Vital Area Identification in a Nuclear Power Plant and Regulatory Revision

Jeong-ho Lee
KINAC
friend25kr@kinac.re.kr

1. Introduction

The Fukushima disaster was an eye opening accident in human history. Station blackout caused by tsunami resulted in core damages in the Fukushima Daiichi nuclear power plants. The devastated accident rang the loud alarm in not only nuclear safety world but also nuclear security world. It was difficult to admit, however it provided some insights to terrorists on how to attack a nuclear power plant leading to significant radiological consequences. The unpleasant concern is not groundless if we consider the uncovered plot from the investigation of 911 terrorist attack. The initial plan was to target a nuclear power plant rather than the World Trade Center and the Pentagon. We learned two lessons from those tragedies: there are terrorist groups watching for a chance to attack a nuclear power plant, and they might improve their strategies based on what they realized from the Fukushima accident.

The lessons make Korean nuclear security society look back the nuclear security regime and its implementation. The Korean government requested IAEA for International Physical Protection Advisory Service (IPPAS) to review the Korean nuclear security infrastructure based on the international standards. The Korean regulatory bodies reassessed evolving threat environment with competent authorities in order to update the Design Basis Threat (DBT). The regulatory bodies requested nuclear power plant operators to re-identify their vital areas and reassess their protective measures.

In this paper, we would like to introduce some of our works related to vital area identification and protection. First, we will discuss what vital areas are. And then, we will introduce methodologies and software tools we developed to identify vital areas. At last, we will address our efforts to strengthen vital area protection including regulatory revision.

2. Vital Area Identification

2.1 Vital Areas

Vital areas are well defined in IAEA nuclear security series (NSS) 13, so called INFCIRC/225/Rev.5. INFCIRC/225/Rev.5 recommends to identify and protect vital areas at a nuclear facility, the sabotage which of could directly or indirectly lead to high radiological consequences1 [1-2].

Figure 1. Graded approach against sabotage stated in IAEA NSS 13.

There are two kinds of vital areas [6]: one is to protect a facility from direct sabotage, the other is to protect from indirect sabotage. Direct sabotage is done by applying energy from an external source, for example explosives, to release radioactive material directly at a nuclear or radioactive material inventory. Indirect sabotage is accomplished by using the potential energy, for instance heat or pressure, contained in the nuclear or radioactive material or in a process system to disperse the material. Vital areas to protect from direct sabotage are areas where nuclear or radioactive material is stored or used, sabotage which of could lead to high radiological consequences. The other vital areas to protect from indirect sabotage contains critical safety systems, for example whose functions are control of reactivity, cooling of radioactive material, and confinement of radioactive material.

2.2 Vital Area Identification Process

There are several concepts to understand before we discuss vital area identification process. It is also important to understand relationships between those concepts. In this section, we will briefly discuss important concepts, and their relations, and overall vital area identification process [6-9].

[1] IAEA NSS-13 does not provide any information on what high radiological consequence is. It might be opened for member states to decide the threshold. Korean regulatory body set high radiological consequence as core damage.

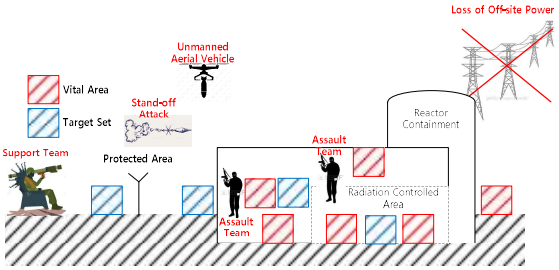

Figure 2. Vital areas, target sets, and DBT

Vital areas are to prevent core damage, which is high radiological consequences in Korea, by adversary attack based on design basis threat. Target sets are combinations of areas, sabotage which of could potentially could lead to core damage. It might be difficult to distinguish between target sets and vital areas. Vital areas are some of areas among target sets to prevent core damage. It is an important assumption in vital area identification that functions of an unprotected system will be lost during sabotage attack. For instance, we should assume that adversaries cut off-site power before they start to attack the site.

Vital area identification process usually starts from looking at a nuclear facility itself. Important information is nuclear or radioactive inventories to identify direct sabotage targets and safety systems to identify indirect sabotage targets. Direct sabotage target in case of a nuclear power plant are usually spent fuel pools and reactor containments. On the other hand, identifying indirect sabotage targets is difficult and complex. There are several ways to identifying indirect sabotage targets. They are described in IAEA NSS No. 16.

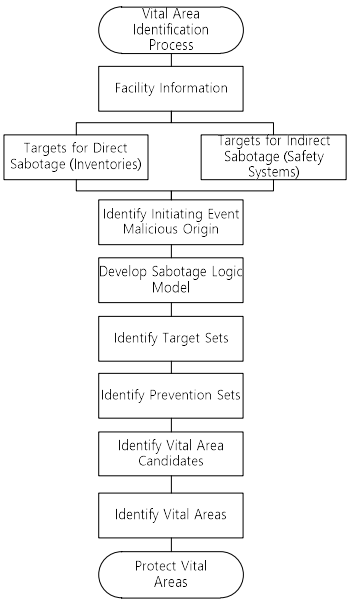

Figure 3. Vital Area Identification Process

Safety analysis on a nuclear facility is a good starting point for identifying indirect sabotage targets. Probabilistic Risk Analysis (PRA) is a widely-used method for safety analysis of a nuclear power plant. A PRA model describes development of situation from initiating events such as systems/components failure, human error, and so on to core damage in detail [3-5].

The first step with the PRA Model is to identify initiating events with malicious origin by introducing new initiating events which are not considered in safety analysis and by getting rid of initiating events beyond adversary capability based on DBT. Safety analysis does not pay much attention to disabling of passive components such as pipe breakage, water tank rupture, cable teardown, and so on. However, those events can happen by malicious attack, so that those should be considered as initiating events with malicious intention. Another thing worth to notice is that safety analysis considers many non-security-related factors such as random failure, common cause failure of system/components, human error, and so on. Time frame that safety analysis concerns is a lifetime of a facility. Those failures and human error would (or should) have pretty low probabilities. Those unlike-to-happen events might be meaningful for the long time period. However, sabotage attack and its consequences are estimated to last for less than a day or days. It will be reasonable to consider those failures will not happen during sabotage attack. Modifying the PRA model from the perspective of nuclear security event is to develop a sabotage logic model.

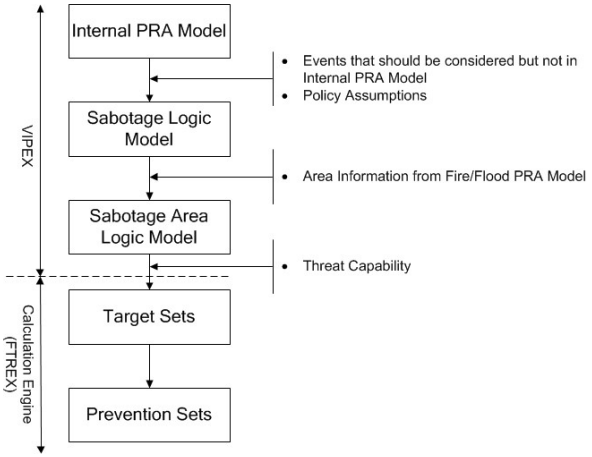

Figure 4. Indirect Sabotage Target Identification Process

The next step is to identify target sets and prevention sets from the sabotage logic model. The sabotage logic model does not look much different from the RPA model since main interest of the PRA model is on systems or components not areas. The sabotage logic model should be converted to sabotage area logic model by converting each entity in the sabotage logic model to an area where the entity could happen. We developed

the sabotage area logic model with area information included in Fire and Flood PRA models.

The sabotage area logic model can be interpreted as paths from normal operation to core damage. Each path is a set of areas disabled by adversaries to achieve core damage. The figure 5 present relationship between sabotage area logic model and the paths (the potential target sets). The paths can be grouped by the number of elements in the sets. The first path in the potential target sets of the figure 5 means that disabling only one area (R5) leads to core damage. The second path is to disable two areas (R4 and R5) resulting in core damage. We need to limit the number of areas that adversaries are able to disabling by assessing their capability and by evaluating response competence.

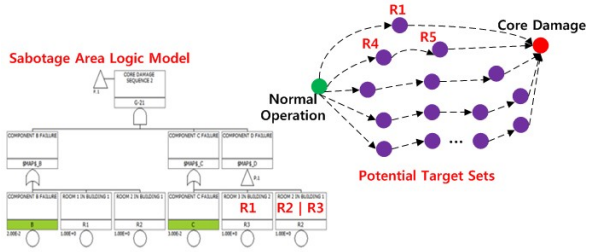

Figure 5. PRA Model and Target Sets

The potential target sets can be presented as Boolean algebra:

<Potential Target Sets>

CD[2] = (R1) + (R4 * R5) + (R4 * R7) + … + (R8 * R9) + (R9 * R10 * R11) + …

Suppose we conclude that adversaries are only capable of disabling only two areas before they are neutralized by response force, we could cut off the paths (potential target sets) with more than three areas. Then, we have the target sets under threat capability:

<Target Sets>

CD = (R1) + (R4 * R5) + (R4 * R7) + … + (R8 * R9)

The prevention sets are the other side of a coin with the target sets on one side. As we discussed, the target sets are sets of area that adversaries should disable in order for core damage. So to speak, it is one way of looking at a nuclear facility from the perspective of adversaries. However, the prevention sets are sets of areas to protect a nuclear facility from core damage. It is the other way of understanding a nuclear facility from the perspective of physical protection. We could generate the prevention sets by applying De Morgan's laws to the target sets.

<Prevention Sets>

$$\overline{CD} = \overline{R1} * (\overline{R4} + \overline{R5}) * (\overline{R4} + \overline{R7}) * \ldots * (\overline{R8} + \overline{R9})$$

[2] "CD" stands for core damage.

It is also identical with:

$$\overline{CD} = \overline{R1} * \overline{R4} * \ldots * \overline{R8} + \overline{R1} * \overline{R4} * \ldots * \overline{R9} + \cdots + \overline{R1} * \overline{R5} * \ldots * \overline{R9}$$

The prevention sets are represented as the unions of sets with the intersections of areas. This means that core damage can be prevented from in the case when at least one intersection of areas is intact from sabotage attack. All those interactions of areas can be considered as vital area candidates. We could select one of the intersections of areas as vital areas.

We developed an assisting software tool for vital area identification so called "Vital Area Identification Package Expert" (VIPEX) in 2012. The software tool is used to develop a sabotage area logic model from an internal PRA model. The software work with the calculation engine called "Fault Tree Reliability Evaluation eXpert" (FTREX) to generation targets sets and prevention sets from the sabotage area logic model. We provided the VIPEX and FTREX to IAEA for training purpose in 2010 [6].

Currently, we are using these software tools for identifying vial areas at nuclear power plants in operation and under construction in Korea. We have just finished identifying vital areas of nuclear power plants 3 whose reactor types are APR-1400 and the newest model of OPR-1000. We are still working on early designs of OPR-1000, CANDU types, and others.

2.3 Regulatory Revision for Vital Area Protection

We have realized some regulatory improvements while we were re-identifying vital areas of nuclear power plants. We could refine our vital area identification process and methodologies. The refined process and methodologies are reflected to the regulatory standard on vital area identification.

Beside vital area identification itself, the most valuable lesson that we learned is that protective measures and contingency response planning focus on not only vital areas but also target sets. Target sets are paths to high radiological consequences disabled by adversaries. They are adversaries' objective to attack a nuclear power plant. Even though protecting vital areas prevents from leading to high radiological consequences, loss of some of target sets increases possibility to high radiological consequences. The risk can be reduced by putting Protective measures in place and planning for contingency response on target set. Our regulatory

3 There are several types of nuclear reactors in Korea. We have Pressurized Water Reactors (PWRs) such as APR-1400, OPR-1000 and its early models, Framatomes, and Westinghouses. Also, we have Pressurized Heavy-Water Reactors (PHWRs) such as CANDU.

framework is based on IAEA recommendations, so that regulatory requirements are mostly on vital areas. We need to revise our regulatory requirements strengthening protection of target sets. For example, 10 CFR Part 734 requires to have protective strategies and management program for target sets. Also, we are working on updating design specification of protective structures for protective structures.

Target sets, along with vital areas, are important interface between security contingency plan and radiological emergency plan5. Functional loss of safety system in target sets not only by safety reasons but also by security events raises risk of radiological emergency. Security events related to target sets should activate not only contingency plan but also emergency plan. Of course, contingency response and emergency response should be coordinated. Current emergency plans in Korean nuclear power plants identify security events on critical safety systems as initiating events. Those emergency plans should be updated according to re-identified target sets in each nuclear power plant.

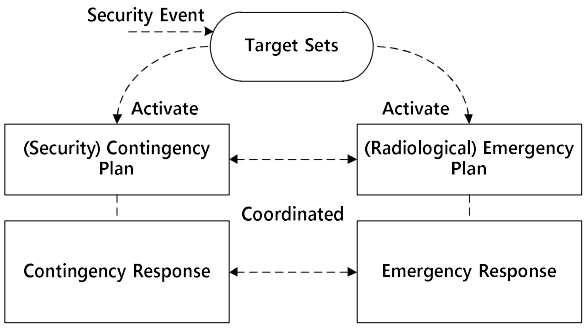

Figure 6. Target Set and Contingency/Emergency Plans

3. Conclusions

There are several works that we have to clarify further in vital area identification process. One of them is how to assess adversaries' capability. As we discussed in the vital area identification process, target sets are cut off from potential target sets according to adversaries' capability. It sounds simple, however it is not. It is difficult to answer the question that how many areas adversaries are capable of disable before they are neutralized. It depends not only on adversaries' capability but also on response forces capability. We need to develop a systematical methodology to address the question.

[4] 10 CFR Part 73 is the Federal regulations for physical protection of plants and material in United States. The requirements for target sets can be found in 73.55.

[5] According to IAEA guidelines, contingency plan is for security events, and emergency plan is for radiological incidents.

Another work, also, is required to deal with spatial interactions. A security event in one area can affect adjacent areas. For example, explosion in an area can disrupt a water pipe, and flooding from the pipe can disable safety systems in nearby areas. The spatial interaction has an influence on a sabotage area logic model which describes the development of the situation caused by sabotage attack. Let's suppose the explosion in the area R4 make impacts on the adjacent areas, R8 and R9 depicted in the Figure 8. In this case, the spatial interactions, expressed in the red arrows, adds two more paths to core damage in a sabotage area logic model. We need to conduct thorough study on spatial interactions in a nuclear power plants.

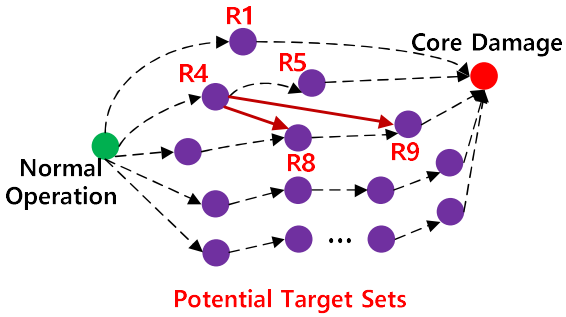

Figure 7. Spatial Interaction in Vital Area Identification Process

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012)

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

[8] VARNADO, G.B., ORTIZ, N.R., Fault Tree Analysis for Vital Area Identification, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, Nuclear Regulatory Commission, Washington, DC (1979).

[9] KOREA ATOMIC ENERGY RESEARCH INSTITUTE, The Application of PSA Techniques to the Vital Area Identification of Nuclear Power Plants, KAERI, Seoul (2004).