A Proposal for a Methodology to Develop a Cyber-Attack Penetration Test Scenario Including NPPs Safety

In Hyo Lee[a], Han Seong Son[b*], Si Won Kim[c], Hyun Gook Kang[d]
[a]Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,
291 Daehak-ro, Yuseong-gu, Daejeon, South Korea
[b]Computer and Game Science, Joongbu Univ., 201 Daehak-ro, Geumsan-gun, Chungnam, South Korea
[c]Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yusung-gu, Daejeon, Korea 34054
[d]Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute,
110 8th Street, Troy, New York, USA
**Corresponding author: hsson@joongbu.ac.kr*

1. Introduction

Cyber security of nuclear power plants became an important issue because of the digitalization of NPPs. Penetration test is a method to evaluate the cyber security of NPPs; so, this approach was performed in some studies [1, 2, 3]. Because they focused on vulnerability finding or test bed construction, scenario based approach was not performed. However, to test the cyber security of NPPs, a proper test scenario should be needed. Ahn et al. [4] developed cyber-attack scenarios but those scenarios couldn't be applied in penetration test because they developed the scenarios based on past incidents of NPPs induced by cyber-attack. That is, those scenarios only covered scenarios which were happened before; so, they couldn't cover other various scenarios and couldn't reflect them into a penetration test.

In this study, a method to develop a cyber-attack penetration test scenario of NPPs especially focused on safety point of view is suggested.

2. Procedure of the Cyber-Attack Penetration Test Scenario Development

In this section a method to develop a cyber-attack penetration test scenario is described. The procedure can be summarized as in Fig. 1.

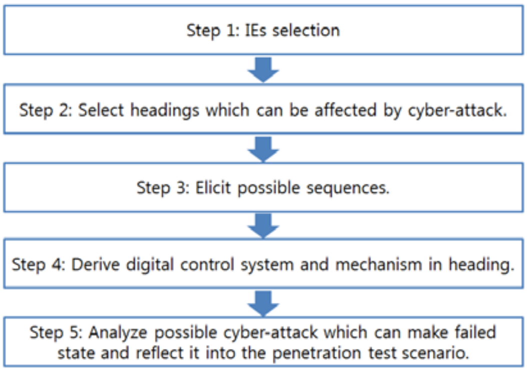
Step 1: IEs selection
Step 2: Select headings which can be affected by cyber-attack.
Step 3: Elicit possible sequences.
Step 4: Derive digital control system and mechanism in heading.
Step 5: Analyze possible cyber-attack which can make failed state and reflect it into the penetration test scenario.

Fig. 1. Summarized procedure of penetration test scenario development.

2.1 IEs Selection

To deal with the cyber security including plant safety, Level 1 PSA results can be utilized. In the plant safety point of view, nuclear fuel integrity must be maintained and radioactive material must not be released to the environment. However, in this study, we only considered nuclear fuel integrity. In the Level 1 PSA, if initiating event (IE) was happened and heat couldn't be removed by mitigation systems, nuclear fuel integrity of NPPs is lost. Because some IEs can be caused by cyber-attack [5,6], selecting possible IEs can be a starting point of the cyber-attack penetration test scenario development.

2.2 Heading Selection

After the IE selection, event tree (ET) should be analyzed because if the mitigation systems or actions were failed, nuclear fuel integrity can be deteriorated. In the ET, an accident sequence starts from the IE and splits into two state (success or fail) when it meets mitigation action (heading). If the heading fails because of the cyber-attack, accident sequence goes to the failed state. For example, headings like "failure of steam removal via MSSVs", "unfavorable moderate temperature coefficient" can be excluded because their failure causes are not related to the cyber-attack. However, headings like "failure of delivering AFW", "failure of HPSIS injection" should be analyzed more detail because they can be failed by cyber-attack. This detailed heading analysis is explained in sub section 2.4.

2.3 Possible Sequences Elicitation

If headings which can be affected by cyber-attack are selected, accident sequences can be summarized. In other words, only accident sequence which can be caused by cyber-attack is remained. Although the remained sequences are occurred by cyber-attack, some sequences hard to be occurred. For example, in case AFW was successfully injected but it isn't injected continuously, this accident sequence should be reconsidered as a target scenario. Because if AFW was successfully injected at the early stage, there might be more chance to cool the reactor. And this sequence may be happened by random failure but hard to implement by cyber-attack at the proper moment. So, in this stage, we should rethink accident sequences hard to be implemented by cyber-attack.

2.4 Detailed Heading Analysis

In this step, headings are analyzed more specifically to develop the accident sequences into a cyber-attack penetration test scenario. Each heading is modeled by fault tree (FT) and some basic events can be affected by cyber-attack. For example, in case of motor operated valve failure, this event can be occurred if a hacker attacks the related digital control system. However, in case of check valve failure, this event can't be occurred by cyber-attack because it is a passive system. So, by analyzing failure mechanism of basic events in the headings, all basic events which can't be occurred by cyber-attack are removed. Also, digital control system of each basic event is identified in this step.

2.5 Cyber-Attack Analysis

Actual failure state such as "valve fail to open" is modeled in PSA model. However, to develop the cyber-attack penetration test scenario, we should identify how the cyber-attack can make that failed state. Hacker's attack goal can be defined by actual failure state as explained. Therefore, based on actual failure state, identification of attack modes including attack type can be performed. Also, there should be defects on that system to implement the cyber-attack on digital control system. From the digital control system of each basic event in sub section 2.5, its vulnerability is identified.

3. Conclusions

To evaluate the cyber security of NPPs, penetration test can be a possible way. In this study, a method to develop a penetration test scenario was explained. Especially, the goal of hacker was focused on nuclear fuel integrity deterioration. So, in the methodology, Level 1 PSA results were utilized to reflect plant safety into the security. From the PSA results, basic event was post processed and possible cyber-attacks were reviewed with vulnerabilities of digital control system.

By following this methodology, it is expected that various penetration test scenarios can be developed which are reflecting safety point of view.

Acknowledgement

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KOFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea (Grant code: No. 1605007-0116-WT111)

REFERENCES

[1] Yongkyu An, Calogero SOLLIMA, and Rizwan-uddin, A Test Bed for Digital I&C and Cyber Security for NPPs, NPIC & HMIT 2015, Charlotte, NC, February 22-26, 2015.

[2] Jinsoo Shin, Gyunyoung Heo, Hanseong Son, Yongkyu An, Rizwan-uddin, Implementation of a RPS Cyber Security Test-bed with Two PLCs, Transactions of the Korean Nuclear Society Autumn Meeting Gyeongju, Korea, October 29-30, 2015.

[3] JAE-GU SONG, JUNG-WOON LEE, GEE-YOUNG PARK, KEE-CHOON KWON, DONG-YOUNG LEE, and CHEOL-KWON LEE, AN ANALYSIS OF TECHNICAL SECURITY CONTROL REQUIREMENTS FOR DIGITAL I&C SYSTEMS IN NUCLEAR POWER PLANTS, NUCLEAR ENGINEERING AND TECHNOLOGY, VOL.45, NO.5, 2013.

[4] Woogeun Ahn, Manhyun Chung, Byung-Gil Min, and Jungtaek Seo, Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs, International Journal of Distributed Sensor Networks, Volume 2015, 2015.

[5] Hyun Gook Kang, RISK EFFECT OF POSSIBLE CYBER TERROR TO NUCLEAR PLANTS, The 18th Pacific Basin Nuclear Conference (PBNC 2012), BEXCO, Busan, Korea, March 18~23, 2012.

[6] In Hyo Lee, Han Seong Son, Hyun Gook Kang, An Analysis of Cyber-Attack on NPP Considering Physical Impact, Transactions of the Korean Nuclear Society Spring Meeting Jeju, Korea, May 11-13, 2016.