Application of Vital Area Identification on Cyber Security at a Nuclear Power Plant

Jeong-ho Lee
KINAC, 1418, Yuseong-daero, Daejeon, Republic of Korea 34101
**Corresponding author: friend25kr@kinac.re.kr*

1. Introduction

Since "Who am I" incident happened to Korea Hydro and Nuclear Power Co. Ltd. (KHNP) in 2015, the Korea government started cyber regulation on its nuclear power plants. At first, the Design Basis Threat (DBT) was revised including cyber threat in 2015 along with the existing physical threat. Then, the newly introduced cyber regulation had been planned according to the seven stages staring from forming a cyber security organization in a nuclear operator, identifying critical digital assets, and so on to implementing technical security measures. We had finished the seven scheduled steps in order to introduce cyber security regulation in the nuclear security regulation. In 2022, we are about to finish the follow-up measures founded from the seven steps of cyber security regulation introduction. Now, we are standing at the starting point of the second phase. In this paper, we would like to discuss what we are planning for the second phase of cyber security regulation.

2. Cyber Security Regulation 1.0

The cyber security regulation is the newest one in nuclear regulation. Nuclear Safety and Security Commission (NSSC) and KINAC prepared the regulation with revising DBT, amending the legal and regulatory requirements, and so on. As those were prepared, we established the plan to introduce the new cyber security regulation at a nuclear facility with seven stages:

1. Forming Cyber Security Organizations
2. Identifying Critical Digital Assets
3. Establishing Defense in Depth Strategy and Incident Response Program
4. Establishing Portable Media and Mobile Device Control Program
5. Establishing Integrity Control Program
6. Establishing Operation / Management Security Control Program
7. Establishing Technical Security Control Program

As those introduction processes are almost finished, the next step must be considered.

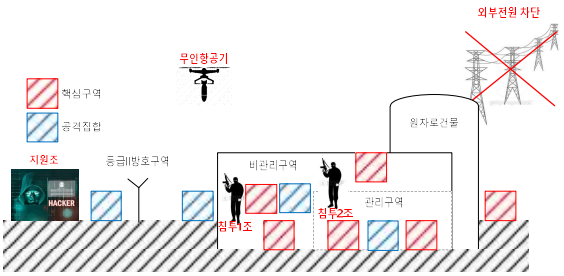
3. Cyber Security Regulation 2.0

When the cyber security regulatory were prepared and newly introduced, the cyber security itself was the main focus. We focused only cyber threat in DBT. We focused only cyber security strategy and measures.

It is time we have to ask questions like:

- How incidents might be progressed if physical and cyber threat happen, so called blended attack, at the same time?
- Are the cyber security strategy and measures effective in this case?

In order to answer those questions, cyber security needs to be interfaced with other domains such as physical protection and safety. The incident[1] happened at the nuclear facility in Syria in 2007 gives us insights to understand what blended attack might look like. Cyber attack might play role to assist intruders and/or to escalate consequences of attack by disrupting CDA functions.



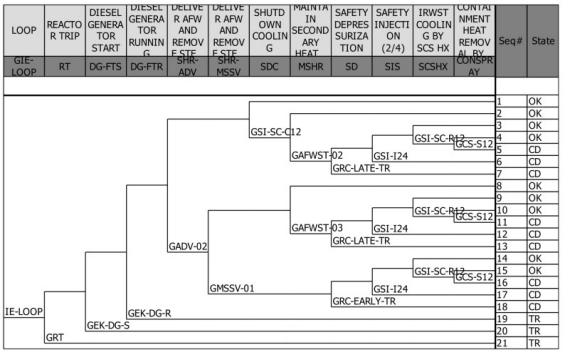
Pic. 1. Blended Attack at a nuclear power plant

Taking a close look at the vital area identification (VAI) process helps us to understand how blended attack might be progressed at a nuclear power plant. IAEA guideline and other documents [1-2] describes basic assumptions including cyber threat to identify vital area candidates to prevent high radiological consequence (HRC) as depicted in Pic. 1. Adversaries disrupts offsite power before they start attack. Then, the adversaries will breach protected areas and approach to target sets.

This attack scenario in VAI process can be understood in terms of how it will progress based on safety analysis. Pic. 2 is the event tree for the case when offsite power is lost (LOOP, Loss of Offsite Power) happens. In the tree, safety systems are depicted in order to mitigate the LOOP event. The targets for the

[1] It was known as "Operation Orchard."

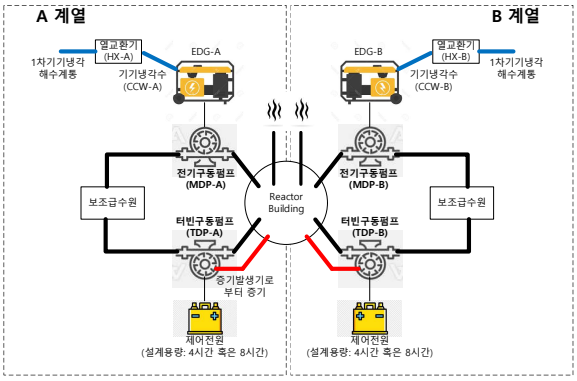
adversaries are the safety systems whose functional failure cause core damage (HRC).



Pic. 2. An Event Tree for LOOP

When offsite power is disrupted, a reactor is tripped, and one of emergency diesel generators (EDG) is started, and secondary cooling system removes the residual heat from the reactor core in order to prevent core damage. The adversaries will try to disrupt some of those functions by physical and/or cyber attacks.

Taking a close look at each of those events will be our next step in cyber security regulation. Those are the questions we are going to ask: reactor trip process can be disturbed by cyber means? EDG start up can be interrupted by cyber means? Delivering auxiliary feed water can be disrupted by cyber means? And so on.



Pic. 3. Safety Systems at a Nuclear Power Plant

We have to break down each of events in Pic. 2 into the system or component level as depicted in the Pic. 3. And, once again, we need to go into digital elements level which can affect to the systems or components. We have to come up with answers if those are possible, which digital elements need to be compromised. When we have answers of those questions, we will be able to improve cyber security regulation and implementation.

4. Conclusion and Future Works

In this paper, we described briefly history of the cyber security regulation since 2015. We discussed the way we introduced the cyber security regulation in order to implant it into the existing nuclear security regulation. While we implanting it, we only focused on the cyber security itself.

For the next step, we are going to seek a way to interface the cyber security with other domain such as physical protection and safety. We have to consider whether current cyber security measures would be well enough to protect nuclear facilities from blended, physical and cyber, attacks. In order to evaluate what we have done so far, we need to look into how attacks will progress in system or component level of a nuclear facility.

REFERENCES

[1] IAEA, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).

[2] SANDIA NATIONAL LABORATORIES, A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities, SAND2004-2866, SNL, Albuquerque, NM (2005).