2011 International Nuclear Atlantic Conference - INAC 2011
Belo Horizonte,MG, Brazil, October 24-28, 2011
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR - ABEN
ISBN: 978-85-99141-04-5

USE OF RISK ASSESSMENT METHODS FOR SECURITY DESIGN AND ANALYSIS OF NUCLEAR AND RADIOACTIVE FACILITIES

Vanderley de Vasconcelos[1], Marcos C. Andrade[1] and Elizabete Jordão[2]

[1] Centro de Desenvolvimento da Tecnologia Nuclear - CDTN/CNEN
Caixa Postal 941
30161-970 Belo Horizonte, MG
vasconv@cdtn.br
mca@cdtn.br

[2] Faculdade de Engenharia Química - FEQ - UNICAMP
Caixa Postal 6066
13.083-970 Campinas, SP
bete@feq.unicamp.br

ABSTRACT

The objective of this work is to evaluate the applicability of risk assessment methods for analyzing the physical protection of nuclear and radioactive facilities. One of the important processes for physical protection in nuclear and radioactive facilities is the identifying of areas containing nuclear materials, structures, systems or components to be protected from sabotage, which could directly or indirectly lead to unacceptable radiological consequences. A survey of the international guidelines and recommendations about vital area identification, design basis threat (DBT), and the security of nuclear and radioactive facilities was carried out. The traditional methods used for quantitative risk assessment, like FMEA (Failure Mode and Effect Analysis), Event and Decision Trees, Fault and Success Trees, Vulnerability Assessment, Monte Carlo Simulation, Probabilistic Safety Assessment, Scenario Analysis, and Game Theory, among others, are highlighted. The applicability of such techniques to security issues, their pros and cons, the general resources needed to implement them, as data or support software, are analyzed. Finally, an approach to security design and analysis, beginning with a qualitative and preliminary examination to determine the range of possible scenarios, outcomes, and the systems to be included in the analyses, and proceeding to a progressively use of more quantitative techniques is presented.

1. INTRODUCTION

In recent years, there has been growing concern of society with acts of terrorism, sabotage, vandalism and theft involving nuclear materials or radioactive sources worldwide [1]. After September 11, 2001, the perception of the physical protection of nuclear facilities changed, as the perception of nuclear safety was altered following TMI-2 accident. After this 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 and external events such as earthquakes, fires, floods, tornadoes and tsunamis. On the other hand, risk assessments commonly conducted in nuclear and radioactive facilities, for design or licensing purposes, involve almost always industrial safety and radioprotection issues without taking into account the security of such facilities.

There are many risk assessment approaches that have been applied in knowledge areas such as nuclear engineering, aerospace engineering, information security, natural hazard risk assessment, national defense and intelligence analysis. They range from intuitive qualitative methods to sophisticated mathematical ones. While some methods require data from historical operations or from system design specifications, others require only opinions from experts or qualitative analysis. Such methods can be applied upon some adjustments, to security design and analysis of nuclear and radioactive facilities.

2. SECURITY OF NUCLEAR AND RADIOACTIVE FACILITIES

As sciences analyzing and describing security risks are relatively new and developing, so there are ambiguities in the use of related terms. At the scope of the present paper, the following security and risk concepts and terminology are adopted. These concepts and terminologies are based on references 3, 4, 5 and 6, if not otherwise indicated.

2.1. Basic Concepts and Terminologies

- *Nuclear safety:* means measures intended to minimize the likelihood of accidents involving radioactive sources and, should such an accident occur, to mitigate its consequences;
- *Nuclear security:* refers to the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. In this paper it is used as synonym of physical protection of nuclear and radioactive facilities [7];
- *Risk*: expresses the combination of the probability of an undesired event and its consequence;
- *Risk assessment:* refers to the technical assessment of the nature and magnitude of a risk. It involves basically the answers to three questions: What can go wrong? How frequently does it happen? What are the consequences?
- *Risk analysis*: includes those functions, as well as methods to best use the resulting information from risk assessment. In this paper it includes methods for threat assessment, vulnerability assessment, scenario likelihood and criticality assessment [8];
- *Risk management:* includes the acknowledgement that if the risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. Risk control and mitigation measures are also encompassed by this concept;
- *Nuclear security risk assessment:* is an analytical and systematic process, which allows the evaluation of the probability of a threat to result in a negative action towards the vital areas of nuclear and radioactive facilities;
- *Vital area*: is 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;
- *Sabotage:* refers to any deliberate act directed against a nuclear or radiological facility, or material in use, storage or transport that could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive or nuclear materials;
- *Threat:* is an entity with motivation, intention and capability to commit a malicious act;
- *Threat assessment:* is an evaluation of the existing threats, usually including intelligence assessments, which describe the motivation, intentions, and capabilities of these threats to commit malicious acts*;*

- *Vulnerability assessment*: is a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses;
- *Criticality assessment:* is a process designed to systematically identify and evaluate an organization's assets based on their values, the importance of its mission or function, the group of people at risk, or the significance of a facility;
- *Design Basis Threat – DBT:* is a comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated. Such definition permits security planning on the basis of risk management;
- *Unacceptable consequence:* it is a threshold of consequence stated to justify that resources should be expended to prevent its occurrence;
- *Safeguards:* refers to measures to protect against accidents. In this paper it is used as synonym of secureguards, a term that includes also the security measures needed to protect against threats [9].

2.2. Nuclear security risk background

The IAEA Nuclear Security Series of publications provides guidance for the prevention, detection and response to theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving radioactive or nuclear materials and their associated facilities. Publications in the Series are issued in the following categories [1]:

- *Nuclear Security Fundamentals*: containing objectives, concepts and principles of nuclear security and providing the basis for security recommendations;
- *Recommendations*: presenting best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals;
- *Implementing Guides*: providing further elaboration of the Recommendations and suggest measures for their implementation;
- *Technical Guidance*s: comprising Reference Manuals, with detailed measures and guidance on how to apply the Implementing Guides in specific areas;
- *Training Guides*: covering manuals for IAEA training courses in nuclear security; and
- *Service Guides*: which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

However, there are not in these publications, any systematic framework to carry out a security risk assessment of nuclear and radioactive facilities. Historically, risk assessment and risk management professionals have focused on accident risks, natural hazard risks, business interruption risks, project risks, and financial risks. In these areas, organizations have used very systematic processes and tools to understand and prioritize these diverse risks, especially those with unacceptable consequences [2, 10]. Security related risks are another broad category of risks with potentially unacceptable consequences. While security related risks require a different approach than other types of risk, the same fundamentals can be applied. Terrorist attacks and other malicious acts are a different type of threat, but they pose risks in much the same way as other threats [11].

A quantitative security risk assessment can be subdivided in the followings steps [8]:

- *Threat assessment*: detection of the presence of hostile groups and the threat level near the facility;

- *Vulnerability assessment*: vital area identification and analysis of the protection systems for the vital areas and evaluation of the accessibility and vulnerability levels.
- *Criticality assessment*: analysis of the potential accidental scenarios in consequence of the success of the attacks on critical targets. Includes the analysis of the costs for the re-establishment of the critical targets and evaluation of the missed indirect incomes because of their unavailability, and evaluation of the economic losses related to every accidental scenario.

The quantification can be done through the followings generalized relations:

$$Risk = Frequency(F) \times Consequence(C) \quad (1)$$

Applying the equation 1 to security risks:

$$F = Initiating\ Event\ Frequency \times Probability\ All\ Safeguards\ Fail \quad (2)$$

$$Risk = [Threat(T) \times Vulnerability(V)] \times Criticality(C)], \quad (3)$$

where *Threat(T)* is a measure of the likelihood that a specific type of attack will be initiated against a specific target (that is, a scenario), *Vulnerability(V)* is a measure of the likelihood that various safeguards against a scenario will fail, and *Criticality(C)* is the magnitude of the negative effects if the attack is successful.

The framework to carry out the nuclear security risk assessment, proposed in this paper, is based on these relations.

3. OVERVIEW OF RISK ASSESSMENT METHODS

Figure 1 illustrates the entire process of risk assessment including the scenario identification, as well as the quantification of scenario frequencies and consequences [10].

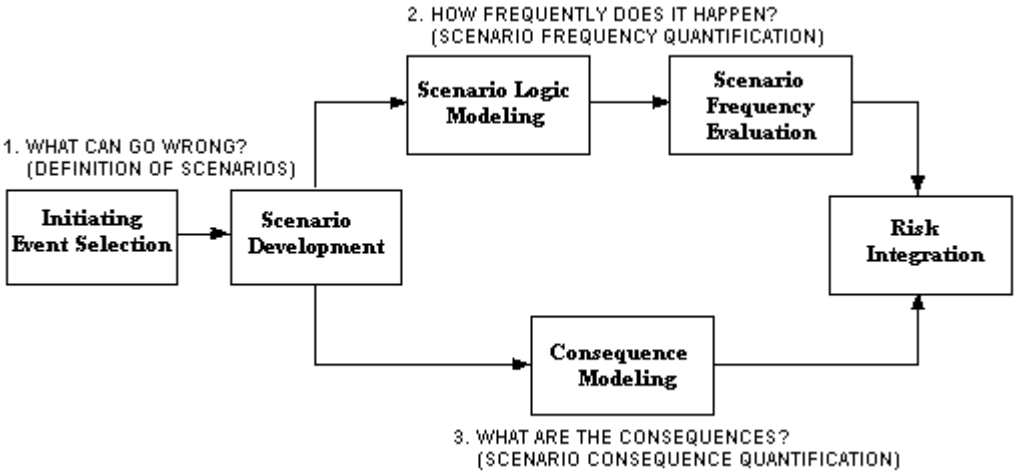

Figure 1. Process of risk assessment through the evaluation of scenario frequencies and consequences [10]

Some of risk assessment methods used in safety assessment processes are briefly described in the next following sections.

3.1. Failure Modes and Effects Analysis (FMEA)

FMEA is a tool that aids in quantifying severity, occurrences and detection of failures, as well as guiding the creation of corrective action, process improvement and risk mitigation plans. It may be useful for: identifying design or process related failure modes before they happen; determining the effect and the severity of these failure modes; identifying the causes and the possibility of occurrence of the failure modes; quantifying and prioritizing the risks associated with the failure modes; and developing and registering action plans that will be implemented to reduce risk [12].

An extension of FMEA focusing on the quantitative parameters for the criticality assigned to each probable failure mode is called FMECA (Failure Mode Effects and Criticality Analysis). The results highlight failure modes with relatively high probability and severity of consequences, allowing remedial efforts to be directed where they will produce the greatest value. The typical goal, when FMECA is performed as part of a design project, is to eliminate failure modes with high severity and high probability, and to reduce those with high severity or high probability. While FMEA is based on a qualitative approach, FMECA takes a more quantitative approach assigning a criticality and a probability of occurrence for each given failure mode.

3.2. Event and Decision Trees

Event Tree Analysis is a technique that uses a graphical logic model that identifies and quantifies possible outcomes following an initiating event. It is a kind of decision tree that provides a logical framework for determining and quantifying the sequence of events that can cause potential accidents. Event trees use inductive logic (normally binary) and are widely used in risk analysis in combination with fault trees. Decision trees are tools for helping to choose between several courses of action. They help to form a balance of the risks associated with each possible course of actions [12, 13].

3.3. Fault and Success Trees

Fault Tree Analysis is a technique used for estimating the frequency of a hazardous incident (called the top event) through a logic model of the failure mechanisms of the system. The analysis is initialized with the selection of an undesired top event and then tracing back to the possible causes, which can be component failures, human errors or any other events that can lead to the top event. This procedure proceeds systematically, identifying the sub-events that are the immediate precursors to the top event, the immediate precursors to the sub-events, and so on, until the basic events that are the primary causes of the top event be reached. Then, it is possible to estimate the frequency or the probability of occurrence of the top event though the logical combination of the primary events, using concepts of Boolean algebra and probability theory [12, 14].

Success trees are logical inverses of fault trees and may be obtained by applying de Morgan's theorem to fault trees. They can also be obtained directly from reliability block diagrams of the analyzed systems.

3.4. Monte Carlo Simulation

Monte Carlo simulation is a method for analyzing uncertainty propagation where the goal is to determine how random variation, lack of knowledge, or error affect sensitivity, performance, or reliability of the analyzed system. Monte Carlo simulation is a sampling method because the inputs are randomly generated from probability distributions to simulate the process of sampling from an actual population. Then, it is tried to choose a distribution for the inputs that most closely matches the available data, or best represents the current state of knowledge. The data generated from the simulation can be represented as probability distributions or converted to error bars, reliability predictions, tolerance zones, or confidence intervals [15].

3.5. Probabilistic Risk Assessment

Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis method intended to identify and assess the risks in complex technological systems for the purpose of improving their safety and performance [10]. PRA presents a set of scenarios, frequencies, and associated consequences, developed in such a way as to inform decisions regarding the allocation of resources to accident prevention, for instance, to evaluate changes in design or operational practice. Decision support in general requires quantification of uncertainty, and this is understood to be part of a PRA. Depending on the application area it is referred as QRA – Quantitative Risk Assessment, PSA – Probabilistic Safety Assessment, or Performance Assessment.

3.6. Other Risk Assessment Methods

Other methods that are potentially applicable to security risk assessment are: Analytic Hierarchy Process; Bayesian Networks; Expert-Opinion Elicitation; Influence Diagrams, Scenario Analysis; System Effectiveness Assessment; Game Theory; Decision Analysis; and Layers of Protection Analysis (LOPA) [16, 17, 18].

4. FRAMEWORK TO SECURITY RISK MANAGEMENT

A proposed framework for nuclear security risk management is illustrated at Figure 2. The application of the methodology begins with the definition of the scope of analysis. The motivation (identification of flaws, weaknesses and lack of controls), objectives and areas to be analyzed should be identified. The vital areas of nuclear and radioactive facilities are preferential targets to attacks.

The threat identification step look for human (hackers, ex-employees and intruders, etc.), environmental (fires, viruses, power outages, etc) or natural (floods, earthquakes, tornadoes, tsunamis, etc.) threats.

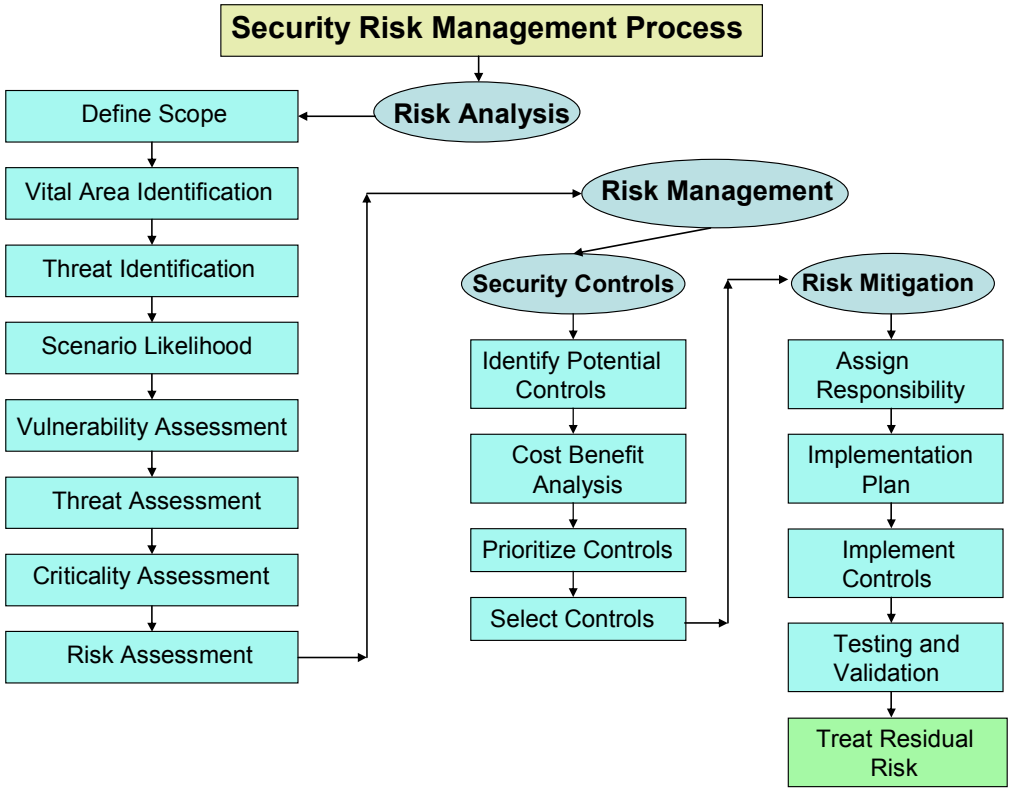

Figure 2. Proposed framework for security risk management

To perform the risk assessment process, the vulnerability, threat and criticality assessment should be carried out. Then, the likelihood of the threats, that depends on motivation, capability and existing controls should be estimated. Vulnerability assessment, as a function of absence or weakness of controls, and criticality assessment, as a measure of the impact to the facility, public or environment, are also part of the process.

The method to choose in each one of the above mentioned steps, if qualitative or quantitative, depends on many factors including the availability of data and support software, as well as the motivation of analysis. Table 1 presents an overview of available risk assessment methods and their potential applicability in the steps defined in the proposed framework. The applicability of such techniques to security issues, their pros and cons and the general resources needed to implement them, should be carefully analyzed on a cost benefit basis.

To complete the risk management process, the security controls and mitigation measures should be analyzed. If the estimated risks considering existing control and mitigation measures are not acceptable, alternative should be analyzed until residual risks are acceptable.

Figure 3 shows an application of one of the most common quantitative risk assessment technique to the analysis of a generic security system. As can be seen, the constructed fault tree shows the prevention, detection, control and mitigation measures and their possible combinations that can lead to top event. The use of this tool in both qualitative and quantitative nuclear security risk assessment processes can be useful for design and analysis of security systems.

Table 1 – Overview of Risk Assessment Methods and their Potential use in Security Risk Assessment (adapted from references 16 and 17)

Methods	Description	Applicability						
		1	2	3	4	5	6	7
Analytic Hierarchy Process	Heuristic approach intended to provide insight into preferences among alternatives.		X	X	X	X	X	X
Bayesian Networks	Graphical structure and set of conditional and unconditional probability distributions, as well as an algorithm for updating uncertainty based on evidence.		X	X	X	X	X	X
Event Trees, and Decision Trees	Diagrams of sequences of uncertain events, where paths through the trees represent specific scenarios.		X	X	X	X	X	X
Expert-Opinion Elicitation	Formal, heuristic process of obtaining information or answers to specific questions about adversaries, threat likelihoods, attack probabilities, vulnerabilities, failure probabilities, and potential consequences.	X	X	X	X	X	X	X
Failure Mode and Effect Analysis	Structured approach for identifying sequences of events that lead to system failure, consequences of failure, and mitigating actions or countermeasures.	X		X		X	X	X
Fault Trees, Success Trees and Attack Trees	Graphical hierarchical trees structure where an undesirable event (top event) and the possible means for this top event to occur are analyzed using probabilities and Boolean algebra.		X	X	X	X	X	X
Influence Diagrams	Graphical representation and algorithm for analyzing the probabilistic relationships among factors relevant to a decision.		X	X	X	X	X	X
Joint Staff Integrated Vulnerability Assessment (JSIVA)	Vulnerability based evaluation of an installation's ability to deter and respond to a terrorist incident, focusing both on omission essential vulnerable assets and antiterrorism/force protection targets such as shopping centers and schools.				X			
Monte Carlo Simulation	Uses probability distributions and relationships to obtain a probability distribution of system or process outputs.		X	X	X	X	X	X
Probabilistic Risk Assessment	Uses probability distributions of system factors to describe the variability of system behavior and estimate the likelihood of unfavorable consequences.		X	X	X	X	X	X
Scenario Analysis	Develops and analyzes uncertain future events using an internally consistent story about how events might unfold over time	X	X	X	X	X	X	X
System Effectiveness Assessment	Quantitative evaluation of the effectiveness of an integrated physical security system.				X			
Computer-Enhanced Scenario Analysis	Develops and analyzes uncertain future events using computer-driven scenario simulations or parametric iterations through a large range of scenario input parameters.		X	X	X	X	X	X
Game Theory	Mathematical analysis of players' strategies for achieving an optimal solution in light of opposition Strategies.		X	X	X	X	X	X
Multi-Objective Decision Analysis	Decision analysis technique that compares alternatives under conflicting objectives.		X	X	X	X	X	X
Layers of Protection Analysis	Simplified methods for assessing the value of protection layers on well-defined accident scenarios, comparing mitigated consequence frequency with risk tolerance criteria.	X	X	X	X	X	X	X

1 - Vital Area Identification 2 – Threat Identification 3 – Scenario Likelihood
4 – Vulnerability Assessment 5 – Threat Assessment 6 – Criticality Assessment 7 – Risk Assessment

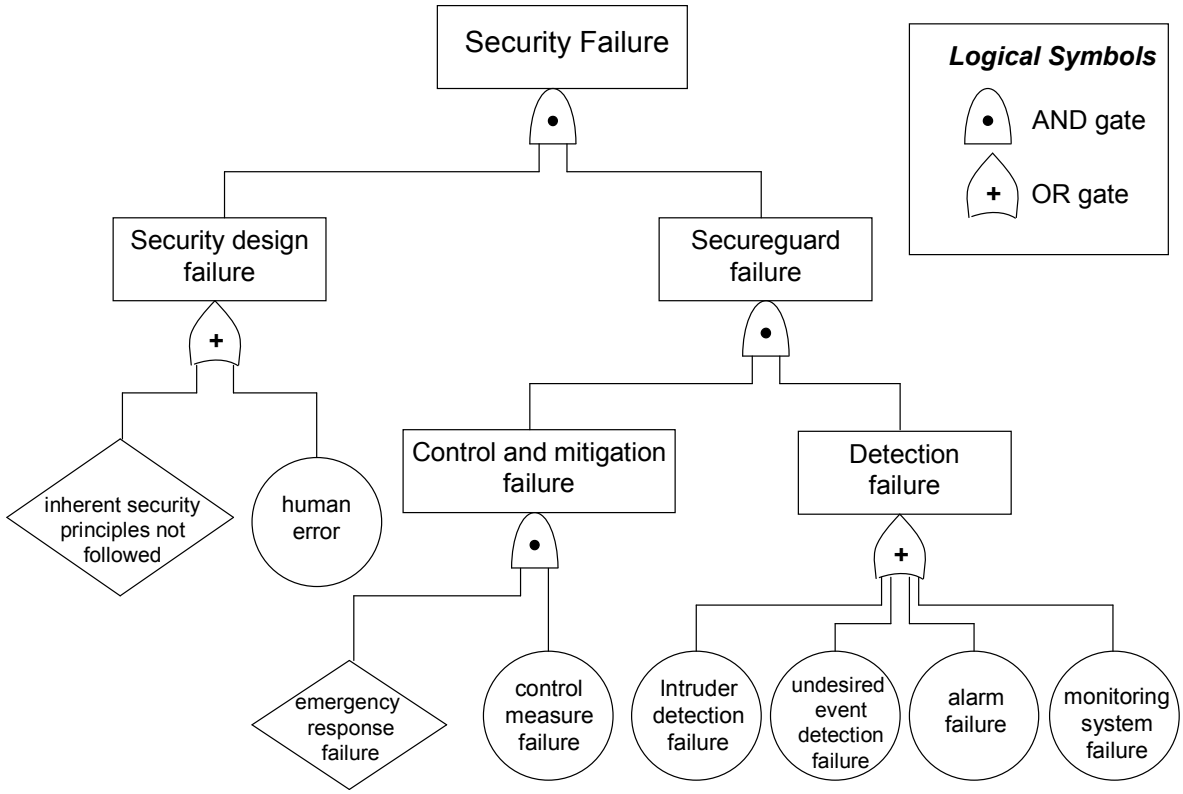

Figure 3. Example of an application of a fault tree to a generic security analysis

5. CONCLUDING REMARKS

A framework to security risk management of nuclear and radioactive facilities was presented. A set of common methods in risk assessment for safety evaluation are proposed to be used in security design and analysis of vital areas of such facilities. These methods can be used in both qualitative and quantitative assessments. Where there are not available data for detailed quantitative assessment, qualitative analysis can lead to identification of weaknesses of prevention, detection, control and mitigation measures, as well as to gain knowledge about specific security features of the facility.

Future works involving the development and application of systematic methodologies for nuclear security risk assessment are suggested. The applicability of risk assessment methodologies to security issues, their pros and cons and the general resources needed to implement them, should be carefully analyzed.

ACKNOWLEDGMENTS

The authors would like to thank the Center of Nuclear Technology Development - CDTN/CNEN, and FAPEMIG (Minas Gerais State Foundation for Research Development) that sponsored this work, and their colleagues of CDTN/CNEN who were involved with this work.

REFERENCES

1. M. Gregoric. "IAEA Nuclear Security Series", *Proceeding of International Forum in Peaceful Use of Nuclear Energy and Nuclear Non-Proliferation Meeting*, Tokyo, Japan, 2-3 February, http://www.jaea.go.jp/04/np/activity/2011-02-02/2011-02-02-15.pdf (2011).
2. F. H. van Duijne, D. van Aken and E. G. Schouten, "Considerations in developing complete and quantified methods for risk assessment", *Safety Science,* **46**, pp. 245-254 **(**2008).
3. F. M. Christensen. et al., "Risk terminology - a platform for common understanding and better communication", *Journal of Hazardous Materials*,.**103**, pp. 181-203 (2003).
4. World Health Organization, *IPCS Risk Assessment Terminology*, International Programme on Chemical Safety (ICPS), Geneva (2004).
5. Comissão Nacional de Energia Nuclear, Proteção Física de Unidades Operacionais da Área Nuclear *Norma CNEN NE-2,01*, Rio de Janeiro, Brazil (1996).
6. International Atomic Energy Agency, *Development, Use and Maintenance of the Design Basis Threat.* IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
7. 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).
8.. G. Tamasi and M. Demichela, "Risk assessment techniques for civil aviation security", *Reliability Engineering and System Safety,* **96**, pp. 892-899 **(**2010).
9. P. Baybut, "Process security management systems: Protecting plants against threats", *Chemical Engineering*, **48 (**2003).
10. M. Stamatelatos et al., *Probabilistic Risk Assessment procedures guide for NASA managers and practitioners - Version 1.1*, Office of Safety and Mission Assurance, NASA Headquarters, Washington D.C. (2002).
11. H. K. Naoki Satoh, "Analysis of information security problem by probabilistic risk assessment", *International Journal of Computers*, **3 (3)**, pp. 337-347 **(**2009).
12. M. J. Borysiewicz et al, *Quantitative Risk Assessment (QRA)*, Institute of Atomic Energy, CoE MANHAZ, Poland (2003).
13. Jaejoo Ha, W. S. Jung and C.K. Park, "The application of PSA techniques to the vital area identification of nuclear power plants", *Nuclear Engineering and Technology,* **37 (3)**, pp. 269-264 **(**2005).
14. P. J. Brook and R. F. Paige, "Fault trees for security system design and analysis", *Computers & Security,* **22 (3)**, pp. 256-264 **(**2004).
15. F. Cadini, J. De Sactis, T. Girotti, E. Zio, A. Luce and A. Taglioni, "Monte Carlo-based assessment performance of a radioactive waste repository", *Reliability Engineering and System Safety,* **95**, pp. 859-865 **(**2010).
16. M. C. Cummings, D. C. McGarvey and P. M. Vinch, *Homeland Security Risk Assessment - Volume I. Setting*, Homeland Security Institute, Washington, D.C. (2006).
17. M. C. Cummings, D. C. McGarvey and P. M. Vinch, *Homeland Security Risk Assessment - Volume II. Methods, Techniques, and Tools*, Homeland Security Institute, Washington, D.C. (2006).
18. U. S. Nuclear Regulatory Commision, *Integrated safety analysis – Guidance document - NUREG-1513*, Office of Nuclear Material Safety and Safeguards, Washington D.C. (2001).