Modern Environmental Science and Engineering (ISSN 2333-2581)
May 2018, Volume 4, No. 4, pp. 460-468
Doi: 10.15341/mese(2333-2581)/05.04.2018/008
Academic Star Publishing Company, 2018
www.academicstar.us

Application to Vital Areas Identification of Nuclear Power Plants Based on PSA

Minho Kang, and Moonsung Koh

Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea

Abstract: Vital Area Identification (VAI) is the process for identifying areas containing nuclear materials, structures, systems or components to be protected from sabotage, which could directly or indirectly lead to unacceptable radiological consequences. Procedures of Vital area identification (VAI) based on Probabilistic Safety Assessment (PSA) which is one of the base techniques for physical protection regulation is developed. Traditionally, the physical protection of safety-critical systems has been a boundary protection of systems. In addition to the boundary protection, the protection of vital areas such as building and areas inside the facility boundary has been introduced as an active physical protection. Under this situation, the vital area identification (VAI) methodology is the base technology for the physical protection regulation.

Key words: vital area identification, probabilistic risk assessment (PRA), nuclear power plant

1. Introduction

Recently, radiation releases by sabotage from the nuclear power plant is important in terms of safety. As a matter of concern, identifying the vital areas in nuclear power plants in preparation for radiation sabotage, which became an urgent problem. In recent years, the boundary of nuclear facilities has been transferred from protection against intruders as "boundary protection" to application of vital area identification to protect the main building and compartment together in the border guard as the "active protection" concept. Considering environmental changes in terms of physical protection, identification of vital areas of nuclear power plants using the probabilistic risk assessment (PRA) methodology is the basis for physical protection regulations.

The United States has been strengthening the physical protection of nuclear power plants since the 1970s, and since September 11, 2001, research has been under way to protect nuclear facilities including nuclear power plants. In addition, the U.S. Nuclear Regulatory Commission (NRC) has enforced vital area identification in the step of designing new nuclear power plants. In recent years, as a result of requiring safety design that incorporates safety, security, and emergency preparedness for improved physical protection of new nuclear power plants, there is a growing interest in technology for identifying vital areas within the nuclear facility. As worldwide interest in identifying of vital areas to protect nuclear facilities against sabotage is growing, the Korea Atomic Energy Research Institute (KAERI) has developed vital area identification technology based on Probabilistic Risk Assessment (PRA) through its own research activities in Korea. Thus, the purpose of this paper is to introduce vital area identification technologies in nuclear power plants of ROK as a result of research and development regarding to vital area identification based on analysis of the status of the vital areas identification technology in United States and IAEA.

Corresponding author: Minho Kang, Master of Science, Researcher; research areas/interests: PRA (Probabilistic Risk Assessment) of nuclear power plant. E-mail: mhkang@kinac.re.kr.

2. Vital Area Identification

At first, before describing the procedure of vital area identification, we introduce the definition of vital area and different methodology of vital area identification between U.S. and ROK.

2.1 Definition of Vital Area

A vital area is defined in INFCIRC/225/Rev.5 (2011) as "an area inside a protected area containing equipment, systems or devices, or nuclear materials, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences". Vital Area Identification (VAI) is the process for identifying areas containing nuclear materials, structures, systems or components (SSCs) to be protected from sabotage, which could directly or indirectly lead to unacceptable radiological consequences. INFCIRC 225/Rev.5 states that "safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malevolent acts, considered in the context of a State's design basis threat, to identify nuclear material, or the minimum complement of equipment, systems, or devices to be protected against sabotage. Also measures that have been designed into the facility for safety purposes should be taken into account. When protecting against sabotage, nuclear material or equipment, systems or devices the sabotage of which, alone or in combination based on analysis, could lead to unacceptable radiological consequences, should be located in a vital area(s)".

On the another hand, in ROK's national law, article 2 of Enforcement Decree of The Act on Physical Protection and Radiological Emergency, the term "vital area" means those areas, in the protected area, fixed for the protection of nuclear facilities, etc. that may produce, directly or indirectly, an unacceptable radiological consequence due to sabotage.

The earliest criteria for identifying vital areas are the Review Guideline 17 of the US Nuclear Regulatory Commission, which basically defines all safety-related devices as vital devices. However, this document was prepared with reference to NRC Regulatory Guide 1.29 "Seismic Design Classification". Therefore, in order to keep the power plant safe from earthquake not the threat of nuclear power plant by outside invaders, and the vital equipment should be located within the vital areas. Since then, U.S. government have begun to develop more systematic methodologies to identify vital areas of nuclear power plants. The main content from these studies is the use of a logical model such as fault tree to identify events where radioactive materials may leak from a power plant, and then finally quantifies the fault tree to determine the target set consisting of the combination of locations required for the sabotage scenario to succeed or the minimal cut sets (MCS) to cause core damage and radioactive material leakage. And that the top event prevention sets (TEPS), which consist of a combination of locations that must be protected to prevent all sabotage scenarios, should be obtained.

2.2 Relation between Probabilistic Risk Assessment (PRA) and Vital Area Identification

2.2.1 Overview of PRA

The Probabilistic Risk Assessment (PRA) method is an evaluating the safety of nuclear power plants and taking the most effective measures to improve safety, considering the design, operation and maintenance of nuclear power plants. In general, risk should be assessed taking into account both the likelihood of an accident and the consequences of the accident. The Deterministic Safety Assessment (DSA) does not take into consideration the possibility of an accident, but carries out a safety assessment only in case of an accident that is considered to be highly influential, so there is limitation that severe accidents could be omitted. If the probability of occurrence of an accident can be presented stochastically, the reliability of the risk assessment can be further secured. The major difference from the deterministic safety evaluation is that it can quantitatively estimate the frequency of core damage by quantitatively calculating the probability of

occurrence of failure by estimating the failure statistical distribution of the main system using the cumulated failure data. That is, the purpose of PSA is ultimately in determining how accurate the reliability data can be used to derive quantitative risk results. The core damage frequency (CDF) and the frequency of large-scale radioactive material leakage by calculating the minimum cut sets (MCSs) that cause core damage and radioactive material leakage. On the other hand, the concept of top event prevention sets (TEPS), which can protect nuclear facilities against sabotage based on PSA results, is applied in the identification of vital areas.

The PRA method has been extensively used since the 1980s for the safety evaluation of nuclear power plants, as it has been found that US TMI-2 accidents in 1979 were already anticipated in WASH-1400, which was the first comprehensive PSA for nuclear power plants. PSA consists of three analysis as follows: an internal PSA evaluates the core damage frequency (CDF), low power and shutdown (LPSD) PRA evaluates the failure probability of the containment building, and the impact of radioactive material leaking out of the damaged containment building to surrounding residents and the environment, which is an external PRA. A full range of PRAs covering internal to an external of plants should be performed to actually assess the risk of nuclear power plants. PRA as a methodology that links physical protection and safety for the selection of vital areas of nuclear facilities will be developed based on the core damage frequency as a result of full-power internal PRA and ultimately used to identify vital areas.

The internal PSA procedure is performed according to the steps in Fig. 1. As a first step, select representative initial events after a classification of power plant failure types of nuclear power plants and develop fault trees and event trees by referring to power plant design information and operation procedures. And then, assign the statistical failure distribution to each failure events and calculate human failure error. Finally, quantify the PRA model and the core damage frequency and minimal cut sets which are combination of initiating events and failure events of mitigating system that can cause core damage are derived through calculation software.

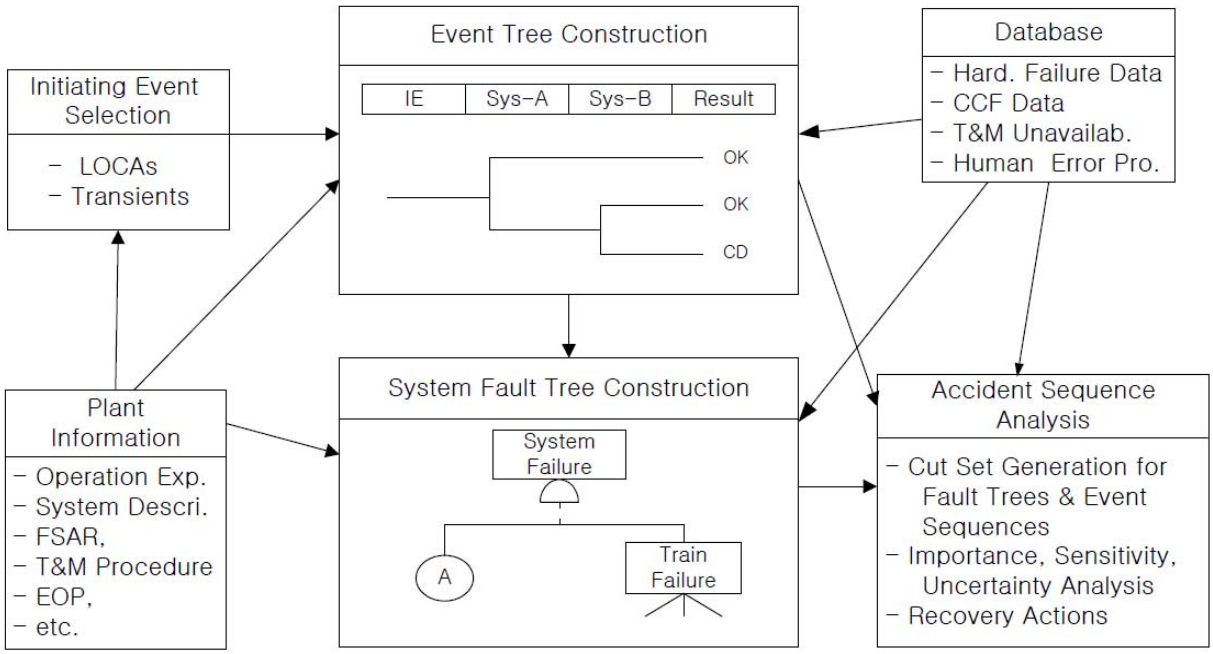

Fig. 1 Procedure of level internal PRA.

2.2.2 Application of Internal PRA Results to Vital Area Identification

As a result of the internal PRA, a combination of failure events that cause core damage can be obtained. Applying this to the vital area identification, the attacker must destroy the minimal cut sets that are minimal combinations of failure events in systems, equipment and devices for success of sabotage scenario and thereby cause the core damage and make the power plant unstable. On the contrary, for the operators, the minimal cut sets must be protected to prevent against sabotage and maintain safe status of power plants. The analysis procedure of an internal PRA for this purpose is described in detail as follows.

(a) Selection of Initiating Events: It is the starting point of the event tree analysis as a cause of the transient state of the nuclear power plant which can be developed as a severe accident. The derivation of the initial event is derived by examining the events considered in the existing accident history and existing analysis, or by performing a logical analysis such as failure mode and effect analysis (FMEA) or master logic diagram (MLD) analysis. Examples of initiating events considered by the PSA include small, medium and large loss of coolant accident (LOCA), station blackout (SBO), and general transient events.

(b) Development of Event Tree: It is an analytical method that quantifies the frequency of each accident event by making tree considered all factors such as system, equipment, and human activity that can mitigate each initial event in the time sequence. In general, one event tree is developed for each initial event, in a manner appropriate for tracking the evolution of the event.

(c) Development of Fault Tree: It is an appropriate method for tracking the cause of the accident result determined by the deductive analysis and proper for tracking the cause of the occurrence of the predefined top event such as the initiating events. In PSA, it is used mainly to identify the cause of a particular system becoming unavailable in the event tree. In general, the fault trees consist of basic events and logical gates. The basic event is the cause of the final failure which is no longer cause of the lower part, such as device failure, human error. Logic gates represent the integration conditions of these basic events, such as OR and AND gates. For example, if two basic events occur at the same time and an upper event is triggered, these two basic events are combined by AND Gate.

(d) Accident Sequence Quantification: The quantification of the accident sequence is to find minimal cut sets which can cause core damage and the frequency of cut sets based on the combination of the occurrence frequency of the initiating event, each accident sequences of event tree, and the failure events of fault tree. Boolean equations are used in this quantification process. Through this process, we can obtain minimal cut sets consist of failure events of system, devices, which leads to core damage. An example of a fault tree is shown in Fig. 2 [2]. The example system shown in Fig. 2. is a system of two trains, the A train with pump P-1A and valve V-1A is the running system, and the B train consisting of P-1B and V-1B is the waiting system. If this system fails to function, it is the case that the A train and the B train fail simultaneously (AND Gate). Thus, just below the top event of the fault tree is an AND gate that indicates that both A and B must fail at the same time. The loss of function of the A series occurs even if either pump P-1A or valve V-1A fails. Therefore, in this case, pump P-1A and valve V-1A are connected and displayed by OR gate. Fault trees are used to compute the probability of failure of the system in combination with the individual fault probability values of the underlying events.

2.3 Vital Area Identification Based On PSA

2.3.1 Vital Area Identification Using Fault Tree Analysis

The late 1970s, the U.S. Sandia National Laboratories (SNL) and the Los Alamos National Laboratory has developed a methodology to

systematically identify vital areas to take advantage of the fault tree methodology. Fault trees and boolean equations can be used to identify location combinations and ultimately select vital areas from candidate location combinations. Existing Methods for identifying vital areas have focused on deriving Boolean equations that lead to a top event for a point view of sabotage practice. However, there is a possibility that the minimal cut sets are missing, and due to this incompleteness, it is difficult to obtain the reliability of the result of selecting the key core area as well. Thus, SAND80-1095 has developed a location-based fault tree to identify location combinations at faster computing speeds.

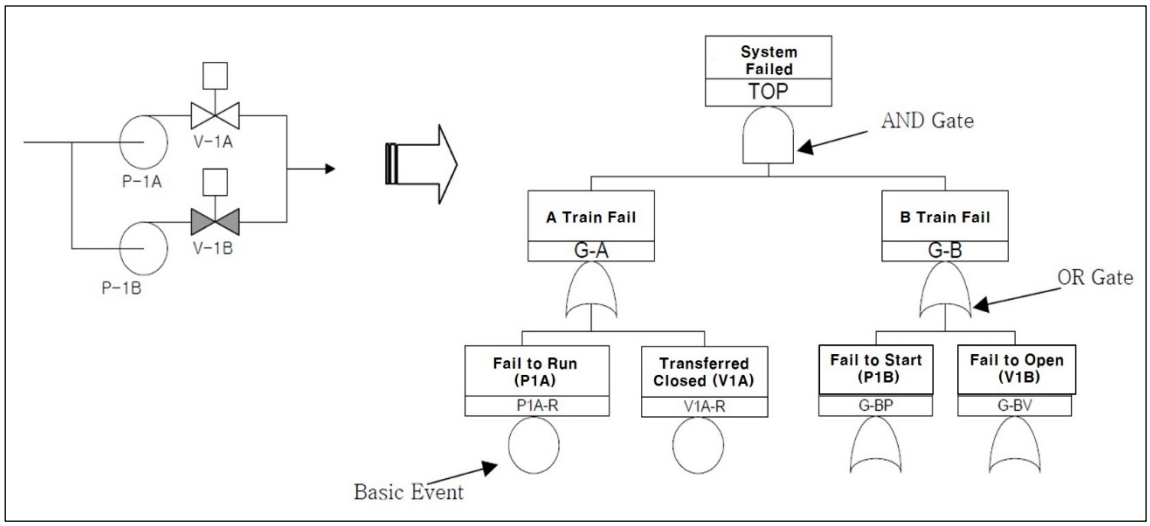

Fig. 2 Example of fault tree in PRA.

Therefore, the U.S. SNL has developed a vital area identification method that uses fault trees with a concrete barrier as a base unit, and this method can be used to create sabotage fault trees directly without using the PSA results. So, this method has limitations in that it does not simulate the risk of an entire plant as accurately as PSA. In other words, the procedure of deriving the target sets and prevention sets based on the sabotage fault tree of SNL and finally selecting the vital area is the same as the domestic study, but since the SNL does not use the PSA results, it is necessary to analyze by the expert and thus this is a high cost vital area identification method. It consists of three different segments, each of which is linked and each segment is added to the right of the previous gate. The definition of each segment is as follows.

(a) Major Fault Tree Segment (MFTS): It is composed of the lower event (Primary Event) and the transfer gate (Transfer-In Gate) as the top gate of the fault tree.

(b) Intermediate Fault Tree Segment (IFTS): The primary event is connected to the top gate at the end, and at least one transfer-in gate is included.

(c) Terminal Fault Tree Segment (TFTS): It is located at the bottom of the fault tree and is composed only of Primary Event

2.3.2 Process Overview of Vital Area Identification based on PSA

As a first step, we need to classify the type of vital areas. When the PSA method is used to identify vital areas, the vital areas can be classified into the following three types.

(a) Type I: Areas where there is a system or building that causes certain initial events

(b) Type II: Areas where mitigation systems are located

(c) Type III: A system that triggers a specific initial event and an area where the mitigation system

For example, if only the Type I area is destroyed, safety of the nuclear power plant can be ensured even if

the initial event occurs, since the accident mitigation system is sound. In addition, even if a Type II area is destroyed and a certain accident mitigation system becomes unavailable, safety of the nuclear power plant will not be seriously threatened unless an initial event causing the nuclear power plant transient occurs. However, if the Type III area is destroyed or the Type 1 and Type 2 areas are damaged at the same time, the safety of the nuclear power plant can be seriously affected. Since the case where Type 1 and Type 2 areas are damaged at the same time is possible through various combinations of vital area, it is possible to grasp the entire combination of vital areas by using PSA results. The VAI process [3] is depicted in Fig. 3. The steps of this process are as follows. The definition of key terms on the below procedure is as follows [3].

(a) Initiating event of malicious origin (IEMO): A maliciously initiated Initiating Event. A malicious act that upsets the operation in such a way that, if mitigation were unsuccessful, would lead to unacceptable radiological consequences.

(b) Initiating Event (IEs): An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

(c) Unacceptable radiological consequences (URCs): A level of radiological consequences, established by the State, above which the implementation of physical protection measures is warranted.

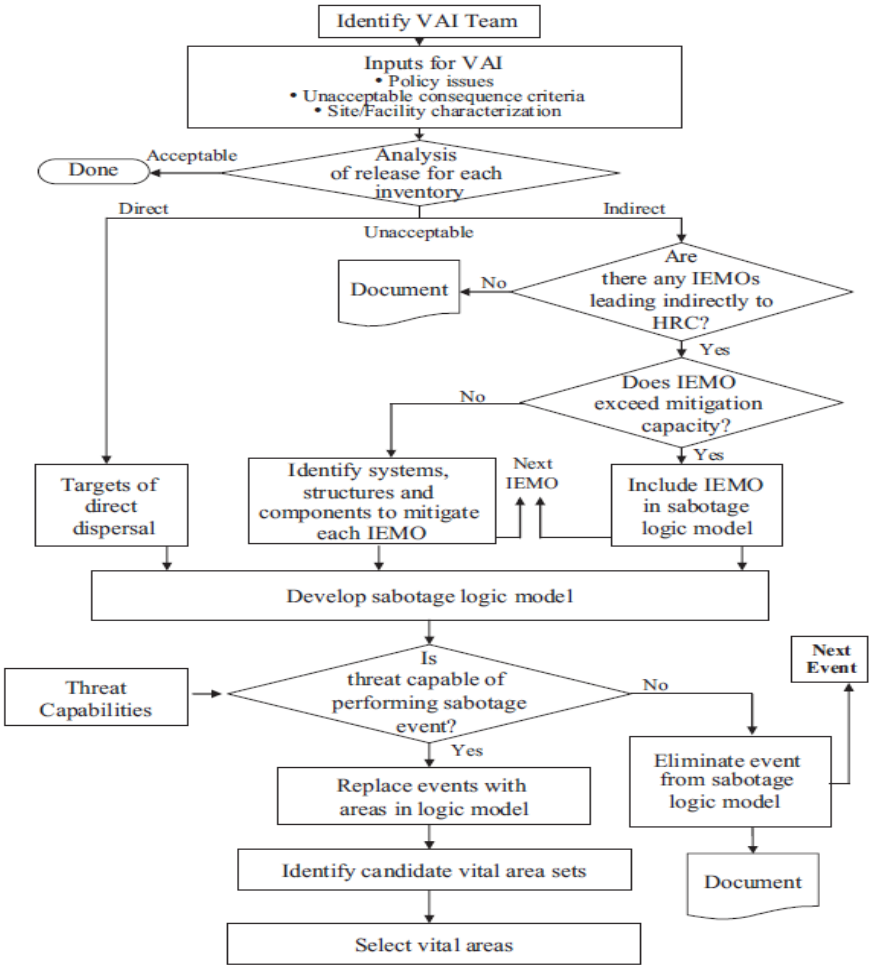

Fig. 3 Vital rea identification process.

The key point here is to use the internal PSA results to identify the combination of fault events that lead to core damage and replace it to an area logic model with converting from each failure event to an area where

initiating event or each failure event can be occurred. This allowed us to find combinations of areas that do not lead to core damage, which are prevention sets. The prevention sets mean that if the adversary is prevented from gaining access to all the areas in one prevention set, he will not be able to complete any of the sabotage attacks.

In the VAI process, the concept of "room" was used as the basic unit area. Here, a room refers to a separate area separated by a firewall in a general arrangement diagram. In other words, the attacker targets each room, and the area damaged by the attack is limited to each room being attacked. It can also be analyzed that multiple rooms are destroyed by simultaneous attacks according to predefined design basis threat (DBT). In each room, the equipment, system, power cable, etc. are located. Therefore, when each room is attacked, it is necessary to identify the equipment, system, power cable, etc. that are failed. At this time, the breakage of the power cable does not only cause the failure of the equipment in the area but also causes the loss of function of the equipment or the system which is supplied with the power source through the power cable even though it is not in the area. Therefore, all relevant equipment and systems that are failed due to breakdown of equipment, systems, power cables, etc. in such attacked areas should also be considered. In order to find accurate site information, the location and relation of the equipment and system identified through the above process must be confirmed through the walk down.

A separate database should be constructed by linking the basic events and the room numbers, which are modelled as causing the failure of the equipment and the system in the PSA fault tree and the devices and systems identified as being unavailable due to the destruction of each room. To do this, we use fire/flood PSA results based on location information collected through walk-downs. It can be explained with the example which can be seen in Fig. 2. To illustrate this process, which can be seen on the below, Fig. 4.

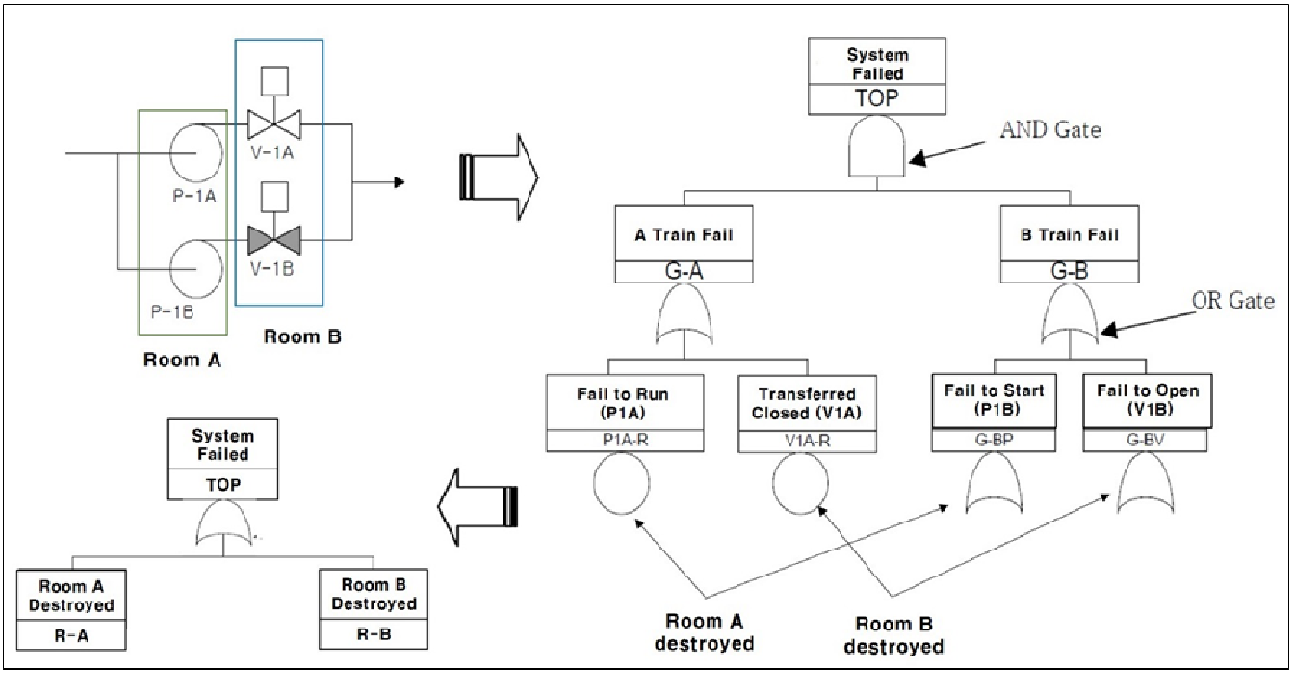

Fig. 4 Conversion from fault tree to sabotage area logic model.

It is assumed that the two pumps P-1A and P-1B are located in room A and that both valves V-1A and V-1B are located in room B. In this case, if one of the rooms in either room A or room B is destroyed by attack, it is assumed that this system becomes unusable and induces a specific initiating event α. the destruction of

the room A and the destruction of the compartment B, like the fault trees at the bottom of Fig. 4, consist of fault trees connected by OR logic gates. In other words, this area fault tree means that a specific initial event α occurs even if only one of the two cases of the destruction of room A and the destruction of the room B occurs. As described above, fire/flood PSA results are used to link each room with basic event in existing fault tree.

As a result, the combinations of rooms causing exceed URC (Unacceptable Radiological Consequence) is a minimal set of cuts (MCSs) in the sabotage area logic model, which can be used as a potential attack target for intruders in the development of sabotage scenarios for validation of physical protection systems. Among the candidates for the vital areas, the operators of nuclear power plants can select the candidate group that satisfies the international standard [4] and finally designate it as the vital areas. Judgment criteria can be considered as an example of the following criteria. In general, additional engineering judgement or trade-off analysis can be performed because one of the vital areas candidates is unlikely to achieve a significantly higher score. (a) Impact of plant safety, plant operation and emergency response (b) Difficulty in protecting vital areas (c) Efficiency of protective measures (d) Cost to protect vital areas.

Another important consideration when developing a sabotage logic model is to assess the threat capabilities based on Design Basis Threat (DBT). Events that are unreliable within threat capacity of the design standard should be excluded from the model development and basic events exceeding criteria of DBT should also be excluded from the sabotage logic model. It should also be noted that basic events that cannot be protected by physical protection systems should be identified. And also, it need to be assumed that threats that could harm the facility without access to nuclear facilities may also occur. For example, in the accident of station blackout, it can be sufficiently generated by interrupting or cutting the power cable from outside the power plant for the purpose of intrusion.

4. Conclusion and Future Work

4.1 Conclusion

The VAI is a very important step in the protection process for sabotage. VAI is the procedure for establishing areas within a nuclear facility that must be protected to reduce or prevent against sabotage. Therefore, there is a growing need to identify vital areas based on systematic methodologies. As a part of it, in KOREA, VAI methodology based on Probabilistic Safety Assessment (PSA) was developed recently. In this paper, we propose a method and result of determining the vital areas to be protected in order to prevent the occurrence of events such as leakage of radioactive material from nuclear facilities due to external intrusion. Based on the results of the internal PSA, it is assumed that all equipment, cables and piping installed in the room are destroyed at the same time, and thus all the equipment in the room cannot perform their functions. Considering the assumption, the objective is to find target sets, combination of rooms which can cause core damage of plants due to sabotage. Identifying target sets is needed to improve vulnerability of plants in terms of physical protection. We can select the vital area set from the candidate vital area sets identified as prevention sets that will be protected to prevent sabotage leading to HRCs.

4.2 Future Work

VAI should be performed repeatedly when threat conditions are changed, or when considering or implementing facility design changes. If the design of plant is changed, the PSA results need to be developed differently from the existing ones by changing the functions of the accident mitigation system and changing the positions of the cables and the cooling water pipes. Therefore, the identification of vital areas should not be done at one time but should be continually revised as additional change needs arise.

The optimal time to apply the VAI process is the design phase of the new facility. Once the vital area analysis and identification is completed at the design stage, it is possible to avoid unnecessary re-establishment of the vital areas and to build the optimal physical protection systems from the construction stage. If such vital areas are set up from the design stage, the PSA-based vital area regulation will be undertaken based on the understanding of the safety system of plant, and thus continuing to complement the protection measures for the vital areas.

References

[1] D. W. Stack and K. A. Francis, Vital area analysis using sets, NUREG/CR-1487, SAND80-1095, 1980.

[2] J. E. Yang, C. K. Park, S. Y. Choi, J. H. Kim and H. G. Kang, PSA based vital area identification of nuclear installations, Korean Nuclear Society, 2002, pp. 199-199.

[3] International Atomic Energy Agency, Identification of vital areas at nuclear facilities, IAEA Nuclear Security Series No. 16, 2012.

[4] International Atomic Energy Agency, Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Rev.5), IAEA, Vienna, 2011.

[5] D. D. Boozer et al., Safeguards System Effectiveness Modeling, SAND76-0428, Albuquerque, NM, 1976.

[6] G. B. Varnado and N. R. Ortiz, Fault Tree Analysis for Vital Area Identification, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, USNRC, Washington DC, 1979.

[7] U.S. Nuclear Regulatory Commission, Vital Equipment Area Guideline Study: Vital Area Committee Report, NUREG-1178, 1988.

[8] G. Bruce Varnado and D. W. Whitehead, Vital area identification for U.S. nuclear regulatory commission nuclear power reactor licensees and new reactor applicants, SAND2008-5644, Sandia National Laboratories, 2008.

[9] Sandia National Laboratories, A Systematic method for identifying vital areas at complex nuclear facilities, SAND2004-2866, 2005.

[10] Regulatory Guide 5.65, Vital area access controls, protection of physical security equipment, and lock controls, U.S. NRC, 1986.

[11] J. E. Yang, C. K. Park, S. Y. Choi, J. H. Kim and H. G. Kang, PSA Based Vital Area Identification of Nuclear Installations, Korean Nuclear Society, 2002, pp. 199-199.

[12] Y. H. Lee, W. S. Jung and J. H. Lee, Vital area identification analysis of a hypothetical nuclear facility using VIPEX, *Journal of the Korean Society of Safety* 26 (2011) (4) 87-95.