An approach to Identify the Risk Induced by Cyber-Attack on the Non-safety NPP I&C System

Hee Eun Kim[a], Jonghyun Kim[b], Han Sung Son[c], Hyun Gook Kang[a,*]
[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 373-1 Guseong-dong,Yuseong-gu, Daejeon 305-701, South Korea*
[b] *Department of Nuclear Energy Engineering, Chosun University, 375 Seosuk-dong, Doong-gu, Gwangju 61452, South Korea*
[c] *The Department of Gaming, Joongbu University 201 Daehak-ro, Chubu-myeon, Geumsan-gun, Chungnam, 312-702,*
[*] *Corresponding author: hyungook@kaist.ac.kr*

1. Introduction

Cyber security is considered as one of the important issue of digital instrumentation and control (I&C) system of nuclear power plant (NPP). There are several cyber security related cases: Davis-Besse NPP in 2003, Brown Ferry NPP in 2006, and Hatch NPP in 2008. However, they were not an attack on the safety system or control system. In Korea, there was a cyber-attack on KHNP on 2014. Even though only non-critical information have been leaked, it shows that NPPs are worth to be a target.

In this study, influence of the attack on the non-safety system will be investigated, because the cyber-attack on the safety system cannot be accomplished easily. To identify the risk from cyber-attack, the result of PSA will be applied.

2. Methods

In this section, the target system for the analysis and method to find out the consequences induced by the cyber-attack will be described.

2.1 Target System

The network system of Korea Hydro & Nuclear Power (KHNP) is composed of NPP control system, internal network and public internet. (Fig. 1.) Airgap prevents the attack from the hacker through internet. Therefore it is almost impossible for the hacker to directly attack the NPP control system to cause a transient.

In the APR 1400 I&C system, the operator console is designed in the common platform for non-safety grade, and the related data communication system is non-safety network. They might be more vulnerable than other safety grade system. If the hacker attacks the non-safety system, the operator can be deceived and guided by the wrong information. Song et al. suggested the possibility of cyber-attack on the critical digital assets, during the NPP maintenance and test activities [3].

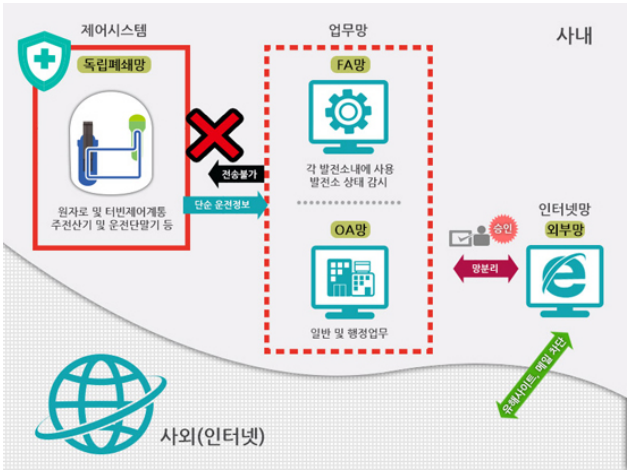

Fig. 1. The network system of KHNP [1].

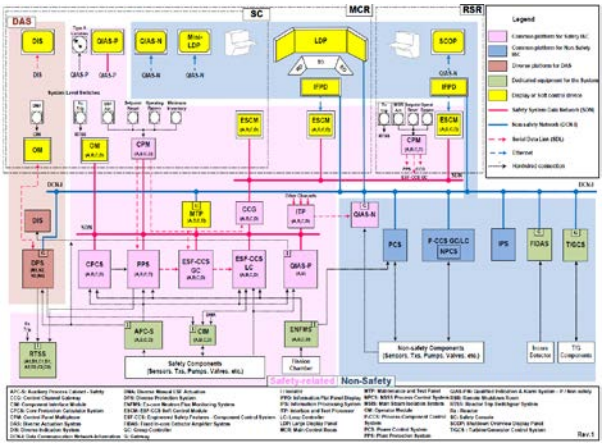

Fig. 2. APR1400 I&C system overview architecture [2].

2.2 Analysis of the PSA Result

Unlike other system, there are manual backup for safety functions of the NPP. Therefore wrong action of human operator caused by cyber-attack need to be considered. To find out the consequences induced by the cyber-attack, basic events of the NPP fault tree (FT) has been analyzed to pick out the safety related

components and actions. In this study, it is assumed that the PSA result is perfect that it includes every failure of components and human operator. A mistake of an operator is out of the scope. Information given to the operator was considered to filter out impossible human failure.

3. Issues related to the cyber-attack on non-safety system

In this section, the target operation for the analysis and risk induced by the cyber-attack will be described.

3.1 Reference operation

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. [4]

3.2 Risks Induced by the Cyber-Attack

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 actions of operator in each instruction steps causes different result according to the step.

Failure of manual operation is failure of backup or recovery operation, so it is not possible to perform other backup or mitigations for wrong action of operator. Operator might undo the safety actions, which cannot be turn back automatically. The operator manipulates several channels concurrently, therefore it causes disabling of redundancy.

Minimal cut set consists exclusively of cyber-attack induced basic events can be obtained. This minimal cut set represents the effective cyber-attack which may cause the core damage. It can be interpreted as a scenario.

4. Conclusions

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.

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] http://blog.khnp.co.kr/blog/archives/13030
[2] Safety I&C System for the APR1400, KEPCO & KHNP, 2013
[3] Song et al., An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants, Nuclear Engineering and Technology, Vol 45, Issue 5, P 637–652, 2013
[4] Kim et al., Dynamic sequence analysis for feed-and-bleed operation in an OPR1000, Annals of Nuclear Energy, Vol 71, P 361–375, 2014