THE APPLICATION OF PSA TECHNIQUES TO THE VITAL AREA IDENTIFICATION OF NUCLEAR POWER PLANTS

JAEJOO HA, WOO SIK JUNG* and CHANG-KUE PARK
Korea Atomic Energy Research Institute
P.O.Box 105, Yuseong, Daejeon, Korea
*Corresponding author. E-mail : jjha@kaeri.re.kr, woosjung@kaeri.re.kr, ckpark3@kaeri.re.kr

Received April 28, 2005

This paper presents a vital area identification (VAI) method based on the current fault tree analysis (FTA) and probabilistic safety assessment (PSA) techniques for the physical protection of nuclear power plants. A structured framework of a top event prevention set analysis (TEPA) application to the VAI of nuclear power plants is also delineated. One of the important processes for physical protection in a nuclear power plant is VAI that is a process for identifying areas containing nuclear materials, structures, systems or components (SSCs) to be protected from sabotage, which could directly or indirectly lead to core damage and unacceptable radiological consequences.

A software VIP (Vital area Identification Package based on the PSA method) is being developed by KAERI for the VAI of nuclear power plants. Furthermore, the KAERI fault tree solver FTREX (Fault Tree Reliability Evaluation eXpert) is specialized for the VIP to generate the candidates of the vital areas. FTREX can generate numerous MCSs for a huge fault tree with the lowest truncation limit and all possible prevention sets.

KEYWORDS : Design Basis Threat, Vital Area Identification, Sabotage-induced Risk Assessment, Location Fault Tree, Top Event Prevention Set Analysis

1. INTRODUCTION

1.1 Design Basis Threat

In 1998, the International Atomic Energy Agency (IAEA) published INFCIRC/225/Rev.4[1], which includes principal international guidelines for the physical protection of nuclear material and nuclear installations. IAEA has initiated a series of nuclear security documents to provide a coherent and integral framework for the documents related to nuclear security. These documents include guidelines and recommendations for the development and maintenance of a design basis threat (DBT), the vital area identification (VAI), export-import of radioactive sources, and the security of the transport of radioactive materials.

The major difference between general industrial sabotage and nuclear sabotage is that the latter involves radioactivity. A sabotage is defined in Ref. 1 (Paragraph 2.12) as "any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public and the environment by an exposure to radiation or the release of radioactive substances".

A DBT is defined in Ref. 1 (Paragraph 2.4) as "the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated."

After September 11, 2001, the date when terrorists attacked the World Trade Center in New York City, the perception of the physical protection of nuclear facilities changed, as the perception of nuclear safety was altered following the TMI-2 accident. After the TMI accident, the concept of risk became popular and the design basis accident (DBA) became a part of the whole spectrum of possible accidents. In the conventional probabilistic safety assessments (PSAs) of nuclear power plants, various risks are analyzed resulting from internal events and external events such as earthquakes, fires, floods, tornadoes, and wind.

Sabotage–induced risk is defined in a loose sense as the risk from events, incurred by terrorist activities against nuclear facilities, which result in a core damage and an eventual environmental radioactive material release [2,3]. Conceptually, a sabotage–induced risk assessment (SRA) [2,3] does not differ greatly from the typical PSAs. In a typical PSA, the DBA is a part of the whole spectrum of initiating events. Similar to the DBA in the PSA, the DBT may be considered as an initiating event in the SRA. For the SRA, the definition of the DBT could be changed.

The DBT could be defined as a possible terrorist attack that can cause accident sequences that might result in core damage and a radioactive material release to the environment.

Thus, the definition of the DBT could be expanded in order to cover a whole spectrum of possible terror activities such as the severe accident scenarios in PSAs[2]. It is important to note that the present definition of the DBT in Ref. 1 focuses on the unauthorized removal of nuclear material or a sabotage.

1.2 Vital Area Identification

A vital area is defined in Ref. 1 (Paragraph 2.17) 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."

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. 4 (Paragraph 7.1.5 of Ref. 1) 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)".

Vital area analysis study and its application for nuclear facilities have been performed since the late 1970s. The original concept of sabotage-induced risk was introduced by WASH-1400 in 1975[4]. The Sandia National Laboratories (SNL) and the Los Alamos National Laboratory (LANL) in the USA have been the leading institutes in the area of VAI studies using a fault tree technique [5-11]. The SNL proposed and initiated the use of fault trees for VAI [5-7]. The LANL performed various vital area analyses of nuclear power plants in order to provide the US Nuclear Regulatory Commission (NRC) with technical support [8-11].

The minimal cut sets (MCSs) and minimal path sets (MPSs), the important outputs of the fault tree analysis (FTA), were used for the VAI of a nuclear power plant [12]. Furthermore, the concept of applying a top event prevention set analysis (TEPA)[13-16] to VAI has been discussed at several small workshops. However, formal documents comprising a detailed TEPA application to VAI do not exist. TEPA generates many prevention sets as candidates for the set of vital areas that should be protected against sabotage. Only one prevention set is selected and the rooms in the selected prevention set are the vital areas to be protected.

For the VAI of nuclear power plants, a software VIP (Vital area Identification Package based on the PSA method) [3] is being developed. The VIP is based on the current PSA techniques. The VIP employs the PSA techniques and results. Furthermore, the fault tree solver FTREX (Fault Tree Reliability Evaluation eXpert)[17,18] is specialized for the VIP to generate prevention sets.

The PSA-based VAI is performed by evaluating the location fault tree (LFT)[2,3,12]. The LFT consists of gates and room failures. Three outputs, MCSs, MPSs, and prevention sets, could be generated through the VAI process. The VAI of an actual nuclear power plant was performed based on the MCSs and MPSs of the LFT [2, 12].

1.3 Objectives of the Paper

As noted in Section in 1.2, there are no formal documents presenting a TEPA application to VAI. Furthermore, it is uncertain whether application of TEPA to VAI for an actual nuclear power plant has thus far been performed. This paper presents a structured framework of a TEPA application to VAI for the physical protection of nuclear power plants.

The current paper describes the FTA and TEPA for the VAI (Section 2), PSA-based VAI (Section 3), and the software VIP (Section 4). The LFT is developed based on the PSA results. The PSA method, including internal as well as external events, is known as the most complete and consistent method for identifying various accident sequences in nuclear power plants through which radioactivity might be released to the environment. Thus, it is logical and natural to use the PSA techniques and results for the VAI of nuclear power plants.

2. FTA AND TEPA

2.1 FTA

FTA is one of the most commonly used methods for the safety analysis of industrial systems, especially for the PSA of nuclear power plants. The fault tree consists of many gates and basic events. The fault tree for the top event is transformed into logically equivalent forms of MCSs. An MCS has the smallest combination of basic events that could result in the occurrence of the top event [19-21]. Hence, the MCSs relate the top event directly to the basic events. In a physical protection analysis, any of the MCSs has the smallest group of room failures whose successful attack induces a top event such as core damage. Thus, any material that has a list of MCSs should be confidentially kept from the terrorists.

The fault tree can be transformed into its equivalent success tree, that is, a dual fault tree, by negation of the fault tree. The dual fault tree is obtained by taking the Boolean complement of the original fault tree. Moreover, the success tree identifies the MPSs that need to be prevented

in order to assure that the top event will not occur. Negation of the fault tree changes all AND to OR gates, and all OR to AND gates. From the viewpoint of physical protection, a MPS has the smallest group of rooms whose successful protection guarantees no top event occurrence. Thus, each MPS could be a candidate set of the vital areas.

2.2 TEPA

TEPA [13-16] is a deterministic technique for finding the prevention sets from the top event MCSs. TEPA generates prevention sets, which are combinations of basic events that can prevent the occurrence of a top event such as core damage. Similar to the MPSs, a prevention set is a collection of basic events which, if they do not occur, precludes the occurrence of the top event. The user can specify the level of prevention. The level of prevention denotes the number of basic events from each MCS to be selected. A prevention set of level L contains at least L basic events from each MCS.

Some practical analyses have been performed using TEPA[13-16]. The fundamental concept underlying the methodology was first published in 1978 in the form of a security related sensor nullification study [5]. As an alternative technique of the traditional risk ranking method based on the importance measures, TEPA has been applied to the real problem of choosing a set of important pumps, valves, or circuit breakers [13-16].

VAI is another application field of TEPA. For VAI, a core damage fault tree that consists of gates and room failures is solved and many prevention sets are generated. If the prevention sets can be ranked in some manner, the most competitive prevention set can be selected and its rooms are the vital areas. One can choose a prevention set that satisfies some criteria such as being easier or less costly to protect the rooms in the selected prevention set.

TEPA utilizes a kind of success path. This approach has desirable defense-in-depth characteristics. Each prevention set has a minimal combination of rooms to be protected in order to avoid a top event such as core damage. The prevention sets of level L are created as follows:

1. Calculate N MCSs by solving the fault tree;
2. Identify all the combinations of the complemented L events from one MCS and connect them with OR gates. This results in a Boolean equation from one MCS. Thus, N Boolean equations are created from N MCSs;
3. Connect the N Boolean equations with AND gates; and
4. Expand and subsume the Boolean equation that is obtained at Step 3.

Let us consider the following top event T for the prevention sets of level L

$$T = AB + ACDE. \tag{1}$$

The prevention sets of level 1 are obtained as follows:

$$\begin{aligned} S_1 &= (\bar{A}+\bar{B})\,(\bar{A}+\bar{C}+\bar{D}+\bar{E}) \\ &= \bar{A}+\bar{B}\bar{C}+\bar{B}\bar{D}+\bar{B}\bar{E} \\ &= \bar{T} \end{aligned} \tag{2}$$

The prevention sets at level 2 are

$$\begin{aligned} S_2 &= (\bar{A}\bar{B})\,(\bar{A}\bar{C}+\bar{A}\bar{D}+\bar{A}\bar{E}+\bar{C}\bar{D}+\bar{C}\bar{E}+\bar{D}\bar{E}) \\ &= \bar{A}\bar{B}\bar{C}+\bar{A}\bar{B}\bar{D}+\bar{A}\bar{B}\bar{E} \end{aligned} \tag{3}$$

Here, the level L could be interpreted as the degree of the defense-in-depth.

The prevention sets at level 1 S_1 are the same as the MPSs. That is, the MPS is a conceptual subset of the prevention set. As explained in Section 2.1, the MPSs could be more efficiently calculated by solving the dual fault tree. The dual fault tree is obtained by taking the Boolean complement of the original fault tree.

3. PSA-BASED VITAL AREA IDENTIFICATION

Since a prevention set has a minimal combination of rooms to be protected in order to avoid a core damage, the prevention sets are candidates for the vital areas. If all the rooms in any one of the prevention sets are protected, the absence of core damage is guaranteed. Thus, a prevention set whose rooms could be the most efficiently and cost-

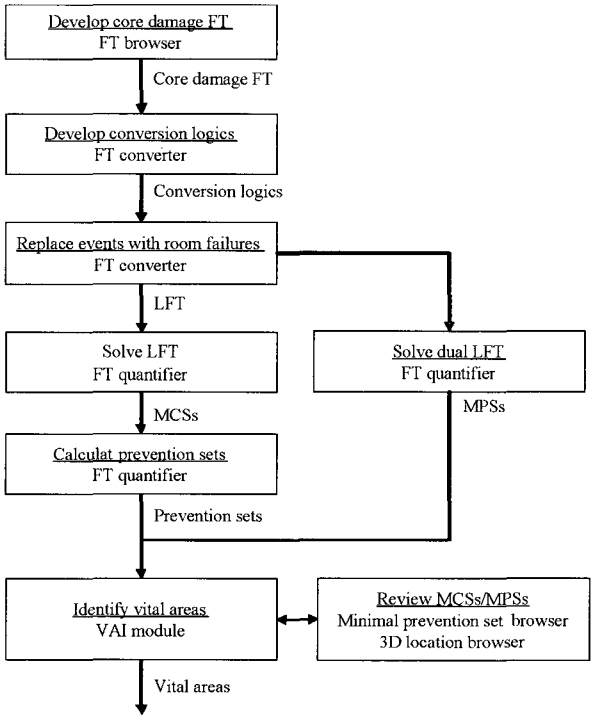

Fig. 1. Overall VAI Procedure and the Main Modules of the VIP

effectively protected is selected and the rooms of the selected prevention set are the vital areas to be protected against sabotage. As shown in Fig. 1, the VAI is performed as follows:

1. Develop a core damage fault tree by combining all the accident sequences in the PSA results.
2. Develop conversion logics from basic events to room failures.
3. Build a LFT by combining the core damage fault tree (FT) and the conversion logics, where the basic events in the core damage fault tree are replaced with room failures.
4. Identify the candidate sets of the vital areas, the prevention sets, by solving the LFT.
5. Identify the vital areas by selecting the most competitive prevention set through expert judgments on the prevention sets.

3.1 Development of a Core Damage Fault Tree

In order to construct the core damage LFT, the first step is to integrate the event trees and fault trees that are generated by the conventional PSA. An event tree includes an initiating event and fault trees of the systems and the functions to mitigate the initiating event.

"Accident sequence fault trees" are constructed by combining the initiator (or its fault tree) and the fault trees for the mitigating systems with AND gates. Then, "a core damage fault tree" is constructed by combining all the accident sequence fault trees of the various event trees with OR gates.

If necessary, new fault trees are developed to reflect the room failures. A typical example is a fault tree for an initiating event. It consists of the basic events that lead to the occurrence of the initiating event.

3.2 Development of Conversion Logics

The destruction of a room (room failure or location failure) by an act of sabotage indicates the destruction of the SSCs contained in the room. The room failures represent the sabotage-induced damage to the respective locations.

In order to reflect these room failures to the core damage fault tree, conversion logics that connect the basic events or the initiating events to the room failures should be developed through the failure mode and an effect analysis (FMEA) of the room failures. The conversion logics have either a one-to-one mapping relation or a logical relation expressed as Boolean equations between the basic events and the room failures (for example, BASIC_EVENT_1 = ROOM_1 + ROOM_2).

If a room has piping for a mitigating system, its failure causes component failures of the mitigating system. Similarly, the destruction of a room that has an air conditioning system, electrical power supply cables, or signal cables/lines could cause component failures of the mitigating systems. In these cases, the room failures should be located in the core damage LFT by developing appropriate conversion logics from the basic events of the components to the room failures.

3.3 Replacement of the Basic Events with Room Failures

In order to identify the vital areas, the core damage fault tree developed above should be converted into the core damage LFT. In this phase, all the basic events of the core damage fault tree should be replaced with the room failures by using the conversion logics developed in the previous step. This conversion could be performed manually or automatically by PSA software [17, 18, 22].

3.4 Selection of Vital Areas

We have two alternatives, MPSs and prevention sets, as candidate sets of the vital areas. Please note that the use of the selected MPS as a candidate set of the vital areas has no concept of defense-in-depth. The prevention sets are more desirable candidates of the vital areas, since they provide defense-in-depth.

As mentioned in Section 2.1, the MPSs could be more efficiently calculated by solving the dual LFT. The dual LFT is obtained by taking the Boolean complement of the core damage LFT.

The successful protection of all the rooms in any prevention set guarantees that core damage does not occur and thus radioactive material release similarly does not occur. Thus, each prevention set is a candidate for the set of vital areas that contains the SSCs to be protected against sabotage. Once a complete set of the prevention sets is identified, each set should be reexamined. Since the actual physical protection of each room may be impossible in practical terms, the final selection of the vital areas is undertaken in close conjunction with the physical protection system design. For example, the prevention sets with rooms that cannot be protected are excluded. By subjective expert judgments to consider the attributes of the rooms in a prevention set, one desirable prevention set is selected and its rooms become the vital areas. The number of rooms and the defensibility of the rooms in a prevention set are typical attributes of the rooms to be considered in the expert judgments. That is, one straightforward way is to select a set of vital areas that has a minimal combination of rooms.

The prioritization of the prevention sets could be implemented by ranking some attributes by experts from related areas such as security, plant operation, regulation, and safety. The physical protection of the vital areas should be feasible and practicable. It must be feasible to employ the existing structures or new constructions to establish a physical barrier around each defined area. It must also be feasible to control the access to each area by minimizing the number of entries and exits and by installing alarms to appropriately secure all points of

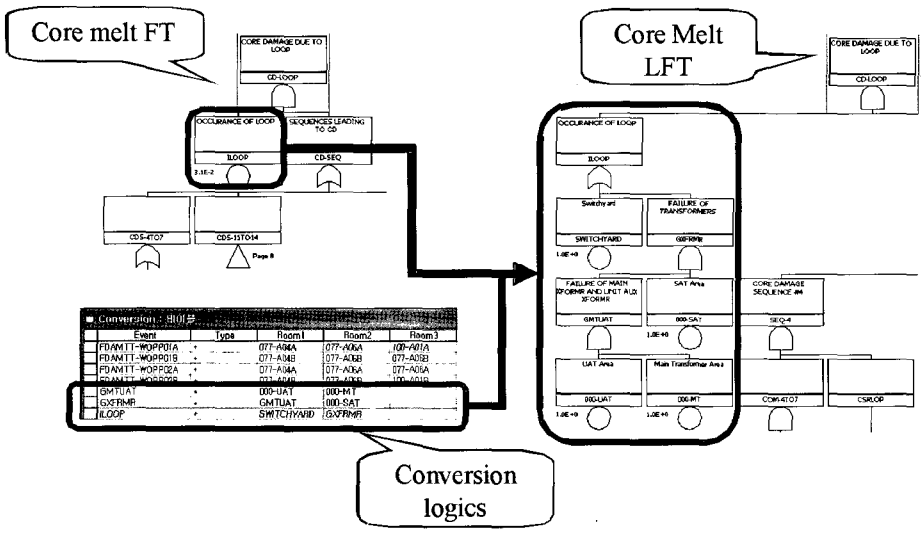

Fig. 2. Replacement of a Basic Event with Location Room Failures

access to the area. Since the physical protection of the vital areas should be feasible, the VAI team should consult with the organization responsible for the physical protection system.

4. VITAL AREA IDENTIFICATION SOFTWARE VIP

The whole VAI procedure and the VIP main modules are depicted in Fig. 1. The VIP has 6 main modules, an FT browser, a prevention set browser, a 3-dimensional location browser, an FT converter, an FT quantifier, and a VAI module. Intended function, input, and output of the main modules are also shown in Fig. 1.

The main functions of the FT browser in Fig. 1 are to edit the core damage fault tree and the conversion logics, convert the core damage fault tree to the core damage LFT according to the conversion logics, and provide a user interface to quantify the core damage LFT.

The core damage fault tree is converted into the core damage LFT by the FT converter. As illustrated in Fig. 2, all the basic events of the core damage fault tree are replaced with room failures in accordance with the conversion logics by the FT converter.

This conversion could be performed manually or automatically by PSA software. Most fault tree quantifiers [17,18,22] could perform the conversion operation by replacing the basic events in the core damage fault tree with conversion logics. During the automatic conversion, duplicated room failures under the same gate are internally reduced into one room failure in order to simplify the LFT.

The FTREX [17,18] is employed as a default fault tree solver to convert the core damage fault tree to the LFT and generate MCSs, MPSs, and the prevention sets. FTREX is a recently developed fast fault tree quantifier, and is based on a BDD (Binary Decision Diagram) algorithm. The fault tree solver FTREX has displayed desirable performance [17,18]. FTREX optionally solves fault trees by the conventional BDD algorithm or a coherent BDD algorithm. FTREX could convert the fault trees into input files for Bayesian network algorithms. Furthermore, FTREX has special features such as truncated probability estimation [23], logical loop breaking [24], and rule-based post processing capabilities.

5. CONCLUSIONS

This paper presents the structured framework of a TEPA application to VAI for the physical protection of nuclear power plants. It is important to note that there might be a huge number of prevention sets when performing a TEPA. Early applications of TEPA to select a set of important pumps, valves, or circuit breakers [13-16] were severely constrained by the computational capabilities of the software and hardware that existed at that time. However, FTREX can generate numerous MCSs, MPSs, and all the possible prevention sets with the lowest truncation limit.

A set of pre-planned strategies could be developed to protect the rooms in the MPSs or prevention sets. On the other hand, the MCSs are used to test pre-planned strategies and to train security staff. Since any of the MCSs has the smallest group of room failures whose successful attack induces a top event such as core damage, any material that has the list of MCSs should be confidentially secured from terrorists.

Before selecting the most competitive prevention set for the vital areas, a sensitivity study should be performed

to demonstrate the completeness of the prevention sets. All the prevention sets are tested to ensure that they prevent every MCS for the chosen level of prevention. Furthermore, each prevention set should be propagated to the LFT since there might be truncated MCSs. When the LFT is solved after setting the room failures in any of the prevention sets to TRUE, there should be no MCSs regardless of the truncation limit. When the huge fault tree is solved, there might be truncated MCSs. The truncated MCSs then could not be taken into account in the prevention sets. Therefore, core damage could occur due to the occurrence of one of the truncated MCSs even though one of the prevention sets is protected. This is an unresolved issue of the TEPA application to VAI.

The electric power utilities should provide physical protection to the identified vital areas. For the efficient identification of vital areas, a software VIP is being developed based on PSA technology, particularly with respect to the TEPA. The VIP is considered to be very useful for the selection of target sets of a physical protection. The method in the present paper is consistent and the most complete for identifying vital areas, since it is based on well-proven PSA technology.

REFERENCES

[1] IAEA, "Physical Protection of Nuclear Material and Nuclear Facilities," INFCIRC/225/Rev.4 (1998).

[2] C.K. Park, W.S. Jung, J.E. Yang, H.G. Kang, "A PSA-based Vital Area Identification Methodology Development," *Reliability Engineering & System Safety*, **82**, 2, pp. 133-140, (2003).

[3] C.K. Park, W.S. Jung, J.E. Yang, H.G. Kang, "Development of a PSA-based Vital Area Identification Methodology for the Physical Security of Nuclear Power Plants," *Proceedings of the 7th International Conference on Probabilistic Safety Assessment and Management*, Berlin, Germany, Jun. 12-19 (2004).

[4] N. Rasmussen, et al., "Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Plants," WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission (1975).

[5] D.D. Boozer and R.B. Worrell, "A Method for Determining the Susceptibility of a Facility to Sensor System Nullification by Insiders." SAND77-1916C, Feb. (1978).

[6] G.B. Varnado and N.R. Ortiz, "Fault Tree Analysis for Vital Area Identification," NUREG/CR-0809, SAND79-0946, Sandia Labs., USA (1979).

[7] D.W. Stack and K.A. Francis, "Vital Area Analysis Using SETS," NUREG/CR-1487, SNAND80-1095, Sandia Labs., USA (1980).

[8] J.M. Boudreau and R.A. Haarman, "Reactor Sabotage Vulnerability and Vital-equipment Identification," LA-UR-82-2831, Los Alamos National Lab., USA (1982).

[9] T.F. Bott and W.S. Thomas, "Reactor Vital Equipment Determination Techniques," LA-UR-83-3026, Los Alamos National Lab., USA (1983).

[10] D.F. Cameron, "Vital Areas at Nuclear Power Plants," LA-UR-85-558, Los Alamos National Lab., USA (1985).

[11] P.Y. Pan and T.F. Bott, "Vital Equipment Determination Techniques Research Study," NUREG/CP-0058-Vol.6, USA (1985).

[12] F. Rahn, "An Approach to Risk-Informed Physical Security, Electric Power Research Institute," EPRI TR-113787, Oct. (1999).

[13] R.B. Worrell and D.P. Blanchard, "Top event Prevention Analysis: A Deterministic Use of PRA," *International Conference on Probabilistic Safety Assessment Methodology and Application*, Seoul, Korea, Nov. 26-30 (1995).

[14] D.P. Blanchard and B.A. Brogan, "Identification of Risk-significant Circuit Breakers Using Top Event Prevention Analysis," *International Topical Meeting on Probabilistic Safety Assessment*, Park City, Utah, Sep. 29 – Oct. 3 (1996).

[15] D.P. Blanchard and R.B. Worrell, "Top Event Prevention Analysis: A Method for Identifying Combinations of Events Important to Safety," *International Topical Meeting on Probabilistic Safety Assessment.* Detroit, Michigan, Oct. 6-9 (2002).

[16] R.A. White and D.P. Blanchard, "Development of A Risk-informed IST Program at Palisades Using Top Event Prevention," *Proceedings of ICONE10 10th International Conference on Nuclear Engineering*, Arlington, VA, Apr. 14-18 (2002).

[17] W.S. Jung, S.H. Han, and J.J. Ha, "A Fast BDD Algorithm for Large Coherent Fault Trees Analysis," *Reliability Engineering and System Safety*, **83**, pp. 369.374, (2004).

[18] W.S. Jung, S.H. Han, and J.J. Ha, "Development of an Efficient BDD Algorithm to Solve Large Fault Trees," *Proceedings of the 7th International Conference on Probabilistic Safety Assessment and Management*, Berlin, Germany, Jun. 12-19 (2004).

[19] W.E. Vesely, F.F. Goldberg, N.H. Roberts, and D.F. Haasl, *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC (1981).

[20] W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, *Fault Tree Handbook with Aerospace Applications*, National Aeronautics and Space Administration (2002).

[21] R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart and Winston, Inc., (1975).

[22] S.H. Han, "PC-Workstation Based Level 1 PRA Code Package-KIRAP," *Reliability Engineering and System Safety*, **30**, pp.313-322 (1990).

[23] W.S. Jung, J.E. Yang, and J.J. Ha, "Development of measures to estimate truncation error in fault tree analysis," *Reliability Engineering & System Safety*, in Press (2005).

[24] W.S. Jung, S.H. Han, and J.J. Ha, "Development of an analytical method to break logical loops at the system level," *Reliability Engineering & System Safety*, in Press (2005).