SAND2008-3573C

VITAL AREA IDENTIFICATION FOR NUCLEAR FACILITIES

G. Bruce Varnado
Sandia National Laboratories*
P.O. Box 5800, MS-1361, Albuquerque, NM 87185-1361

ABSTRACT

Vital areas are those nuclear facility areas that are protected against sabotage in order to prevent malicious acts that could lead to unacceptable radiological consequences. Methods for the systematic identification of vital areas were developed in the late 1970s and applied to all United States nuclear power plants [1], [2], [3]. Those methods have been expanded and updated for use in an International Atomic Energy Agency guidance document on vital area identification that is scheduled to be published in the near future. In addition, the United States Nuclear Regulatory Commission is developing guidance for nuclear power plant license applicants to use in defining vital areas in new plants. This paper provides a review of the latest vital area identification process and the technical basis for the methods used in that process.

INTRODUCTION

Nuclear facilities may contain large inventories of radioactive materials that could, if released, cause radiological hazards to workers, the public, and the environment. Any deliberate act directed against a nuclear power plant that could directly or indirectly endanger public health and safety by exposure to radiation is defined as radiological sabotage [4], [5]. International Atomic Energy Agency and Nuclear Regulatory Commission guidance specify requirements for protection of nuclear facilities against radiological sabotage, including the location of vital equipment in vital areas (VAs). It is therefore necessary for each nuclear facility licensee to identify the VAs that the required physical protection measures will be applied to in order to prevent sabotage. For large, complicated nuclear facilities, such as nuclear power plants, it is desirable to determine the minimum number of VAs that must be protected in the plant to minimize the cost, safety, and operational impacts of physical protection measures.

As noted above, nuclear facilities must provide protection against malicious acts that could lead directly or indirectly to unacceptable radiological consequences (URC). Malicious acts that could lead directly to URC are those in which the attacker applies energy (such as using explosives or incendiary devices) to the nuclear material to disperse it. Direct sabotage attacks generally require the attacker to gain physical access to the area in which the material is used or stored. Malicious acts that lead indirectly to URC are those in which the attacker uses thermal or mechanical energy stored in the material or in a process system to disperse the material. Indirect sabotage attacks may be possible without gaining direct access to the material, such as through attacks on cooling or other process or safety systems. The vital area identification (VAI) process described in this paper can be used to identify a minimum set of areas to protect in order to ensure that none of the possible direct or indirect sabotage attacks can be completed.

VAI PROCESS

The VAI process is depicted in Figure 1. The steps of VAI are as follows:

1. Address policy considerations—The regulatory body must make key policy decisions (such as URC criteria) that form the basis for VAI.
2. Evaluate site and facility characteristics—Determine the inventories of nuclear and radioactive material and the facility and site characteristics needed to determine whether sabotage could lead to URC.
3. Perform conservative analysis—Determine whether the complete release of any inventory could exceed the URC criteria. Include direct dispersal of any such inventory as an event in the sabotage logic model and continue with the process described below.
4. Identify initiating events of malicious origin (IEMO)—Identify any initiating events (IE) [6] that can, alone or in combination with other malicious acts, lead indirectly to URC and identify the systems required to mitigate those IEs.
5. Develop sabotage logic model—Construct a sabotage logic model that identifies the combinations of events that would lead to URC.
6. Assess threat capabilities—Eliminate from the sabotage logic model any events that the assumed threat does not have the capability to perform.
7. Identify areas corresponding to sabotage logic model events—Identify the locations (areas) in which direct dispersal, IEMOs, and the other events in the sabotage logic model can be accomplished. Replace the events in the sabotage logic model with their corresponding areas.
8. Identify candidate VA sets—Solve the sabotage area logic model to identify the combinations of locations that must be protected to ensure that URC cannot occur.
9. Select a VA set—Select the VA set that will be protected to prevent sabotage leading to URC.

1. POLICY CONSIDERATIONS

The State regulatory body is responsible for establishing sabotage protection requirements for nuclear facilities, including requirements for VA identification and protection. The regulatory body must address the following policy considerations in order to set the requirements for VAI:

- What is the explicit definition of URC?
- For what operational states must VAs be identified and protected?
- What constitutes a safe facility state that should be achieved following a sabotage attack for each operational state?
- Is it necessary to assume that equipment unavailability events (maintenance and random failure) occur concurrent with a sabotage attack?
- Can credit be taken for accident management recovery actions following a sabotage attack?
- What is the threat against which the facility should be protected (design basis threat [DBT])?

The answers to these questions, as specified by the regulatory body, set the ground rules or assumptions for the analyses performed in the VAI process.

2. SITE AND FACILITY CHARACTERISTICS

The first step in performing the VAI analysis is to determine the inventories of nuclear or radioactive material present and the facility and site characteristics that will be needed to determine

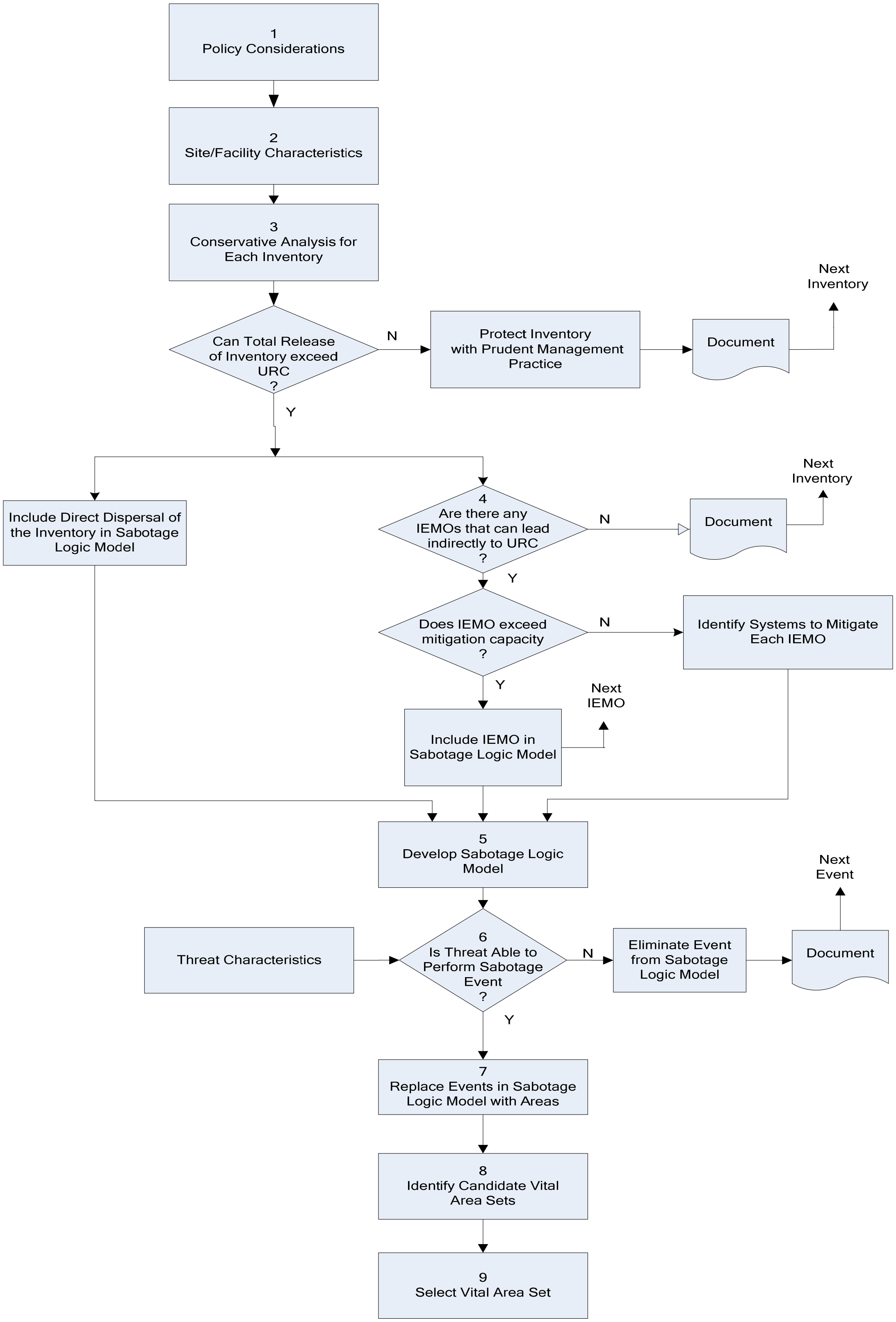
1
Policy Considerations
2
Site/Facility Characteristics
3
Conservative Analysis for Each Inventory
Can Total Release of Inventory exceed URC ?
N
Protect Inventory with Prudent Management Practice
Document
Next Inventory
Y
Include Direct Dispersal of the Inventory in Sabotage Logic Model
4
Are there any IEMOs that can lead indirectly to URC ?
N
Document
Next Inventory
Y
Does IEMO exceed mitigation capacity ?
N
Identify Systems to Mitigate Each IEMO
Y
Include IEMO in Sabotage Logic Model
Next IEMO
5
Develop Sabotage Logic Model
Threat Characteristics
6
Is Threat Able to Perform Sabotage Event ?
N
Eliminate Event from Sabotage Logic Model
Document
Next Event
Y
7
Replace Events in Sabotage Logic Model with Areas
8
Identify Candidate Vital Area Sets
9
Select Vital Area Set

Figure 1. VAI Process

whether sabotage could lead to URC. This requires information on the following:

- The site (area in which the facility is located)—Required information includes the population density in the vicinity of the facility and other site characteristics needed to determine the potential consequences of radiological releases.
- The facility—Required information includes the locations of nuclear and radioactive materials; material forms, characteristics, and quantities; critical safety functions (e.g., control of reactivity, cooling of radioactive material, and confinement of radioactive material) [7]; and the process and safety system details.

The information needed for site and facility characterization should be available from the facility safety analysis documentation.

3. CONSERVATIVE ANALYSIS OF RADIOLOGICAL CONSEQUENCES

A conservative analysis should be performed to determine the potential radiological consequences of the complete release of each nuclear or radioactive material inventory at the facility. The analysis should be performed without consideration of physical protection and mitigation measures present at the facility. The calculation of radiological consequences should be based on conservative data and assumptions. The purpose of this conservative analysis is to eliminate from further consideration any nuclear or radioactive material inventories so small that even an unmitigated release will not exceed URC. If the potential radiological consequences estimated for an inventory under these conservative analysis conditions are below the level of URC, radiological sabotage is not possible for this inventory. Consequently, it is not necessary to designate any VAs associated with this inventory, and the inventory may be protected in accordance with prudent management practice.

If the potential radiological consequences of the release of a complete inventory are equal to or greater than the URC limit, the possibility of sabotage that could lead directly to URC must be considered. Consequently, the direct dispersal of the inventory should be included in the sabotage logic model as a potential malicious act leading directly to URC, and the remaining steps of the VAI process should be performed for the inventory. The feasibility that the threat could cause direct dispersal of the inventory is addressed when the threat characteristics are considered later in the process.

4. INITIATING EVENTS OF MALICIOUS ORIGIN

To determine the areas that must be protected to prevent acts that lead indirectly to URC, two types of sabotage attacks must be considered:

1. The attacker causes an IE that creates conditions more severe than the facility mitigating systems can accommodate (that is, events that are beyond the safety design basis).
2. The attacker causes an IE *and* disables the systems needed to mitigate the effects of the IE.

An IE that is deliberately caused by an adversary in an attempt to cause a release from a facility is called an IE of malicious origin, or IEMO. Facility safety analyses, such as a deterministic safety assessment (DSA) or a probabilistic safety assessment (PSA) report [8], will have already identified and analyzed many IEs that could be caused by random failure, human error, etc. These events could also be caused by malicious acts and can serve as a starting point for identifying IEMOs. When identifying the IEMOs, the VAI team should consider events that may not be included in the safety analyses and that must be included in the VAI process (that is, events that are impossible or extremely unlikely to occur accidentally but could be caused maliciously). Each IEMO should be assessed to determine whether there are systems capable of mitigating it.

Every IEMO that exceeds mitigating system capacity should be included in the sabotage logic model as a potential malicious act leading to URC. The feasibility that the DBT could cause an IEMO that exceeds mitigating system capacity is addressed when the threat characteristics are considered later in the process.

In order to address IEMOs that are within mitigating system capacity, the combinations of IEMOs and mitigating system disablement events that could lead to URC must be determined. These combinations of events that lead indirectly to URC are detailed in the sabotage logic model. The feasibility that the DBT could cause the IEMOs or disablement events is addressed when the threat characteristics are considered later in the process.

The specific systems that are used to mitigate IEs depend upon the facility and the amount or type of the radioactive material it contains, and may differ depending upon the facility operational state. Systems that are used to mitigate IEs are those that support safety functions such as reactivity control, decay heat removal, coolant boundary integrity, and containment integrity [6], [9]. The systems that directly perform critical safety functions are defined to be front line systems, while those required for proper functioning of the front line systems are defined to be support systems. The successful operation of a front line system may depend upon the availability of one or more support systems, and it is essential that these dependencies be identified. If a PSA has been prepared for the facility, the information on front line and support systems should be readily available from the PSA or supporting documentation.

Front line or support system success criteria are defined as the minimum performance needed for the fulfillment of the system’s safety function under the specific conditions created by an IEMO [9]. Relevant information for developing front line system and support system success criteria is given in facility safety analyses. The success criteria for front line systems are of particular importance for the VAI analysis because they define the starting points for the subsequent logic modeling of the system sabotage scenarios. Success criteria include performance measures (e.g., flow rate, response time) and hardware requirements (e.g., the number of required flow paths, power trains, etc.),

5. SABOTAGE LOGIC MODEL

The next step in performing a VAI is constructing a sabotage logic model that identifies the events or combinations of events that could lead to URC. These include the direct dispersal of radioactive material, IEMOs that exceed mitigating system capacity, and the combinations of events (IEMOs and mitigating system disablement events) that will lead to URC for IEMOs that are within mitigating system capacity.

Direct dispersal and IEMOs that exceed mitigating system capacity are included in the logic model as single events leading to URC. The portion of the logic model that deals with IEMOs within mitigating system capacity includes each such IEMO combined with the malicious disablement of the specific systems designed to mitigate the IEMO. Logic models for system disablement are developed to the component level using a top-down approach. The logic models must be developed in sufficient detail to allow linking of disablement events to the facility locations (areas) in which disablement can be accomplished.

A PSA will contain detailed logic models that can be used, directly or with some modification, in developing the sabotage logic model for IEMOs within mitigating system capacity. The model development is typically done in two stages. The first stage is the development of the facility sabotage logic model that represents the combinations of IEMOs and disablement of front line systems leading to URC. The second stage is the development of system sabotage logic models for individual front line systems and the support systems upon which they depend. The logic models are developed either by modifying existing logic models from the facility PSA, if one has been prepared, or by developing logic models using facility system configuration information and the success criteria and dependency information. This process produces the facility sabotage logic model that links each IEMO with the disablement of the front line systems required to mitigate it, and system logic models that detail the ways front line systems can be disabled (either directly or by disabling their support systems). The basic events in the sabotage logic models will be the direct dispersal events, the IEMOs, and the events that disable mitigating system components.

6. THREAT CAPABILITY TO PERFORM SABOTAGE EVENTS

The sabotage events addressed in the preceding sections do not consider the capability of the threat to perform the malicious acts required to cause URC. All events that could lead directly or indirectly to URC are included to ensure that no potential VAs are overlooked, without regard to whether the DBT capabilities are sufficient to perform the sabotage acts. If the DBT characteristics change, the information and models developed in the preceding steps will be valid for use in identifying VAs under the changed threat conditions.

In this step of the process, any events that are not credible, given the DBT capabilities, should be eliminated from consideration. The threat capability to perform the direct dispersal of material, to cause the IEMOs, and to disable the mitigating systems should be assessed. The events that are beyond the capability of the threat should be removed from the sabotage logic model. An analysis of the potential consequences more realistic than the conservative analysis discussed above may also be performed at this point in the process.

Furthermore, any events that cannot be prevented by the facility physical protection system should be identified. Generally, any events that the threat can accomplish without gaining access to the site should be assumed to always occur. For example, it is practically impossible for the facility physical protection system to prevent the loss of offsite power, because the threat can cause loss of offsite power in many ways without gaining access to the facility. Therefore, the VAI process should assume that offsite power is unavailable. Any other such events in the sabotage logic model should be identified and flagged for proper treatment in the area identification process described below.

7. SABOTAGE AREA LOGIC MODEL

The next step in the VAI process is identifying and documenting the areas from which an adversary could accomplish each event in the sabotage logic model. The information about these areas is collected through a structured process and verified by conducting a walk-down of the facility. The area data are entered into the sabotage logic model by replacing each event (each direct dispersal event, IEMO, and each mitigating system disablement event) in the model with the area or areas from which it can be caused. Events that the threat can perform without gaining access to the facility should be replaced with a logical “1” in the logic model. The result is a sabotage area logic model in which the basic events are facility areas.

Additional consideration is required to address spatial interactions between adjacent areas. There may be cases in which a malicious act in one area can disable equipment, components, or devices in one or more adjacent areas. External event safety analyses such as seismic, fire, and flooding PSAs provide useful information on spatial interactions. Additional guidance on how to address spatial interactions is available in Reference [10].

8. CANDIDATE VA SETS

Identifying candidate sets of VAs is accomplished in the following two steps:

1. The sabotage area logic model is analyzed to determine all combinations of areas an adversary would have to gain access to in order to complete sabotage scenarios that could lead to URC. Each such combination of areas is a minimal cut set of the sabotage area logic model. These combinations of areas are potential adversary target sets that can be used to develop sabotage scenarios for physical protection system evaluation exercises.
2. The sabotage area logic model is analyzed to determine minimal combinations of areas that must be protected to ensure that no sabotage scenarios that lead to URC can be completed. This step is accomplished by finding prevention sets [11] for the sabotage area logic model. A level 1 prevention set contains at least one area from each of the minimal cut sets of the sabotage area logic model and is equivalent to one of the solutions for the Boolean complement of that logic model. If the adversary is prevented from gaining access to all the areas in a prevention set, he will not be able to complete any of the sabotage attacks represented in the sabotage area logic model. Each of the level 1 prevention sets contains a minimal complement of equipment, systems, or devices which, if protected against sabotage, ensures that no sabotage attacks can be completed. Protection of each area in any one of these sets will prevent all of the sabotage scenarios that could lead to URC.

9. VA SET SELECTION

Each of the candidate VA sets meets the international requirements for a set of facility VAs [4]. The facility operator may choose to protect any one of the candidate VA sets. In making the selection of a set of areas to protect, the operator could take into account various factors important to safe and efficient operation of the facility. For example, the operator might select the candidate VA set that provides the optimum combination of the following:

- Low impacts on safety, plant operations, and emergency response
- Low difficulty of providing protection
- High effectiveness of protection measures
- Low cost of protecting the VAs

It is unlikely that one candidate VA set will receive the highest rating for each of the selection criteria. Thus, it will be necessary to make trade-offs between the ratings in the various areas and select the candidate VA set that is the overall best choice. This can be done using engineering judgment, or by employing a more structured analytical approach. References [12] and [13] provide examples of structured trade-off analysis methods.

CONCLUSION

All nuclear facilities are required to identify and protect VAs to prevent radiological sabotage. The VAI process described in this paper can be used to identify a minimum set of areas which, if protected, will preclude all radiological sabotage scenarios. The VA set will include the following:

- All areas from which the DBT has the capability to cause direct dispersal of radioactive material that exceeds the URC criteria
- All areas from which the DBT could cause IEs that exceed the mitigation capability of facility systems
- A minimum combination of areas whose protection will either prevent each IE that can be mitigated or protect a minimum set of equipment needed to mitigate the IE

Using the VAI process will allow nuclear facility operators to minimize the impact of physical protection on operation, safety, and cost of the facility while meeting physical protection requirements.

REFERENCES

[1] D.D. Boozer, et. al., *Safeguards System Effectiveness Modeling*, SAND76-0428, Albuquerque, NM, Sandia National Laboratories, 1976.

[2] G. B. Varnado and N. R. Ortiz, *Fault Tree Analysis for Vital Area Identification*, NUREG/CR-0809, SAND79-0946. Albuquerque, NM: Sandia National Laboratories, 1979.

[3] G. B. Varnado and R. A. Haarman, *Vital Area Analysis for Nuclear Power Plants*, SAND80-0553C. Albuquerque, NM: Sandia National Laboratories, 1980.

[4] International Atomic Energy Agency, “The Physical Protection of Nuclear Material and Nuclear Facilities,” INFCIRC/225/Rev. 4 (corrected), IAEA, Vienna, 1999.

[5] 10 Code of Federal Regulations, Part 73.2.

[6] International Atomic Energy Agency, “Safety of Nuclear Power Plants: Design,” NS-R-1, IAEA, Vienna, 2000.

[7] International Atomic Energy Agency, “IAEA Safety Glossary, Version 2.0,” IAEA, Vienna, 2006.

[8] International Atomic Energy Agency, “Safety Assessment and Verification for Nuclear Power Plants,” Safety Standards Series No. NS-G-1.2, IAEA, Vienna, 2001.

[9] International Atomic Energy Agency, “Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1),” Safety Series No. 50-P-4, IAEA, Vienna, 1992.

[10] International Atomic Energy Agency, Self-Assessment Guidelines for the Engineering Safety Aspects of the Protection of Nuclear Facilities against Sabotage, IAEA, Vienna, 2007.

[11] 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.

[12] R. L. Keeny and H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, Wiley, New York, 1976.

[13] T. L. Saaty, *Decision Making for Leaders*, Vol. II, AHP Series, RWS Publications, Pittsburg, PA, 2002.

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.