International Journal of Nuclear Security

Volume 2
Number 2 *ASTECHNOVA Conference*

Article 5

12-24-2016

Modified Fault Tree Method for Vulnerability Analysis of Nuclear Medicine Facility Security System Case study: Radiotherapy Facility, Sardjito General Hospital

Haryono Budi Santosa
Department of Nuclear Engineering and Engineering Physics, Universitas Gadjah Mada, Yogyakarta, Indonesia

International Journal of Nuclear Security, Vol. 2, No. 2, 2016

Modified Fault Tree Method for Vulnerability Analysis of Nuclear Medicine Facility Security System Case study: Radiotherapy Facility, Sardjito General Hospital

Haryono Budi Santosa; Susetyo Hario Putero; Achmad Chilmi Nur, Samsiatun Mudzkiyah, and Sheila Amalia
Department of Nuclear Engineering and Engineering Physics, Universitas Gadjah Mada, Yogyakarta, Indonesia Email: hbs@ugm.ac.id; susetyo@ugm.ac.id

Abstract
Assessing the vulnerability of physical protection systems (PPS) in nuclear medicine facilities is needed to prevent a security incident that could lead to the malicious use of nuclear material. Theft and sabotage of nuclear materials is becoming globally recognized. The current methods of assessing vulnerability tend to be oriented toward complex nuclear security; consequently, it is excessive to use such methods in simple facilities (i.e., radiotherapy facilities in hospitals).

The fault tree analysis is a method to assess vulnerability for a simple nuclear facility. The method's primary events (i.e., basic events and undeveloped events) are able to accommodate fault causes that result from threats.

The implementation of this new evaluation method for a radiotherapy facility using Cobalt-60 (Co-60) in Sardjito Hospital shows that its PPS are vulnerable; the threat of interrupting the electrical supply lines make the detection functions fail.

Keywords: physical protection system (PPS), vulnerability, methods, modification

I. Introduction

Nuclear materials are being stolen from nuclear facilities. Radiation sources from Caesium-137 (Cs-137) were stolen in Brazil in 1987; six people died and 20 others suffered radiological damage, as well as other radiation-related issues. Some hospitals in Indonesia use nuclear radiation for medical services, which means that malicious attacks are a possibility in the future. Nuclear security has become a national concern for Indonesia. Consequently, a physical protection system (PPS) is always implemented in nuclear facilities and nuclear medical facilities.

Understanding the susceptibility of a PPS in a nuclear medical facility is important. The existing methods of assessing the vulnerability of a PPS tend to be implemented in complex nuclear facilities. However, not many methods that analyze vulnerability for simple nuclear facilities such as nuclear medical facilities exist. Thus, a simple method to analyze vulnerability needs to be developed.

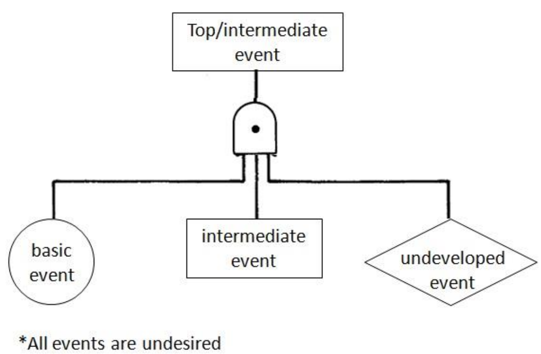
The fault tree analysis learns from an undesired event in system levels and relates event to its causes in component levels, which provides an opportunity to include security threats. Finding a modified fault tree method of analysis for analyzing the vulnerability of a PPS is the topic of this research.

II. Method

Fault tree analysis is a deductive failure analysis that focuses on one particular undesired event and provides a method for determining the causes of that event. The undesired event appears as the top section in a fault tree diagram constructed for the system, and generally consists of a complete or catastrophic failure **[*1*]**. This top event is then deduced using a binary system to arrive at the primary event. Some intermediate events are possible between the top event and the primary event. These intermediate events are fault events that occur because of one or more antecedents' causes act through logic gates. Finally, the primary event is the event for one reason or another that has not been further developed. There are four events in the category of primary event (i.e., basic, undeveloped, conditional, and external).

The two important events in this occasion are a basic event and an undeveloped event. The basic event is the event, which does not to be developed further, while the undeveloped event is the event in which further development is unavailable, possibly because it is external to the system.

The basic designed structure or hierarchy of events in a fault tree analysis/diagram is shown below:



a) Basic event structure for AND gate

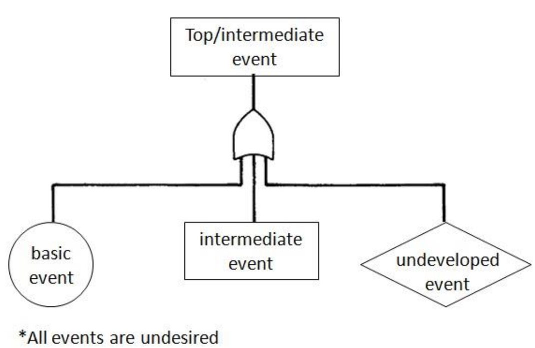
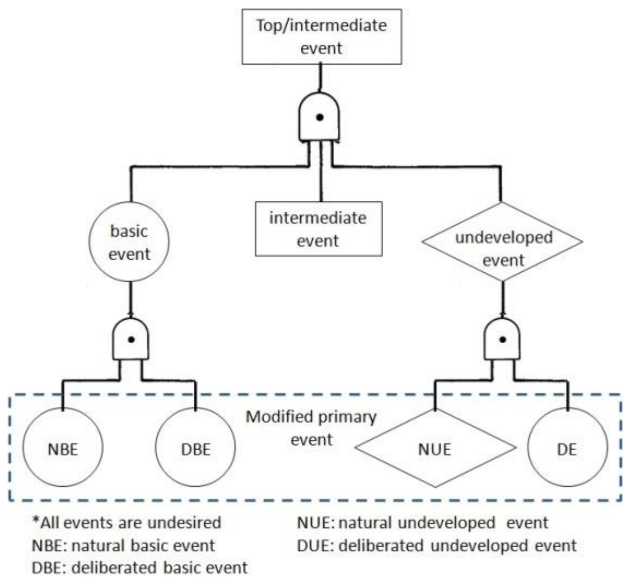


Figure 1. Basic event structure of fault tree analysis

The basic event and undeveloped event may be explored in order to understand their characteristics based on the question, "is there any opportunity to put a deliberate and malicious action (security threat) within it?" The developed method modifies the basic event structure (Fig. 1) in its primary event. The result is shown below:



a) Modified basic event structure for AND gate

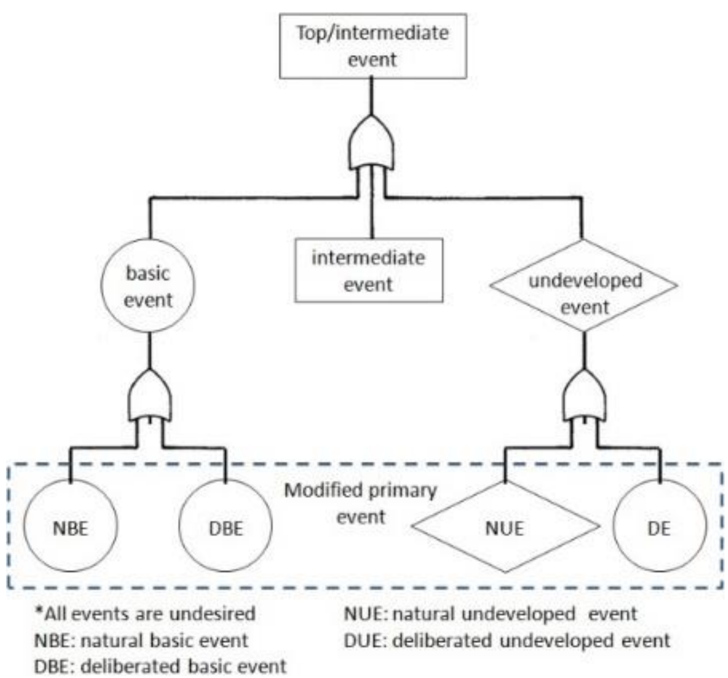


Figure 2. Modified basic event structure of fault tree analysis.

International Journal of Nuclear Security, Vol. 2, No. 2, 2016

The natural basic event (NBE) is a basic event that occurs naturally (i.e. the technical failure of component functions). Meanwhile, the deliberate basic event is the failure of component functions that occur deliberately (a threat). The natural undeveloped event is an event that is not naturally developed. In addition, the deliberate undeveloped event is an event that has a nature of deliberate occurrence (deliberately interrupting the power supply).

Modifying the primary event in a fault tree analysis enriches the capability of this method to include any deliberate action (a security threat).

III. Result

Using the modified fault tree to analyze the PPS of radiotherapy facilities, Sardjito General Hospital shows that its detection system is highly vulnerable. The fault tree diagram produced is shown below.

The security incident will occur if detection functions fail, if functions are delayed, or if there are response functions. The analysis is focused on a detection function because it consists of equipment and human action.

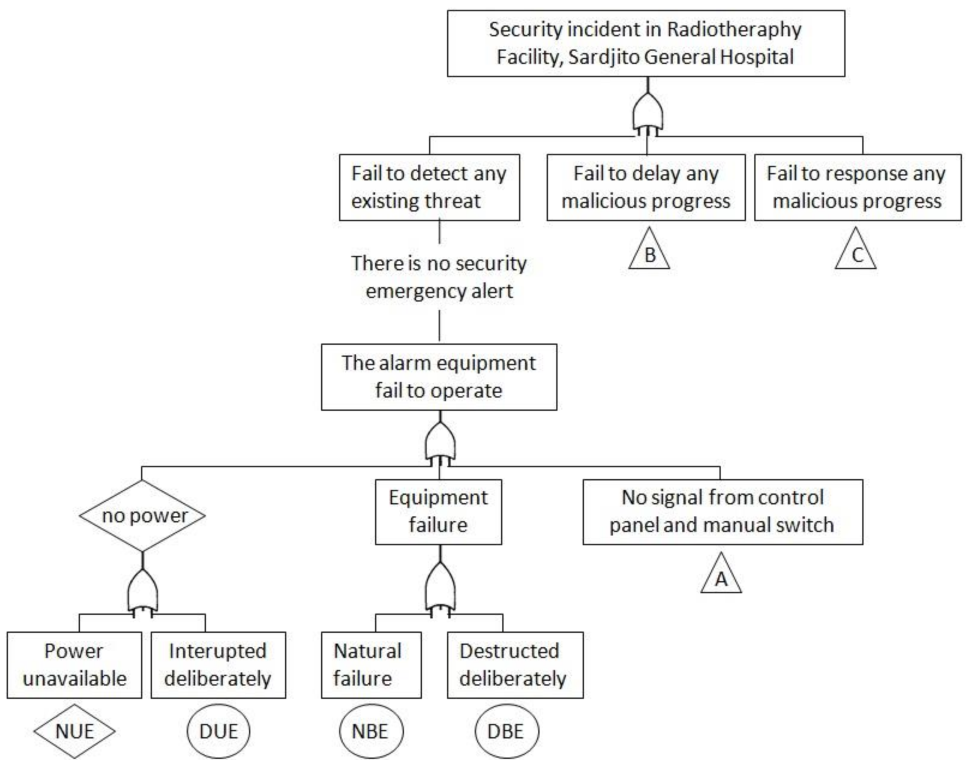


Figure 3. Modified fault tree diagram for the PPS of the Sardjito General Hospital's Radiotherapy Facility.

IV. Discussion

Overall, the result shows that the modified fault tree analysis is able to include the security threat as part of its primary event. The diagram demonstrates that the detection function will fail because of three causes; every cause is able to fail the detection function (OR logic). The threat may affect power supplies and equipment failures. The malicious act may interrupt the power supply deliberately, as well as destruct the alarm equipment. If one of these threats occurs, the detection function fails directly. This means the PPS is highly vulnerable to security incidents.

There are two possible results regarding security threats. The first is that the threat becomes a single cause, which is able to fail the system function; this case is given in the result of the implementation (Fig. 3). If it is assumed that the probability of threat occurrence is one that means that any threat will always succeed. Consequently, the PPS is highly vulnerable and must be redesigned.

The second possibility is that the cause of the top event is an "AND combination" of threats and component failures. Using the similar assumption that the probability of a threat is one, the probability of the combination of threats and component failures is the probability of component failures.

V. Conclusion

The result shows that the fault tree analysis may be modified to provide a method of vulnerability evaluation for a PPS in a simple nuclear facility. The criteria used for evaluation are inherently provided by the method; there are only two vulnerability states that are highly vulnerable or similar to the failure probability of the hardware system of the PPS.

VI. Acknowledgements

We thank the Department of Nuclear Engineering and Engineering Physics, Faculty of Engineering, and the Universitas Gadjah Mada for its financial support of our research. We also thank the unit of Radiology and Nuclear Medicine at Sardjito General Hospital, as well as the staff that provided the operational support of our research.

VII. Works Cited

1. US Nuclear Regulatory Commission, "Fault Tree Handbook" (NUREG 0492, Washington, DC, 1981), (available at http://www.nrc.gov/docs/ML1007/ML100780465.pdf).

VIII. Author Bio and Contact Information

Haryono Budi Santosa
Santosa is a lecturer in the Department of Nuclear Engineering and Engineering Physics at Universitas Gadjah Mada Indonesia, after graduating from the Nuclear Engineering Program in 1987. His research focuses on safety and reliability engineering. In 2014, Santosa joined the nuclear security working group in the department. He has published his works in several international conferences and journals.
Email: hbs@ugm.ac.id