition, by using the result of this study, the test plan for the cyber-attack can be suggested. If the scenario is given, the criteria for the test target selection can be obtained. It includes the target component and information.

Other types of cyber-attack, or other target need to be investigated to expand the study.

References

[1] KESLER, B.: The Vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insights, 2011, 10:15-25.

[2] http://blog.khnp.co.kr/blog/archives/13030

[3] SONG, J.G., LEE, J.W. PARK, G.Y, KWON, K.C., and LEE, DY.: An analysis of technical security control requirements for digital I&C systems in nuclear power plants, Nuclear Engineering and Technology, 2013, 45(5): 637–652.

[4] KANG, H.G.: Risk Effect of Possible Cyber Terror to Nuclear Plants. In: The 18th Pacific Basin Nuclear Conference, Busan, Korea, 2012,

[5] BASRA, G., *et al.*: Digital instrumentation and control systems in nuclear power plants: International Atomic Energy Agency, 1998.

[6] KIM, Y, and KIM, J.: Identification of human-induced initiating events in the low power and shutdown operation using the Commission Error Search and Assessment method, Nuc Eng Tech, 2015, 47: 187–195

[7] SHEN, S.H., SMIDTS, C., and MOLSEH, A.: A methodology for collection and analysis of human error data based on a cognitive model: IDA, Nuc Eng Des, 1997, 172: 157-186.

[8] JOHN, F., *et al.*: ATHEANA User's Guide (NUREG-1880), Sandia National Laboratories, 2007.

[9] BERNHARD R, and VINH ND.: The Commission Errors Search and Assessment (CESA) Method, Laboratory for Energy Systems Analysis (LEA), 2007.

[10] KIM, *et al.*: Dynamic sequence analysis for feed-and-bleed operation in an OPR1000, Annals of Nuclear Energy, 2014, 71: 361–375.