IAEA-NUCLEAR SECURITY SERIES-XXXX

(DRAFT)

Identification of Vital Areas at Nuclear Facilities

International Atomic Energy Agency

June 2007

FOREWORD

In response to a resolution by the IAEA General Conference in September 2002, the IAEA has adopted an integrated approach to protection against nuclear terrorism. This approach coordinates IAEA activities concerned with physical protection of nuclear material and nuclear installations, nuclear material accountancy, detection and response to trafficking in nuclear and other radioactive material, the security of radioactive sources, the security in the transport of nuclear and other radioactive material, emergency response and emergency preparedness measures in Member States and in the IAEA, and the promotion of adherence by States to relevant international instruments. The IAEA also helps to identify threats and vulnerabilities related to the security of nuclear and other radioactive material. However, it is the responsibility of the States to provide for the physical protection of nuclear and other radioactive material and associated facilities, to ensure the security of such material in transport, and to combat illicit trafficking and the inadvertent movement of radioactive material.

The International Atomic Energy Agency (IAEA) recommendations for protection of nuclear installations against sabotage are contained in INFCIRC/225/Rev.4, *The Physical Protection of Nuclear Material and Nuclear Facilities,* 1999, and IAEA-TECDOC-967 (Rev.1) *Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities,* May 2000. After the attacks of 11 September, 2001, the perception of the potential terrorist threat to nuclear installations changed, significantly and the IAEA initiated an effort to develop a series of guidance documents on the security of nuclear and radioactive materials and facilities. A new document, *Physical Protection of Nuclear Material and Nuclear Facilities against Sabotage,* currently being finalized, will provide the overarching framework for IAEA physical protection guidance against sabotage.

This publication provides detailed guidance with regard to vital area identification in support of INFCIRC/225/Rev. 4 and the Nuclear Security Series Implementing Guide: *Physical Protection of Nuclear Facilities and Nuclear Material against Sabotage*. INFCIRC/225/Rev. 4 recommends that "safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malicious acts, considered in the context of the State's design basis threat, to identify nuclear material, or the minimum complement of equipment, systems or devices to be protected against sabotage." This publication presents a structured approach to identifying the areas that contain equipment, systems, and devices to be protected against sabotage. The method builds upon safety analyses to develop sabotage logic models for sabotage scenarios that could cause unacceptable radiological consequences. The sabotage actions represented in the logic models are linked to the areas from which they can be accomplished. The logic models are then analysed to determine areas that must be protected to prevent these unacceptable radiological consequences.

The responsible officers at the IAEA regarding this document were David Ek and Arvydas Stadalnikas of the Office of Nuclear Security, and Sok Chul Kim of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The IAEA is preparing a set of guidance documents to be published in the *Nuclear Security Series* to assist Member States in the evaluation of their nuclear physical protection systems. The overarching publication for protection against sabotage in this set is *Physical Protection of Nuclear Material and Nuclear Facilities against Sabotage*. This publication, one of the supporting documents in the series, presents a systematic process for identifying the ***vital areas*** of a nuclear facility.

Identification of vital areas is an important step in process to protect against sabotage. ***Vital area identification*** (VAI) is the process for identifying the areas in a nuclear facility around which protection will be provided in order to prevent or reduce the likelihood of sabotage. INFCIRC/225/Rev. 4 (corrected) [1] — henceforth referred to as INFCIR/225 — indicates that safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malicious acts considered in the context of a State's design basis threat and designate as vital areas those areas containing nuclear material which, if sabotaged, could lead directly to unacceptable radiological consequences (URCs), and those areas containing the minimum set of equipment, systems, or devices which, if sabotaged, could lead indirectly to URCs[1]. All measures that have been designed into the facility for safety purposes should be taken into account when identifying vital areas.

1.2. OBJECTIVE

The objective of this publication is to describe a process that can be used to (i) identify all candidate sets of vital areas at a nuclear facility and (ii) select a specific set of vital areas that will be protected. The process for selection of a specific set of vital areas to be protected is based on consideration of the potential radiological consequences of sabotage, and the operational, safety, and physical protection objectives for the facility.

1.3. SCOPE

This publication focuses solely on the process for VAI at nuclear facilities. The VAI process can be used to identify the vital areas at existing facilities, and to evaluate the effect that design changes to existing facilities and design and layout features of new facilities may have on vital area selection.

1.4. STRUCTURE

Section 1 provides the background, objectives, and scope of this publication. Section 2 discusses the process used to identify vital areas, and the expected results of the process. Also, it outlines policy considerations that must be addressed by the competent authority (State regulatory body) and actions by the operator prior to the start of VAI, and describes the step-by-step process leading to the selection of a

[1] Unacceptable radiological consequences, as discussed in INFCIRC/225, refer to relatively severe radiological consequences resulting from large nuclear facilities such as nuclear power plants. (This can be inferred from the requirement to use vital areas in protected areas to prevent URC. This level of protection, afforded by two layers, is similar to that required to prevent the theft of Category 1 nuclear material.) In the context of a graded approach, there may be URCs for which the level of protection afforded by a vital area inside a protected area is not warranted.

minimum set of areas in a nuclear facility that should be protected as vital areas. Section 3 provides guidance for documenting the results of VAI. The Appendix provides an example of how logic models can be solved to identify candidate vital area sets.

2. VITAL AREA IDENTIFICATION PROCESS

This section describes the process used to identify vital areas in a nuclear facility. INFCIRC/225/Rev 4 defines a vital area as "an area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences." [1] The vital area concept is used to define a boundary around the vital equipment, systems, or devices to which physical protection can be applied. The objective of the VAI process is to identify a minimum set of areas of a facility containing the vital equipment, systems or devices that, if adequately protected, will prevent these URCs.

2.1. PROCESS OVERVIEW

The VAI process is depicted in Figure 2-1. The steps of VAI are as follows:

- Gather information that is input to the VAI process.
    - Policy considerations. Address the key policy considerations essential to the VAI process.
    - Site and facility characteristics. Determine the inventories of nuclear and radioactive material. Evaluate the facility and site characteristics needed to determine whether sabotage could lead to URCs.
    - Conservative analysis for each inventory. 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.
- Identify any initiating events of malicious origin (IEMOs)[2] that can lead indirectly to URCs.
- Identify any IEMOs that exceed the capacity of mitigation systems. Include each such IEMO as an event leading to URCs in the sabotage logic model.
- Identify systems to mitigate each IEMO. For each IEMO that does not exceed mitigating system capacity, identify the safety functions necessary to mitigate the IEMO, the systems that perform the safety functions, and the success criteria for the systems.
- Develop a sabotage logic model. Develop model that identifies the combinations of events (direct dispersal, IEMOs that exceed mitigating system capacity, and IEMOs coupled with mitigating system disablement) that would lead to URCs.
- Eliminate from the sabotage logic model any events that the assumed threat does not have the capability to perform.
- 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.
- Solve the sabotage area logic model to identify the combinations of locations that must be protected to ensure that URCs cannot occur.
- Select the vital area set that will be protected to prevent sabotage leading to URCs.

Facility safety analyses can provide valuable information and models to support VAI. If a deterministic safety assessment (DSA) or a probabilistic safety assessment (PSA) has been completed for the facility, it will provide analyses of response of the facility to various initiating events (IEs) that could be caused by random failure, human error, etc. These events could also be caused by malicious acts. DSAs and PSAs provide extensive information on site and facility characterization that will be useful to the VAI team. Information on DSA and PSA can be found in Ref. [3]. Either type of analysis will contain information

that can be used to construct the logic models needed for VAI. Ref. [4] provides a discussion of how DSA and PSA results can be used to construct sabotage fault trees for a facility. A PSA will contain detailed logic models that can be used, directly or with some modification, in the VAI process. Ref. [5] describes a particular analysis tool that uses PSA information to identify vital areas in a nuclear power plant.

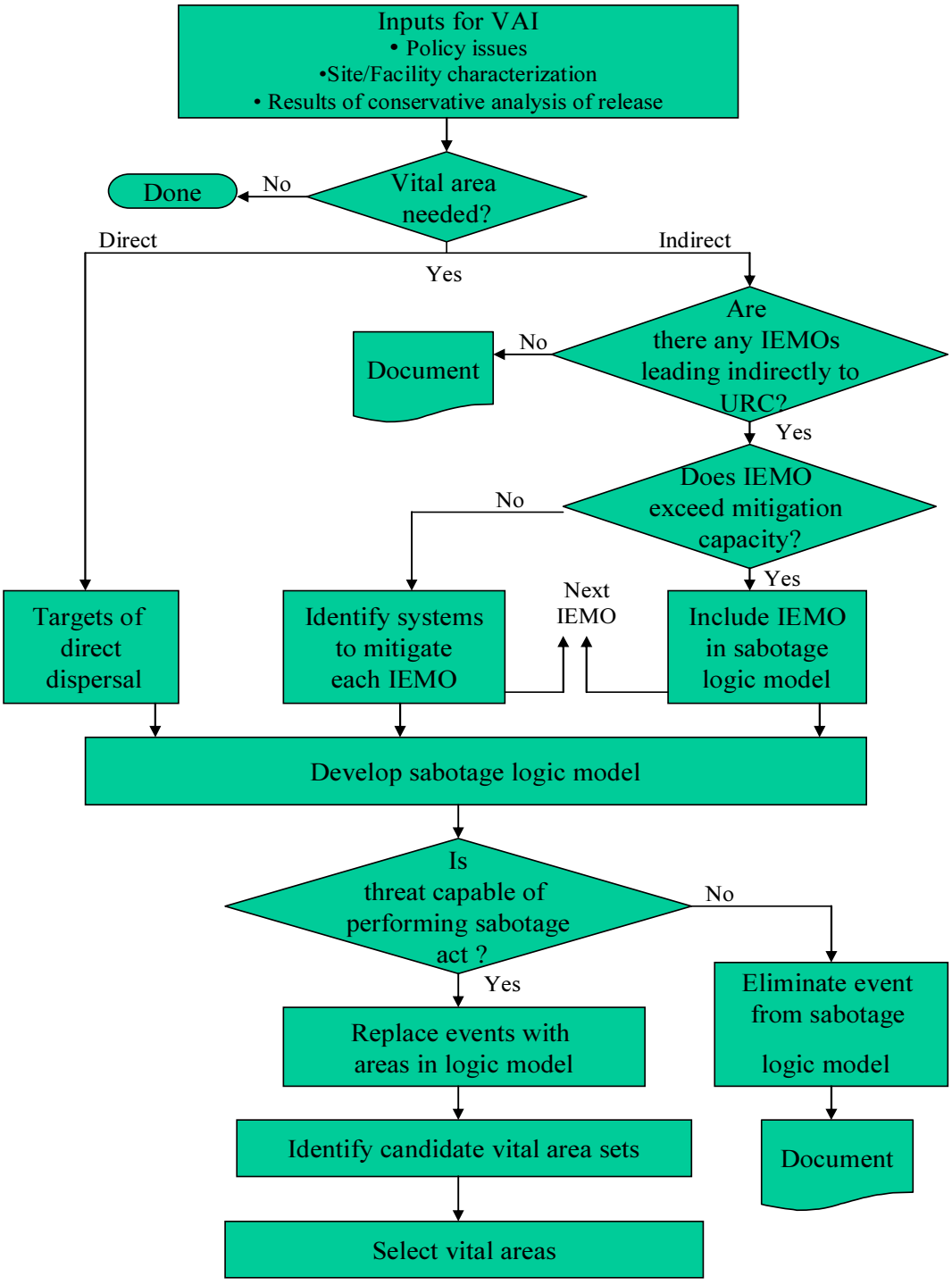

Fig. 2-1. VAI process

2.2. INPUT TO VAI PROCESS

2.2.1. Policy considerations

The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection [6]. This framework should provide for the establishment of applicable requirements for protection against sabotage. The State should define the division of responsibilities between the licensee/operator and the State. The State should ensure that the prime responsibility for the implementation of protection against sabotage of nuclear material or of nuclear facilities rests with the licensee/operator. The State (competent authority) should specify what level of protection against sabotage is appropriate.

Nuclear facility operators, vendors or designers should establish a set of vital areas around which protection will be applied to prevent malicious acts leading to URCs. Policy considerations to be addressed prior to initiation of the VAI process are:

- the explicit definition of unacceptable radiological consequences that will require vital areas;
- the operational states for which vital areas must be identified and protected;
- the safe facility state that should be achieved following a sabotage attack for each operational state;
- whether equipment unavailability events other than malicious disablement acts must be considered to occur concurrent with a sabotage attack;
- whether the analysis can take credit for accident management recovery actions following a sabotage attack;
- the threat against which the facility should be protected.

More detailed consideration will be given to each of these issues in the following sections.

2.2.1.1. Unacceptable radiological consequences

The first significant policy consideration is the explicit definition of *unacceptable radiological consequences* for which vital areas would be required as discussed in Section 7.1.5 of Ref. [1]. URC means that a consequence induced by a release of radioactive material or direct exposure to radiation is severe enough to warrant expenditure of resources to specifically prevent its occurrence. Typically, these consequences would be defined in terms of exposure dose or an unacceptable plant state, such as core damage for an NPP. A discussion on unacceptable radiological consequences and a consequence categorization table for sabotage can be found in Section 5 of Ref. [7].

2.2.1.2. Determination of operational states to be assessed

Some facilities may have more than one operational state, such as normal operation, plant shutdown, and reactor refueling for power reactors. These different operational states may rely on different equipment to perform necessary safety functions and may require different physical protection measures to protect the equipment and material. The competent authority should identify or approve the operational states to be considered in the VAI process. The identification of vital areas for all operational states can be accomplished by analysing each operational state, or by identifying a bounding operational state that will ensure protection during all states. Operational states to be assessed should be determined considering the possibility of URCs during each operational state.

2.2.1.3. Safe facility state

There may be a number of facility states that, if achieved subsequent to an accident or transient, are designed to maintain the facility in a safe state. In principle, all nuclear facilities must maintain the fundamental safety functions [8] of:

- control of reactivity
- cooling of radioactive material
- confinement of radioactive material.

For nuclear power reactors, the safety function of cooling of radioactive material is often further itemized as reactor coolant pressure control, reactor coolant inventory control, and decay heat removal.

Any facility state accepted for this purpose should be one where the necessary safety functions can be accomplished for a reasonable period, either by the safety equipment designed to perform those functions, or by alternative arrangements such as emergency preparedness and response. The defined facility safe state(s) may differ for analysis of different facility operational states. The competent authority should identify or approve the safe facility state for each facility operational state.

2.2.1.4. Equipment unavailability

Although VAI focuses on the consequences of malicious acts, equipment unavailability could conceivably occur, by chance or as a result of maintenance outages, concurrent with a malicious act. The results of the VAI need to be deterministic; that is, an area is either vital or it is not. Therefore, the assumptions that establish the requirements for the VAI should specify whether the analysis must include concurrent equipment unavailability due to random failure or maintenance[2].

2.2.1.5. Credit for recovery actions

Safety and other analyses used as input for VAI frequently contain explicit or implicit assumptions about personnel actions. These actions may involve routine or emergency operator actions needed to maintain the facility in a safe state. They may also be implicit in the way that the facility response to events is modelled. The VAI team should be careful to identify all implicit and explicit assumptions about personnel actions included in the safety and other analyses used as input to the VAI. After these actions have been identified, the team should determine whether credit can be taken for such actions as part of the facility response to sabotage. During the course of the VAI, the team may also identify possible recovery actions to compensate for disabled equipment. In this case too, the VAI team should determine whether credit should be taken for the recovery actions as part of the facility response to sabotage. The VAI team should document the rationale for crediting personnel actions, including recovery actions.

2.2.1.6. Threat characteristics

Physical protection of nuclear facilities should be based on the State's current evaluation of the threat [6]. The competent authority should specify the threat characteristics against which the operator should provide protection in a design basis threat or other threat evaluation. The threat characteristics are used in the VAI process to determine the malicious acts the threat is capable of performing.

2.2.2. Site and facility characteristics

The first step in performing sabotage analysis is to determine the inventories of nuclear or radioactive material present and the facility and site characteristics that will be needed to determine whether sabotage could lead to URCs. This requires information on:

[2] In order to ensure that a facility is adequately protected when maintenance is being performed in a vital area, the competent authority may require the operator to designate and protect temporary vital areas or take other compensatory measures.

- the site (area in which the facility is located).
  - Information on the population density in the vicinity of the facility and other site characteristics may be needed to determine the potential consequences of radiological releases if the criteria for URCs is directly related to off-site exposure rather than a surrogates, such as core damage or containment failure.
- the facility.
  - Information is needed on the locations of nuclear and radioactive material; inventory forms, characteristics, and quantities;
  - Information on the nuclear facility's critical safety functions (e.g. shielding, criticality prevention, cooling, confinement, fire prevention, structural integrity); and the process and safety system details in order to determine the equipment, systems, and devices that must be protected in order to prevent URCs.

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

2.2.3. 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 limits. A more realistic assessment is made later in the sabotage analysis process to determine whether a release that exceeds URC limits is credible for those inventories whose unmitigated release could produce URCs.

If the potential radiological consequences estimated for an inventory under these conservative analysis conditions are below the level of URCs, sabotage leading to URCs is not possible for this inventory[3]. Consequently, it is not necessary to designate any vital areas associated with this inventory. Such inventories may be protected in accordance with prudent management practice.

2.3. DIRECT SABOTAGE OF INVENTORY

If the potential radiological consequences of the release of a complete inventory are equal to or greater than a URC limit necessitating protection in a vital area, the possibility of sabotage that could lead directly to URCs and that might require that vital areas be defined, must be considered. Acts that lead directly to release of radioactive material are ones that apply energy from an external source (for example, an explosive or incendiary device) to disperse the material.

Consequently, the direct dispersal of the inventory should be included in the sabotage logic model as a potential malicious act leading directly to URCs necessitating protection in vital areas, and the remaining steps of the vital area identification 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.

[3] There may be circumstances where an adversary could, through criticality, increase the radionuclide inventory. Therefore, an inventory for which potential consequences did not initially exceed the URC might, through malicious action, do so.

2.4. INDIRECT DISPERSAL OF INVENTORY

If the potential radiological consequences of the release of a complete inventory are equal to or greater than a URC limit, the possibility of sabotage that could lead indirectly to URCs that might necessitate identification of vital areas must be considered. Malicious acts that lead indirectly to release are ones that use the potential energy (i.e. heat or pressure) stored in the radioactive material or in a process system to disperse the material. Indirect sabotage attacks do not require that the adversary gain access to the area in which the material is located; instead, they involve attacks against equipment, systems, or devices that normally maintain the facility in a safe state. To determine the areas that must be protected to prevent acts that lead indirectly to URCs, two types of sabotage attacks must be considered, namely those:

- causing an initiating event (IE) [2] that creates conditions more severe than the facility mitigating systems can accommodate (that is, events that are beyond the safety design basis);
- causing an IE and disabling 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 initiating event of malicious origin (IEMO).

2.4.1. Initiating events of malicious origin

The main purpose of this step in the VAI process is to produce a list of malicious acts by which the potential adversary might initiate a chain of events leading to URCs. Many IEs will have already been identified and analysed in facility safety documentation, such as a DSA or PSA report [3]. When identifying the IEMOs, the VAI team should consider three categories of events that may not be included in the safety case and that must be included in the VAI process.

1. The first category of IEMOs not included in safety assessments involves situations where there is no process energy or other energy sources present that could disperse radioactive material. For example, malicious acts involving explosives or other sources of energy for breaching or dispersal could cause barriers to fail or radioactive material to be dispersed in a manner not possible without a malicious act. Because these IEs are not possible without a malicious act, they are not usually addressed in the safety analysis.
2. The second, related, category of IEMOs that may not have been addressed in the safety analysis includes those IEs that are so unlikely to occur randomly that they are excluded from consideration. For example, multiple independent IEMOs or massive breaches or failures of passive components that, while extremely improbable as random events, can be accomplished by the potential adversary equipped with explosives or other resources, including in situ resources.
3. The third category of IEMOs involves sources of radioactive material releases that may not have been within the scope of safety documents. For example, Level 1 PSAs at nuclear power reactors address only events with the potential to lead to core damage and, thereby, the release of radioactive material from the reactor core. Other inventories of radioactive material that might be the source of release leading to URCs (such as irradiated fuel and radioactive waste) also need to be considered in the VAI process.

There are four approaches that can be used to identify the IEMOs to be addressed in the VAI process. Because the objective is to produce a list of IEMOs that is as complete as possible, the VAI team should use as many of these approaches as possible.

1. Review of safety documentation. This should be the starting point for this part of the VAI process. Lists of IEs in DSAs and PSAs, in fire analyses, seismic analyses, and other safety evaluations for the facility being analysed and for similar facilities should be reviewed. Because any of the IEs that can occur randomly can also be caused by malicious acts, this set of IEs should

be included in the list of IEMOs. Note that the assumptions in safety analyses regarding the nature of these IEs and the plant response to them should be reexamined in the context of malicious acts and revised where appropriate.

2. Reference to other VAIs. Where other VAI analyses have been performed for similar facilities, lists of the IEMOs used should be reviewed. It is particularly important to identify IEMOs that do not correspond to IEs in facility safety documentation.
3. Engineering evaluation. The facility systems (operational and safety) and major components should be systematically reviewed to identify any additional IEMOs, for example where any consequences of malicious acts of which the potential adversary is deemed capable (e.g., disabling, causing to operate spuriously, breaching, disrupting, collapsing, or igniting) could lead directly, or in combination with other malicious acts, to URCs.
4. Deductive analysis. In this approach, 'unacceptable radiological consequences' are systematically decomposed into all possible events that could cause it to occur. Successful operation of systems and other preventive actions are not included. The events at the most fundamental level are then candidates for the list of IEMOs for the facility.

Each IEMO should be assessed to determine whether there are systems capable of mitigating it. The IEMOs, either alone or in combination with mitigating system failures, are included in the sabotage logic model as indicated below.

2.4.2. IEMOs that exceed mitigating system capacity

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

2.4.3. IEMOs that are within mitigating system capacity

In order to address IEMOs that are within mitigating system capacity, the combinations of IEMOs and mitigating system disablement events that could lead to URCs must be determined. These combinations of events that lead indirectly to URCs are detailed in the sabotage logic model. The feasibility that the threat 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 ones that support safety functions such as reactivity control, decay heat removal, coolant boundary integrity, and containment integrity. The concept of safety functions is discussed in Refs. [2] and [9]. The systems that directly perform critical safety functions are defined to be front line systems and those required for proper functioning of the front line systems are defined to be support systems [9]. 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 [5]. If only a DSA is available, then the VAI team can usually derive most or all of this information from the accident analyses employing engineering judgment. If the DSA lists safety groups, these lists can be helpful in identifying front line systems and their dependencies. There may be other dependencies, beyond the safety analysis, that relate to specific malicious acts or sabotage scenarios. For example, explosive breaching of a cooling water pipe may cause flooding that disables equipment near the pipe breach. Such spatial interactions should be analysed in the VAI process (Section 2.7.3).

Successful operation of a front line system (success criteria) means 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 also hardware requirements, such as the number of required flow paths, power trains, etc.

Defining success criteria for support systems may be more complicated. In most cases support systems serve more than one front line system, and consequently each possible state of the system (e.g. three trains operating, two trains operating, one train operating, no train operating) has a different effect on the front line systems that perform a certain safety function. Thus, the success criteria for a support system vary with different safety functions and associated front line systems.

Some facilities may have large numbers of IEMOs that can lead indirectly to URCs. For such facilities it may be desirable to group together any IEMOs that have the same mitigating system performance requirements. Grouping IEMOs in this way will reduce the logic model development effort that follows. All IEMOs in a group require that front line systems and support systems meet essentially the same success criteria to prevent URCs. Thus, the same logic can model sabotage scenarios beginning with any of the IEMOs in a group. Facilities that have only a small number of IEMOs may not require IEMO grouping.

If a PSA has been performed for the facility, the PSA documentation should contain the grouping of IEs considered in the PSA; the same groupings can be employed for the corresponding IEMOs. Relatively few IEMOs do not correspond to IEs addressed in PSAs, and those generally must be categorized in separate groups. If a PSA has not been performed for the facility, it may be possible to begin with groupings of IEs from other safety documentation or another source. However, IEMO groupings depend upon the design of the facility, so groupings taken from other sources must be carefully evaluated to ascertain whether they are appropriate for the facility being analysed.

The steps discussed in Section 2.6 generate:

- a list of IEMOs that exceed the mitigation capacity of facility systems;
- a list of IEMOs that can be mitigated and the front line systems and support systems needed to respond to each one;
- front line and support system success criteria for each IEMO that can be mitigated;
- references to supporting documentation;
- grouping of IEMOs (if needed).

2.5. 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 URCs necessitating protection in vital areas, including the direct dispersal of radioactive material, IEMOs that exceed mitigating system capacity, and the combinations of events that will lead to URCs for IEMOs that are within mitigating system capacity. A logic model can be a statement; an algebraic expression; or a graphical representation, such as a fault tree or an event tree. The solution of different representations for the same logical problem will give the same results. The sabotage logic model includes all direct dispersal events and all IEMOs and associated mitigating system failures that will cause URCs.

Direct dispersal and IEMOs that exceed mitigating system capacity are included in the logic model as single events leading to URCs. 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.

Information provided in the facility safety analyses and other safety documentation can be used to develop the sabotage logic model for IEMOs within mitigating system capacity. Typically, this is 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 URCs. This is accomplished using information gathered in Sections 2.4.1, 2.4.2, and 2.4.3 and information from the facility safety analysis. The second stage is developing sabotage logic models for individual front line systems and the support systems they are dependent upon. This activity is performed 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 portion of the facility sabotage logic model that links each IEMO with the disablement of the front line systems and corresponding support systems that are required to mitigate the IEMO.

The sabotage logic model will have the direct dispersal events, the IEMOs, and the events that disable mitigating system components as basic events. A simple example of a sabotage logic model is provided in the Appendix.

2.6. 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. All events that could lead directly or indirectly to URCs are included to ensure that no potential vital areas are overlooked without regard to whether the assumed threat capabilities are sufficient to perform the sabotage acts. If the assumed threat characteristics change, the information and models developed in the preceding steps will be valid for use in identifying vital areas under the changed threat conditions[4].

In this step of the process, any events that are not credible given the assumed threat capabilities should be eliminated from consideration. A more realistic analysis of the potential consequences of threat actions than the conservative analysis recommended in Section 2.2.3 may be performed at this point in the process. The threat capability to perform the direct dispersal of material (Section 2.3), to cause an IEMO (Section 2.4.1), and to disable mitigating systems (Section 2.4.3) should be assessed. Events that are beyond the capability of the threat may be removed from the sabotage logic model.

In addition, any events that are beyond the ability of the facility physical protection system to prevent should be identified. In the analysis of the sabotage logic model, any such events will be assumed to occur always. Generally, any events that the threat can accomplish without gaining access to the site should be assumed to occur. For example, it is practically impossible for the facility physical protection system to prevent the loss of offsite power; 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 in Section 2.7.

[4] The competent authority may require that the VAI steps described in Sections 2.7 and 2.8 be completed before assessing the threat capability to perform the events in the sabotage logic model. Such an approach, while requiring additional analytical effort, will identify all potential vital area sets without regard to threat characteristics.

2.7. 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 walkdown of the facility. Spatial interactions among the adjacent areas should also be considered as discussed below.

2.7.1. Data collection and entry

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 in the nuclear facility from which it can be caused. The result is a sabotage area logic model. The sabotage area logic model can then be solved as described in the following section to determine the combinations of areas from which malicious acts could cause URCs and the minimum combinations of areas that should be protected to prevent URCs.

Design documents for the nuclear facility provide the information needed to identify the areas in which the sabotage events can be accomplished. General arrangement drawings should provide area, room, walls and doors and access route information. Piping and instrumentation diagrams, isometric drawings, safe shutdown analyses, and fire and seismic PSAs are other sources of information on equipment locations. Because any area included in the logic model may be selected as a vital area, it must be practical to provide protection around each of them. Therefore, it must be feasible to employ existing structures or new construction to establish a physical barrier around each defined area. It must also be feasible to control access to each area, to minimize the number of entrances to and exits from it, and to appropriately alarm and secure all points of access to the area.

Areas should be documented by marking them on facility arrangement drawings or other facility design and layout documents to clearly define the area boundaries. Area information is entered into the sabotage logic model by replacing the events in the model with the areas within which each event can be performed. Depending upon approach, this may be accomplished automatically by some type of linking table (‘location map’) or manually by modifying the sabotage logic model directly so that all variables are areas. The result of this task is a sabotage area logic model.

2.7.2. Walkdown

Area information should be verified by conducting a VAI walkdown. In preparation for the VAI walkdown, the team should review the location information[5]. The VAI walkdown team should include representatives from the facility safety, security, design and operating organizations.
The main objectives of the VAI walkdown are to:

- verify the areas from which the threat could accomplish direct dispersal.
- verify the set of areas from which the threat could accomplish each IEMO identified in Section 2.4.
- verify the set of areas from which the threat could accomplish each of the actions to disable equipment, components, or devices that are identified in the sabotage logic model.
- assess the potential for spatial interactions between adjacent areas.

2.7.3. Spatial interactions

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

[5] For new designs, an analysis of the vital areas should be made prior to construction. The walkdown is conducted prior to turnover of the facility to the operator to confirm the analysis.

adjacent areas. External event PSAs such as seismic, fire and flooding PSAs and Ref. [10] provide useful information on spatial interactions.

2.8. CANDIDATE VITAL AREA SETS

Identifying candidate sets of vital areas is accomplished in two steps:

1. The sabotage area logic model is analysed to determine all combinations of areas to which an adversary would have to gain access in order to complete sabotage scenarios that could lead to URCs. Each such combination of areas is a minimal cut set of the sabotage area logic model. The combinations of areas from which malicious acts could cause URCs can be useful in configuring and evaluating the facility physical protection programme. These combinations of areas can be reviewed to identify potential adversary targets as a basis for development of sabotage scenarios for physical protection system design and evaluation.
2. The sabotage area logic model is analysed to determine the minimum combinations of areas that must be protected in order to ensure that no sabotage scenarios 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 minimum complement of equipment, systems, or devices that, 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 sabotage scenarios that could lead indirectly to URCs[6].

The process of solving the sabotage area logic model to identify candidate vital area sets is illustrated in the Appendix.

2.9. VITAL AREA SET SELECTION

This step in the VAI process is to select a vital area set from the candidate vital area sets identified in Section 2.8. This VAI guidance document provides recommendations for the selection process, but does not prescribe specific methods to be used.

Each of the candidate vital area sets meets the recommendation in Section 7.1.5 of Ref. [1] for a set of facility vital areas. The facility operator may choose to protect any one of the candidate vital area 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 vital area set that provides the optimum combination of:

- low impacts on safety, plant operations, and emergency response;
- low difficulty of providing protection;
- high effectiveness of protection measures; and
- low cost of protecting the vital areas.

It is unlikely that one candidate vital area set will receive the highest rating for each the selection criteria. Thus, it will be necessary to effect trade-offs between the ratings in the various areas and select the

[6] Level 2 prevention sets (prevention sets that contain at least two areas from each of the minimal cut sets) could be used to identify candidate vital area sets for higher assurance of protection or defense in depth. Sabotage area logic models that contain single areas from which an adversary could cause URC will not have any level two or higher prevention sets.

candidate vital area set that is the overall best choice. This can be done using engineering judgment, or a more structured analytical approach (such as the analytic hierarchy process) can be employed. Refs. [12] and [13] provide examples of structured trade-off analysis methods.

The results of vital area selection process are:
1. A table that evaluates each of the candidate vital area sets in terms of each of the attributes considered in the selection of a vital area set and documents the aggregate score or ranking with associated rationale for each candidate vital area set.
2. A recommended vital area set with the best overall score or ranking.

The vital area set that should be protected to prevent sabotage will include:

- all areas from which the assumed threat has the capability to cause direct dispersal of radioactive material that exceeds the URC criteria,
- all areas from which an adversary could cause IEs that exceed the mitigation capability of facility systems, and
- either all areas from which an adversary could initiate events that safety systems can mitigate or areas in which minimum sets of equipment needed to mitigate the IEs are located.

3. DOCUMENTATION OF RESULTS

3.1. OBJECTIVES AND PRINCIPLES OF DOCUMENTATION

The objective of the analysis documentation is to demonstrate that the VAI satisfies the requirements of the competent authority. The documentation should be well structured, concise and easy to review and update. Updates may be required to reflect changes in the assumed adversary characteristics as well as modifications to the facility operation, safety systems and measures, and the locations of facility components, equipment, or devices. The documentation should explicitly present the assumptions made in the policy considerations topics discussed in Section 2.2.1 and comply with quality assurance requirements of the competent authority.

3.2. ORGANIZING DOCUMENTATION

The organization of the documentation should be governed by two general principles:

1. Traceability: for review and updating the analysis, it should be possible to trace any information with minimum effort.

2. Sequentiality: the order of appearance of the analysis in the report should follow the order in which the analysis was performed, namely:
   - input
     - basic assumptions used in the process
     - conservative analysis results
   - potential direct dispersal events
   - identification of IEMOs
   - identification of safety systems that mitigate IEMOs
   - logic model development
   - threat capability assessment
   - sabotage event area identification
   - identification of candidate vital area sets
   - selection of a set of vital areas.

3.3. PROTECTING INFORMATION

The VAI process generates sensitive information that should be protected properly according to information security requirements of the competent authority. The information security requirements and procedures will depend upon the legal system in the state where the facility is located. Everyone who has access to the information generated in the VAI process should be required to understand and follow the information security requirements.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev. 4 (corrected), IAEA, Vienna (1999).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, NS-R-1, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[4] SANDIA NATIONAL LABORATORIES, A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities, SAND2004-2866, SNL, Albuquerque, NM (2005).

[5] KOREA ATOMIC ENERGY RESEARCH INSTITUTE, The Application of PSA Techniques to the Vital Area Identification of Nuclear Power Plants, KAERI (2004).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Amendment to the Convention on the Physical Protection of Nuclear Material, International Law Series No. 2, Vienna (2006).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Facilities and Nuclear Material against Sabotage, Nuclear Security Series (pending), Vienna (2007)

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Version 2.0, IAEA, Vienna (2006).

[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, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Nuclear Security Series No.4, 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] THOMAS L. SAATY, *Decision Making for Leaders*, Vol. II, AHP Series, RWS Publications, Pittsburg, PA (2002)

APPENDIX: EXAMPLE SABOTAGE LOGIC MODEL

This appendix provides a step-by-step solution of a simple logic model to illustrate how candidate vital area sets can be identified. The solution of the example logic model demonstrates how the concepts of minimum cut sets and minimum protection sets are applied in the VAI process.

A logic model can be a statement, an algebraic expression or a graphical representation such as a fault tree or an event tree. The solution of different representations for the same logical problem will give the same results. A logic model is 'solved' by applying the rules of Boolean algebra to the model. Table A-1 provides definitions of common logic symbols and Boolean algebra rules.

Consider a fictitious facility that has the following characteristics:

1. There are two initiating events (IEs) identified for this facility, IE1 and IE2, that if unmitigated will result in releases that exceed the URC limits established by the competent authority.
2. Safety system S1 is designed to mitigate IE1 and system S2 is designed to mitigate IE2.
3. System S1 has two trains of equipment, T1 and T2. If either of these trains functions properly, S1 can successfully mitigate IE1 (that is, both trains must fail for S1 to fail).
4. System S2 has three trains, T3, T4, and T5. Either T3 or both T4 and T5 must function in order for S2 to successfully mitigate IE2 (that is, S2 will fail to mitigate IE2 if either T3 and T4 fail or T3 and T5 fail).
5. The trains in the systems have components (designated by C below) that must operate for the trains to function.
   - T1 fails if either of two components (C1 or C2) fails.
   - T2 fails if either C3 or C4 fails.
   - T3 fails if either C5 or C6 fails.
   - T4 fails if either C7 or C8 fails.
   - T5 fails if either C9 or C10 fails.
6. In order to cause the IEs and disable the various components a saboteur would have to gain access to different plant areas, designated with L labels below.

Event	Location
Disable C1	L1
Disable C2	L2
Disable C3	L2
Disable C4	L2
Disable C5	L3
Disable C6	L3
Disable C7	L5
Disable C8	L6
Disable C9	L6
Disable C10	L6
Cause IE1	L8
Cause IE2	L9

The statements above constitute one form of a logic model for sabotage of the facility. By carefully analysing these statements, we could determine the combinations of locations that a saboteur would have to enter to cause all the IEs and component failures that would lead to URCs. For example, if a saboteur

could gain access to L2 and L8 he could initiate IE1 and disable S1, resulting in a release that exceeds URC limits. The saboteur can cause IE1 if he gains access to L8. If the saboteur disables both T1 and T2, S1 will not be able to mitigate IE1. T1 can be disabled by disabling C2 and T2 can be disabled by disabling C3. Both C2 and C3 can be disabled from L2, so by gaining access to both L2 and L8 the saboteur can cause URCs. By reviewing the statements and location table in detail, all the combinations of locations from which IEs can occur sufficient to cause URCs could be identified.

As long as the facility is simple enough, it is possible to derive the location combinations from which sabotage can be accomplished by inspection as done in the previous paragraph. A more useful approach is to represent the relationships between IEs, disablement events and locations in a logic equation. The event to be represented in this logic equation is release in excess of URCs. Using the definitions in Table A-1, the following equations are developed corresponding to statements 1 through 5 above:

$$URC = IE1*S1 + IE2*S2 \quad (1)$$
$$S1 = T1*T2 \quad (2)$$
$$S2 = T3*T4 + T3*T5 \quad (3)$$
$$T1 = C1 + C2 \quad (4)$$
$$T2 = C3 + C4 \quad (5)$$
$$T3 = C5 + C6 \quad (6)$$
$$T4 = C7 + C8 \quad (7)$$
$$T5 = C9 + C10 \quad (8)$$

In these equations, S1 means safety system 1 is disabled, T1 means train 1 is disabled, C1 means component 1 is disabled, etc. Replacing the events in these equations with the locations in which they can be caused and simplifying using the rules of Boolean algebra yields the following results:

$$T1 = L1 + L2 \quad (9)$$
$$T2 = L2 + L2 = L2 \quad (10)$$
$$T3 = L3 + L3 = L3 \quad (11)$$
$$T4 = L5 + L6 \quad (12)$$
$$T5 = L6 + L6 = L6 \quad (13)$$
$$S1 = (L1 + L2)*L2 = L2 \quad (14)$$
$$S2 = L3*(L5 + L6) + L3*L6 = L3*L5 + L3*L6 \quad (15)$$
$$URC = L8*L2 + L9*(L3*L5 + L3*L6) = (L8*L2) + (L9* L3*L5) + (L9*L3*L6) \quad (16)$$

For this simple example, there are three combinations of locations from which a saboteur could cause URCs:

$$URC = L8*L2 + L9* L3*L5 + L9*L3*L6 \quad (17)$$

Each combination of locations from which sabotage can be caused is called a cut set of the sabotage location equation. The objective of VAI is to find a minimum set of areas to be protected against sabotage to prevent all possible scenarios leading to URCs. This means that we must protect at least one of the areas in each combination of areas from which sabotage can be accomplished. Each combination of locations whose protection will prevent all sabotage scenarios is a prevention set for the logic model and constitutes a candidate vital area set. For simple sabotage location equations it is possible to directly determine the combinations of locations whose protection will prevent sabotage. From equation 17, it can be seen that if the adversary is prevented from gaining access to the following combinations of areas, URCs cannot occur.

$$\text{URC Prevented} = \underline{L8}*\underline{L9} + \underline{L8}*\underline{L3} + \underline{L2}*\underline{L9} + \underline{L2}*\underline{L3} + \underline{L8}*\underline{L5}*\underline{L6} + \underline{L2}*\underline{L5}*\underline{L6} \quad (18)$$

In equation 18, the underline indicates that access to the location is prevented; for example, L8 means access to L8 is prevented. In Boolean algebra terms, L8 is the complement (non-occurrence or NOT) of L8. For the example facility, there are six candidate vital area sets as shown in equation 18. This result can also be derived algebraically by forming the complement of the sabotage location equation and simplifying using the rules of Boolean algebra. The protection of any one of the candidate vital area sets will ensure that a saboteur cannot cause URCs. If, for example, we select the set L2 and L3 as the final vital area set, these are the only two areas of the plant that would be protected as vital areas. Protecting these two areas will ensure that none of the possible sabotage scenarios can be completed.

Fault trees can be used to efficiently represent the sabotage logic for more complicated facilities. Figure A-1 provides a fault tree for the example facility that will be solved to further illustrate the process of identifying candidate vital area sets. The top event in this tree is release in excess of URC limits (represented by the symbol URC). The logic gates show the ways the events in the tree combine to cause the top event, and the tree is developed down to the level of component failures. Figure A-2 shows the fault tree with all terminal events replaced with the locations from which the events can be caused. This sabotage location fault tree is solved using the Boolean algebra concepts applied in equations (1) through (17) to produce the same results. The expression in parenthesis beside each gate is the solution for the gate in terms of the terminal events in the tree. One way to generate the level 1 protection sets for a fault tree is to form and solve the dual for the tree. The dual of a fault tree is formed by changing each OR gate in the tree to an AND gate, each AND gate to an OR gate, and each event to the complement (NOT) of the event. There are a variety of software packages available for solving fault trees and generating the prevention sets (candidate vital area sets) needed in the VAI process.

In summary, the sabotage logic model for a facility can be developed in a number of equivalent forms. The solution of the logic model produces candidate vital area sets that can be protected to prevent sabotage. Any one of the candidate sets will contain a minimum set of equipment needed to ensure that no sabotage scenarios can be completed.

Table A-1 Common Logic Model Representations

Logic Symbols		
Symbol	**Operation**	**Definition**
+	**OR**	Either of two events occurs. A+B means that either event A or event B occurs.
*	**AND**	Both of two events occur. A*B means that both event A and event B occur.
Logic Gates		
Symbol	**Gate Name**	**Definition**
	**OR Gate**	Output occurs if any of the inputs occur.
	**AND Gate**	Output occurs if all of the inputs occur.
Boolean Algebra Rules		
A+A=A	A+A*B=A	$\overline{(A+B)} = \overline{A} * \overline{B}$
A*A=A	A*(B+C)=A*B+A*C	$\overline{(A*B)} = \overline{A} + \overline{B}$

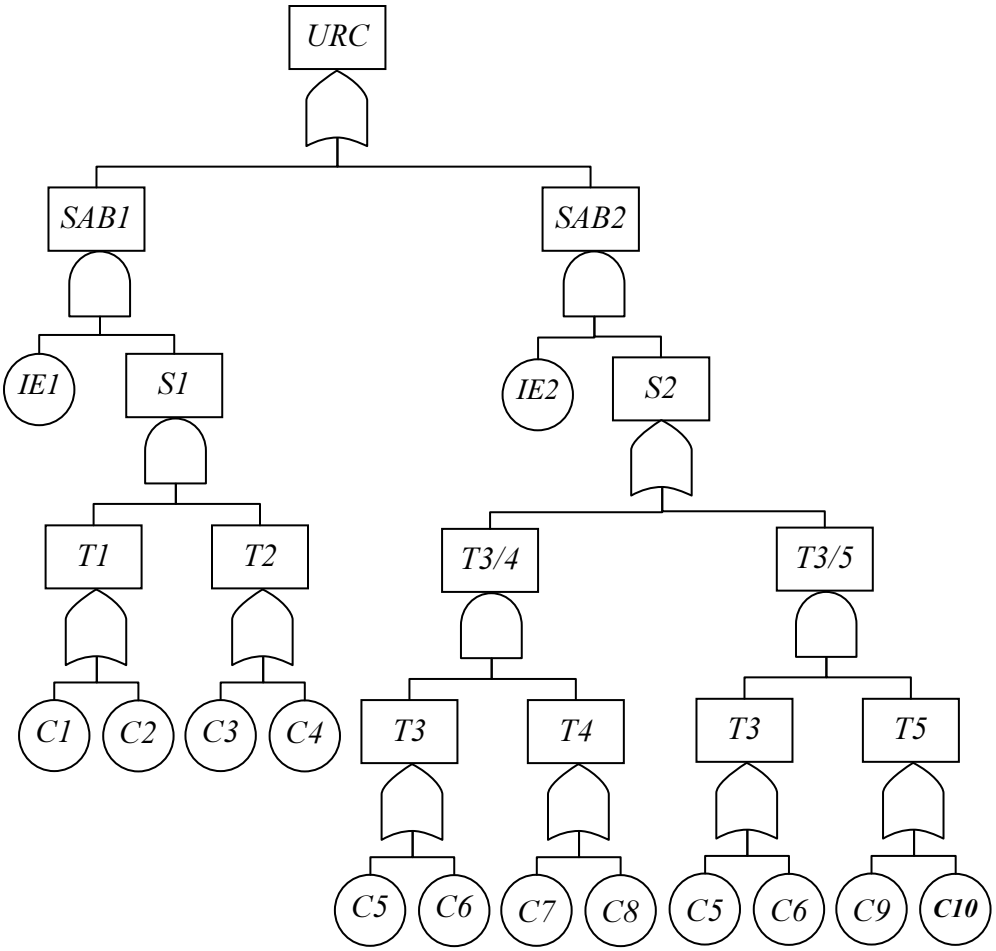

Figure A-1 Sabotage Fault Tree

DEFINITIONS

Candidate vital area set — A prevention set (complement cut set or minimal path set) for a sabotage area logic model that identifies a set of areas whose protection will prevent malicious acts leading to unacceptable radiological consequences. Sabotage cannot be accomplished unless the saboteur can enter at least one area in the prevention set.

Deterministic safety analysis (DSA) — A comprehensive, structured analysis that assesses the performance of the facility against a broad range of operating conditions, postulated initiating events, and other circumstances, demonstrating that normal operation can be carried out safely, in such a way that facility parameters do not exceed operating limits.

Front line system — A system that directly performs a facility safety function. See also the definition of support system (paragraph 3.7 of Ref. [9]).

Initiating event (IE) — An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. Referred to in Ref. [8] as a postulated IE.

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

Logic model — A statement, algebraic expression, or graphical representation that captures the combinations of item failures that lead to an undesired event or undesired system state.

Probabilistic safety assessment (PSA) —A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk [8].

Sabotage — 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 exposure to radiation or the release of radioactive substances (paragraph 2.12 of Ref. [1]).

Sabotage logic model — A logic model that documents the malicious events or combinations of malicious events that could lead to unacceptable radiological consequences. A sabotage area logic model identifies the physical areas from which the malicious events can be performed. The sabotage area logic model can be analysed to identify the combinations of areas from which sabotage resulting in unacceptable radiological consequences can be committed and also the areas that must be protected to prevent unacceptable radiological consequences.

Success criteria — The minimum system performance that will allow for performance of a system safety function under the specific conditions created by an initiating event (adapted from paragraph 3.8 of Ref. [9]).

Support system — A system required for the proper functioning of one or more front line system(s) (paragraph 3.7 of Ref. [9]).

Unacceptable radiological consequences (URCs) — One or more quantitative measures of dose, radioactive material release, or plant condition that have been established as thresholds (lower limits) and that, if equaled or exceeded, are deemed to represent a condition that would endanger the health and

safety of facility personnel, the public, or the environment to such a degree that a State would develop regulations that require resources be expended specifically for its prevention.

Vital area — An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequence. (paragraph 2.17 of Ref. [1]).

Vital area identification (VAI) — The process used to identify nuclear material, and the minimum set of structures, systems, or components to be protected against sabotage (adapted from paragraph 7.1.5 of Ref. [1]).