Sandia National Laboratories
Operated for the U.S. Department of Energy by
Sandia Corporation

John C. Matter
Manager
International Security Projects

P.O. Box 5800
Albuquerque, NM 87185-1361

Phone: (505) 845-8103
Fax: (505) 284-5437
Internet: jcmatte@sandia.gov

October 24, 2008

XE Corporation
Suite 307
4611 Greene Ave NW
Albuqueruqe, NM 87114 :

According to our records you were on the distribution list for the report "A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities," SAND2004-2866, published in May 2005. The copy of the report you received may have been marked incorrectly to indicate that it contained Official Use Only (OUO) information. We have confirmed that the report does not contain OUO information, and it has been approved for Unlimited Release. If you have any copies of the report that bear OUO markings, please remove, cover, or obliterate those markings. No restrictions on storage or distribution of the document are needed. Thank you for your assistance.

Best regards,

John C. Matter

SAND2004-2866
Official_Use_Only
Printed May 12, 2005

A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities

AUTHOR(S): JOHN HOCKERT, DAVID F. BECK

PREPARED BY
Sandia National Laboratories
Albuquerque, NM 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, A Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Abstract

Identifying the areas to be protected is an important part of the development of measures for physical protection against sabotage at complex nuclear facilities. In June 1999, the International Atomic Energy Agency published INFCIRC/225/Rev.4, "The Physical Protection of Nuclear Material and Nuclear Facilities." This guidance recommends that "Safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malevolent 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 report presents a structured, transparent approach for identifying the areas that contain this minimum complement of equipment, systems, and devices to be protected against sabotage that is applicable to complex nuclear facilities. The method builds upon safety analyses to develop sabotage fault trees that reflect sabotage scenarios that could cause unacceptable radiological consequences. The sabotage actions represented in the fault trees are linked to the areas from which they can be accomplished. The fault tree is then transformed (by negation) into its dual, the protection location tree, which reflects the sabotage actions that must be prevented in order to prevent unacceptable radiological consequences. The minimum path sets of this fault tree dual yield, through the area linkage, sets of areas, each of which contains nuclear material, or a minimum complement of equipment, systems or devices that, if protected, will prevent sabotage. This method also provides guidance for the selection of the minimum path set that permits optimization of the trade-offs among physical protection effectiveness, safety impact, cost and operational impact.

Acknowledgment

This report benefited greatly from two meetings with a panel of International Atomic Energy Agency (IAEA) technical experts in Vienna in August 2002 and January 2003 relating to a course on Vital Area Identification that Sandia National Laboratories is assisting the IAEA in developing. Of special note were the contributions of IAEA staff members Aybars Guerpina, Mark SooHoo, and Roger Barnes and the expert panel chairperson, David Foster. The peer review of this report performed by Iain J. McNair and his associate, G Grint**,** both of the Health & Safety Executive / HM Nuclear Installations Inspectorate (UK); Andrei Glukhov of the Pacific Northwest National Laboratory; David Foster of Utility Security Inc. (Canada); James J. Johnson of James J. Johnson and Associates; and Jeffrey LaChance and Timothy Wheeler, both of Sandia National Laboratories, was also extremely valuable in identifying areas where improvements in the approach and clarifications of the discussion were practicable and appropriate. Guidance from David Beck, David Ek, James Blankenship, and Linda Ehart, also of Sandia National Laboratories, led to the preparation of this report and was significant in shaping its focus. Joann Wylie, of XE Corporation, assisted with the review of various drafts pointing out errors and providing insightful comments. Juliana Newman and Barbara Haschke of Ktech also provided extremely valuable help in improving the clarity and layout of the report.

Contents

Figures

Tables

This page intentionally left blank.

Nomenclature

DSA	deterministic safety analysis
IAEA	International Atomic Energy Agency
IE	initiating event
LOCA	Loss of Coolant Accident
MAIE	malevolent act initiating event
PORV	power operated relief valve
PSA	probabilistic safety analysis
QA	quality assurance
VAI	vital area identification

1. Introduction

The need for physical protection of nuclear facilities has long been recognized. However, the events of September 11, 2001 have increased the urgency of ensuring that adequate protection is provided.

This report describes a systematic method to identify areas[1] containing nuclear material, or the minimum complement of equipment, systems, or devices to be protected against sabotage. Because these areas are referred to as vital areas, the process is referred to as vital area identification (VAI). VAI focuses on "what to protect," while physical protection system design addresses "how to protect." Further, VAI is an evaluation of what to protect without consideration of the threat's capability to overcome physical protection measures or the difficulty of providing physical protection.[2] VAI identifies areas, structures, systems, and components to be protected; the threat to these items and the ease or difficulty of protecting the items against a threat are considered after the areas and items to be protected are identified.

1.1 Objectives, Intended Audience, and Scope of This Report

In 1999, the International Atomic Energy Agency (IAEA) published physical protection recommendations for nuclear facilities in INFCIRC/225/Rev. 4, "The Physical Protection of Nuclear Materials and Facilities" (Reference 1). This INFCIRC states, in Paragraphs 7.1.1, 7.1.2, and 7.1.5:

> An act of sabotage[3] involving nuclear material or against a nuclear facility could create a radiological hazard to the personnel, and a potential radioactive release to the public and the environment. Radiological hazards are strongly dependent on the threat to be considered, on the type of nuclear material, on the inventory of nuclear material and associated fission products, on the design of the facility or package and on its safety features. Consequently, a plant-specific or package design evaluation of the potential for sabotage and associated radiological consequences should be made in close consultation between safety and physical protection specialists.
>
> The concept of physical protection to protect against sabotage requires a designed mixture of hardware (security devices), procedures (including the

[1] For this report, an area is defined to be a location that has four walls, a ceiling, and floor or any component, such as a motor control center or electrical rack, or location for which an enclosure or other means of providing penetration delay, access control, and intrusion detection could feasibly be constructed.

[2] Identification of potential adversary targets has traditionally considered the capability of the potential adversary to create adverse consequences if it gains access to the target. For example, Category I Special Nuclear Material (see INFCIRC/225/Rev. 4) is a theft target because the potential adversary is considered capable of fabricating a nuclear explosive device from Category I SNM. Natural uranium would not be considered a theft target if the potential adversary is not considered capable of enriching natural uranium or fabricating a plutonium production reactor/reprocessing complex to convert the material into a form that can be used in a nuclear explosive device. If the potential adversary has these capabilities then natural uranium would also be a theft target.

[3] Sabotage is defined to be 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. Terms in italics are defined in the glossary of this report.

organization of guards and the performance of their duties) and facility design (including layout). The level of the physical protection measures should be specifically designed to take into account the nuclear facility or nuclear material, the State's design basis threat[4] and the radiological consequences. Emergency procedures should be prepared to counter effectively the State's design basis threat.

Safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malevolent 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. Also measures that have been designed into the facility for safety purposes should be taken into account. When protecting against sabotage, nuclear material or equipment, systems, or devices, the sabotage of which, alone or in combination based on analysis, could lead to unacceptable radiological consequences,[5] should be located in a vital area(s).[6]

This report presents an approach that complex nuclear facilities can employ to identify vital areas in a manner that meets the recommendations of Section 7.1.5 of Reference 1. The VAI approach focuses on identifying all candidate sets of vital areas at a facility and providing process for the selection of a set of facility vital areas that is most effective in contributing to facility protection against sabotage during physical protection system design.

1.1.1 Objectives

The VAI method is intended to apply to complex nuclear facilities that have inventories of radioactive materials that could create a radiological hazard to the personnel, and a potential radioactive release to the public and the environment. A complex facility employs multiple redundant or diverse safety systems to control or mitigate radiological hazards. This method can also be employed in facilities where such multiple safety systems are not needed; however, for these facilities, vital areas may be identified by simpler, less costly methods than the one presented in this report. The examples given in this report are taken from nuclear power reactors, the most numerous members of the class of complex nuclear facilities with large inventories of radioactive materials. However, the VAI method presented here can be employed in other complex nuclear facilities, such as nuclear fuel reprocessing plants and high-level nuclear waste treatment facilities.

[4] The design basis threat is defined to be the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is evaluated.

[5] Unacceptable radiological consequences are defined to be a possible result of sabotage that is deemed, by the facility or competent authority, to be sufficiently serious that the facility for which VAI is being performed is required to employ special physical protection measures to protect against it.

[6] A vital area is defined to be 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.

1.1.2 Intended Audiences

This report has several intended audiences. The first is the competent authority[7] of a State that is developing requirements for VAI at nuclear facilities. This report identifies the policy issues that need to be addressed in developing VAI requirements. The second is facility managers, security specialists, and safety specialists responsible for planning, performing, and documenting VAI at complex nuclear facilities. This report provides detailed recommendations for planning and managing the conduct of VAI using the method described. The main emphasis is on the approach for performing VAI rather than the details of the underlying tools, such as fault tree analysis. Nevertheless, the report does address a third audience, the probabilistic safety analysts who support the VAI, by providing an appendix with detailed guidance and instructions for developing the fault tree model necessary to implement this method.

1.1.3 Scope

This report focuses solely on the performance and management of the VAI process to identify vital areas to provide protection against unacceptable radiological consequences. It does not address appropriate protection measures for vital areas or the design of physical protection systems. It is not concerned with those characteristics and attributes of the potential adversary[8] that relate to the ability to defeat physical protection measures. Although facilities and the competent authorities of States may wish to require or provide physical protection against other undesirable consequences, such as costly facility damage or facility outages, these issues are outside the scope of this report.

VAI focuses on determining the areas within the facility that require special physical protection because of the nuclear material or equipment, systems, or devices that they contain. Therefore, VAI does not focus on identifying large external events that could be caused by potential adversaries and that might cause unacceptable radiological consequences, such as aircraft crashes into nuclear facilities, although such events may be identified in the course of the VAI analysis. These postulated large external events do not affect the identification of vital areas because on-site physical protection cannot protect against such events. The comprehensive identification of such events and the development of appropriate protection measures, including possible facility design changes or additional protection measures outside the facility, should be the subject of a separate study.

VAI focuses on identifying vital areas at existing facilities, not on designing facilities for sabotage protection. However, the VAI method presented can provide valuable insights regarding equipment that needs to be protected against sabotage, physical separation of redundant or diverse safety systems, and types of accident management features to enhance

---

[7] The competent authority is defined to be the organization(s) empowered under the legislative authority of a State to establish and ensure the proper implementation of the State's system of physical protection. If the elements of the State's system of physical protection are divided between two or more authorities, competent authority in this document refers to that authority responsible for establishing and ensuring the proper implementation of the requirements for VAI.

[8] The potential adversary is defined to be an individual or a group, some of whom may have authorized access to the facility (i.e., insiders), who might attempt sabotage. The term also refers to the attributes and characteristics of such individuals that relate to the types of malevolent acts that they are capable of once they gain access to areas within the facility. Where a design basis threat has been established, these attributes and characteristics are often defined as a part of the design basis threat.

sabotage protection. Sabotage protection features and measures should be considered early in the design of complex nuclear facilities; review of the evolving design should consider the effect of design changes on sabotage protection. These considerations are broader and include analysis and design of physical protection features in addition to VAI.

Based upon the IAEA outline of the process, a VAI method must identify as vital all equipment that is sufficient to perform the fundamental safety functions identified for the facility, thereby protecting it against malevolent acts.[9] A VAI method must also identify those areas where a malevolent act that exceeds the design basis of the facility safety groups can be accomplished. This is simple in concept, but it can be difficult to accomplish, particularly for complex facilities. In such cases safety groups frequently consist of multiple, redundant equipment items and some equipment items may be part of more than one safety group, making it difficult to ensure that the complement of equipment, systems, or devices selected for protection is minimal, yet adequate to ensure that malevolent acts would not cause unacceptable radiological consequences. For safety and risk analysis purposes, such complex facilities and their equipment, systems, and devices are analyzed using fault trees.[10] This paper describes one VAI method, focused on complex nuclear facilities and employing fault tree analysis to address the complex interactions of facility equipment, systems, and devices.

1.2 Fundamental Concepts

Several concepts need to be understood when establishing requirements for VAI, when planning a VAI, and when performing a VAI. These include that key questions to be answered during the VAI, the meaning of terms used in VAI, and the basic approach to VAI. These fundamental concepts are presented in the following.

1.2.1 Key Questions

Key questions to be answered during a VAI include, but are not limited to:

- What is the specific meaning of unacceptable radiological consequences and what measure is to be employed to determine whether the consequences of acts by a potential adversary are unacceptable?

- What are the sources of radioactive material that can be released to cause unacceptable radiological consequences?

[9] See paragraph 4.6 of NS-R-1, “Safety of Nuclear Power Plants; Design” (Reference 2). For a nuclear reactor, the fundamental safety functions are: (1) control of reactivity; (2) removal of heat from the core; and (3) confinement of radioactive materials and control of operational discharges, as well as accidental releases. Safety functions for boiling water reactors, pressurized water reactors and pressure tube reactors are discussed in more detail in the annex to Reference 2. Fundamental safety functions can be established for other types of nuclear facilities in a similar manner.

[10] See Section 4.2.1 of 50-P-4, “Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)” (Reference 3) and Paragraph 4.154 of NS-G-1.2, “Safety Assessment and Verification for Nuclear Power Plants” (Reference 4).

- What malevolent acts (referred to as malevolent act initiating events [MAIEs]) can a potential adversary commit that might cause radioactive material to be released, causing unacceptable radiological consequences?

- What safety groups (combinations of safety systems) must a potential adversary disable concurrent with the MAIEs to cause unacceptable radiological consequences?

- What equipment must be disabled to disable the facility safety groups needed to respond to MAIEs?

- What plant areas must the potential adversary gain access to in order to perpetrate the MAIEs and disable equipment, shutting down the safety groups needed to respond to the MAIEs?

- What are the minimum sets of areas (referred to as candidate vital area sets) that, if protected, will prevent the potential adversary from carrying out any combination of MAIEs and disabling of safety groups that would cause unacceptable radiological consequences?

- How can the physical protection design process determine which of the candidate vital area sets is best to designate as the set of facility vital areas?

1.2.2 Definition of Vital Area Terms

A VAI analysis employs methods developed and traditionally employed for nuclear safety analysis and evaluation to support the design and implementation of facility physical protection measures. The disciplines of nuclear safety and physical protection employ different terminology. In some cases they employ similar terminology for related but different concepts. This section highlights the differences in terminology and introduces the definitions of important terms used in this report.

Sabotage

Sabotage is "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."[11] Vital areas are established to protect against a subset of the malevolent acts that are included in the definition of sabotage. These malevolent acts are those that can be protected against with on-site measures and that 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. To determine precisely the malevolent acts within this class, it is necessary to define clearly what it means to endanger the health and safety of personnel, the public and the environment. This is accomplished by establishing the specific meaning of unacceptable radiological consequences.

[11] Paragraph 2.12 of Reference 1.

Unacceptable Radiological Consequences

Unacceptable radiological consequences are a possible result of sabotage that is deemed to be sufficiently serious that special physical protection measures are required to protect against it. Unacceptable radiological consequences are the serious sabotage-related events that the physical protection program is specifically designed to provide protection against. The physical protection program will also provide protection against malevolent acts with lesser consequences. Reference 1 requires that vital areas be afforded a special higher level of protection (e.g., at least two physical barriers with access controls and intrusion detection and assessment).[12] The use of a systematic approach to VAI is intended to ensure that vital areas are selected in manner that ensures that malevolent acts that could result in unacceptable radiological consequences cannot be accomplished without overcoming this special higher level of protection. Section 2.1 discusses this further.

Malevolent Act Initiating Event (MAIE)

A malevolent act initiating event is a malevolent act by which the potential adversary might initiate a chain of events leading to unacceptable radiological consequences. These MAIE include the Initiating Events (IEs), events identified during design as capable of leading to anticipated operational occurrences or accident conditions, that are considered in facility safety analyses. However, they also include three additional classes of events not usually considered in safety analyses. The first such class includes events where there is no process or other energy normally present that could disperse radioactive materials. However, a potential adversary with explosives, incendiaries, or other energy could accomplish malevolent acts that dispersed the radioactive material. The second class of events includes those events so unlikely to occur randomly that they need not be considered in safety analyses. These might include the catastrophic failure of barriers confining or containing radioactive material. Although such catastrophic failures are extremely unlikely, they could be caused by a potential adversary with explosives. The third class includes sources of radioactive material that might not have been considered in the safety analysis. For example, a Level 1 Probabilistic Safety Analysis (PSA) for a nuclear power reactor only addresses events with the potential to cause damage to the reactor core. Therefore, it would not address events that could cause radioactive material releases from the spent fuel pool or radioactive waste storage and handling system. Initiating events in these three classes, in combination with the IEs considered in the facility safety analyses comprise the universe of MAIEs.

Potential Adversary Characteristics and Design Basis Threat

A potential adversary is an individual or a group who might attempt sabotage; some of them may have authorized access to the facility (i.e., insiders). Potential adversary characteristics are those attributes and characteristics of such individuals that relate to the types of malevolent acts that they are capable of once they gain access to areas within the facility. Characteristics of interest would typically include:

- Knowledge of the facility, of the location of safety system components, and of sabotage techniques; and

[12] Paragraphs 2.17, 7.2.3, 7.2.11, and 7.2.12 of Reference 1.

- Possession of quantities and types of explosive, incendiary, and sabotage devices and knowledge and training in their use.

However, potential adversary characteristics do not include those attributes of potential adversaries that relate to their ability to defeat physical protection measures. Therefore, potential adversary characteristics would typically not include:

- Armaments and weaponry;
- Tactical training and knowledge of facility guard and response force tactics;
- Facility access authorization.

Other attributes, such as the number of potential adversaries and types of vehicles that might be used by potential adversaries, would be considered part of the potential adversary characteristics only because of their indirect relationship to the quantities and types of explosives, incendiary, and sabotage devices.

The design basis threat is "the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is evaluated."[13] Thus, the specification of the design basis threat should include specifying all potential adversary characteristics as well as the attributes of potential adversaries that relate to their ability to defeat physical protection measures. It is not necessary to establish the design basis threat before performing VAI; however, it is necessary to establish potential adversary characteristics before performing a VAI. The potential adversary characteristics must be established in order to identify the types of MAIEs that must be considered in the VAI. For example, a potential adversary with sufficient explosives might be able to breech a reactor vessel, while a potential adversary without explosives might not be able to so, even if he gained access to it. Furthermore, potential adversary characteristics also affect the locations from which the potential adversary can damage equipment and the types of equipment that can be damaged. For example, a potential adversary without explosive or a cutting torch would probably not be able to breech piping to disable a facility system. Likewise, a potential adversary without knowledge of the facility might not be able to determine the precise location of cabling underground piping that could be damaged to disable a facility safety system. In situations where the established design basis threat does not include all the potential adversary characteristics required to perform a VAI, the facility should request clarification from the organization that established the design basis threat (e.g., the State's competent authority.)

Defense-in-Depth and the Single Failure Criterion

The disciplines of nuclear safety and physical protection both employ a concept referred to as defense-in-depth. The nuclear safety discipline has a precise definition of the concept of defense-in-depth, including a very structured approach to ensuring that defense-in-depth is incorporated in facility design, particularly for nuclear reactors. In the context of safety, defense-in-depth is a concept applied to all safety activities — whether organizational, behavioral, or design related — that ensures that they are subject to overlapping provisions, so

[13] Paragraph 2.2.4 of Reference 1.

that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. The approach for applying this concept to the design of nuclear reactors is outlined in Sections 4.1 through 4.4 of Reference 2. One element of defense-in-depth is the use of the "single failure" criterion in the design of the safety groups, which means that the safety group shall be designed to perform its safety function under the assumption that a single failure (and all its consequential failures) occurs in any element of the safety group.

The physical protection discipline has traditionally employed a broader definition of defense-in-depth and a less structured approach in implementing it in physical protection system design. Reference 1 defines defense-in-depth as "a concept used to design physical protection systems that requires an adversary to overcome multiple obstacles, similar or diverse, in order to achieve his objective."[14] Physical protection design has employed the less stringent principle of "minimum consequence of component failure" rather than the single failure criterion.[15] This principle allows for provisions for contingency plans so that the physical protection systems can continue to operate effectively in the event of component failure. It notes that redundant equipment that takes over automatically is highly desirable in some cases, but does not specifically require that it be incorporated in the design of physical protection systems.

1.2.3 Baseline VAI Approach

The basic approach for VAI presented here involves designating as vital and protecting against sabotage:

- All areas from which a potential adversary could cause MAIEs that facility safety groups cannot mitigate to a facility safe state (typically safe shutdown, see Section 2.3); and
- **Either** those areas from which a potential adversary could cause MAIEs that facility safety groups can mitigate to a facility safe state **or** those areas containing one train/division of the safety systems (including the associated piping, water sources, power supplies, controls, and instrumentation) required to achieve a safe state after such an MAIE.

This approach, consistent with typical physical protection design approaches, requires that the minimum complement of equipment, systems, or devices to be protected against sabotage be able to achieve a facility safe state, but does not take into account the effects of a single failure. This approach also builds on the existing defense-in-depth approach for physical protection, which includes:[16]

- A protected area boundary, including a physical barrier, enclosing all vital areas;
- Searches to prevent introduction of articles for use for sabotage;
- A second physical barrier surrounding each vital area;

---

[14] Paragraph 2.3 of Reference 1.

[15] See paragraphs G112 and G114 of 1AEA-TECDOC-967 (Rev.1), "Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities" (Reference 11).

[16] See Paragraphs 2.1.7, 7.1.3, 7.1.4, 7.2.3, 7.2.4, 7.2.10, 7.2.11, and 7.2.12 of Reference 1.

- Intrusion detection and assessment at each of these physical barriers;
- Access controls that limit protected area and vital area access to a minimum number of persons whose trustworthiness has been assured; and
- Guards and response forces.

The VAI approach presented here can be readily adapted to take into account the effects of a single failure. The modifications required to account for postulated single failures are discussed in Sections A.2.1 and A.2.3.5.

1.3 Report Structure

This report is divided into sections corresponding to the policy framework needed, the organization and management of a VAI project, the five major steps for performing VAI, and the documentation of VAI results.

1.3.1 Section 2 – Policy Framework

The policy framework is basically the set of assumptions that need to be made to perform a VAI. It covers issues that cannot be resolved based upon purely technical considerations, but requires policy decisions on the part of the facility performing VAI or the competent authority overseeing the VAI activities. These issues include:

- Clearly defining what is meant by unacceptable radiological consequences in VAI;
- Establishing vital areas for various facility operational states, if applicable;
- Defining the safe state of the facility at which the analysis can be terminated if there are no radiological consequences;
- Setting a policy for dealing with the possibility that random failures will occur concurrently with possible malevolent acts when performing VAI;
- Ensuring that an appropriate minimum complement of equipment, systems, and devices remains protected from sabotage when an item that is in a vital area is unavailable due to maintenance;
- Defining circumstances in which it may be appropriate to take credit, in the VAI, for the operability of items that are not located within vital areas; and
- Establishing treatment of human errors and recovery actions.

The policy framework also briefly addresses the requirements for documenting the VAI.

1.3.2 Section 3 – Management and Organization

This section includes the actions and activities necessary for the organizing and managing a VAI project. It includes identifying prerequisites for performing a VAI; selecting and training personnel, and organizing the team that will perform the VAI; establishing a project schedule and estimating the budget for performing a VAI; and establishing a quality assurance (QA) process for performing a VAI.

1.3.3 Section 4 – Identifying Sources of Radioactive Releases and Possible Malevolent Act Initiating Events

This step is the starting point of the actual VAI analysis. The potential sources of radioactive releases to the environment are identified and screened to determine whether they can be the source of a release that creates unacceptable radiological consequences. The facility operating states to be analyzed are identified, and the safety functions designed into the facility are identified. Much of this information is drawn from deterministic safety analyses (DSAs) or probabilistic safety analyses (PSAs). The MAIEs that can challenge these functions are identified. The relationship between MAIEs, safety functions, front line systems, and support systems are established and categorized.

1.3.4 Section 5 – Sabotage Fault Tree Modeling

This step deals with the construction of a logic model (a sabotage fault tree) that models scenarios leading to unacceptable radiological consequences.[17] The facility sabotage fault tree[18] identifies the MAIEs for which unacceptable radiological consequences cannot be presented and links the remaining MAIEs with the safety functions that must be accomplished to prevent unacceptable radiological consequences. The fault tree is developed further to identify the malevolent acts that could disable the equipment, systems, and devices so that these safety functions are not accomplished. The result of this step is a fault tree logic model of the set of sabotage actions that could cause unacceptable radiological consequences.

1.3.5 Section 6 – Collecting Location Data

This step in the process is the identification of the locations from which the potential adversary could accomplish the set of MAIEs and the malevolent acts that could disable the equipment, systems, and devices causing the failure of associated safety functions. This location information is collected through a structured walkdown process described in the discussion of this step. Finally, the location information is entered into the fault tree logic model to create a

[17] As discussed in Section 5, where PSAs have been prepared, the requirement to convert the event trees to a fault tree is related to limitations in PSA software. If PSA software without these limitations is available, then VAI can be performed using combined event trees and fault trees.

[18] A fault tree is graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. A sabotage fault tree is a fault tree that describes the ways in which systems and components can be disabled to sabotage the facility leading to unacceptable radiological consequences. This fault tree may incorporate the physical locations from which systems and components can be disabled. In this case, the sabotage fault tree cut sets identify the combinations of areas from which sabotage resulting in unacceptable radiological consequences can be committed.

model of the set of locations from which malevolent acts could cause unacceptable radiological consequences.

1.3.6 Section 7 – Identifying Candidate Sets of Vital Areas

This step in the process solves the sabotage fault tree developed in the previous steps to obtain minimal cut sets,[19] each of which identifies combinations of areas from which malevolent acts could cause unacceptable radiological consequences. The Boolean complement of this fault tree is then developed. This is referred to as the facility protection location tree because it identifies the equipment and areas that can be protected to prevent unacceptable radiological consequences. The facility protection location tree is solved to obtain the minimal path sets,[20] each of which identifies a combination of areas that contain the minimum complement of equipment, systems, or devices that, if protected against sabotage, will prevent unacceptable radiological consequences. Each minimal path set is a candidate for the set of vital areas that contains the minimum complement of equipment, systems, or devices to be protected against sabotage.

1.3.7 Section 8 – Selecting Vital Areas

In this step in the process, which typically occurs as a part of physical protection system design, one minimal path set is selected as vital areas for the facility. The description of this step outlines criteria that should be employed to select the facility vital areas. It also presents various options for designating additional areas as vital areas to increase physical protection defense-in-depth, including consideration of providing vital area protection to equipment, systems, and devices employed for accident management.

1.3.8 Section 9 – Documenting Results

This section describes all aspects of documentation of the VAI analysis. This is mainly directed toward providing guidance for the preparation of documentation to demonstrate that the VAI analysis meets the recommendations of Section 7.1.5 of INFCIRC/225 (Reference 1), and that it satisfies the requirements established by the competent authority of the State in which the facility is located.

1.3.9 Section 10 – Conclusions

This section of the report summarizes the advantages of the VAI method presented in this report.

---

19 A minimal cut set is the smallest combination of primary events (usually basic events) such that, if they all occur, will cause the top event to occur. In such a minimal cut set, all of the primary events must occur for the top event to occur.

20 The minimal cut sets of the Boolean complement of the fault tree are referred to as minimal path sets.

1.3.10 Appendix A – Fault Tree Analysis Details

This section of the report provides detailed instructions for performing the fault tree model development and analysis necessary to identify vital areas employing this method. It presents a detailed approach for constructing the sabotage fault tree model as described in Section 5. It also provides detailed guidance for incorporating location equipment into the fault tree model as discussed in Section 6.2. Finally it provides the details about how the fault tree model is to be transformed and solved to identify candidate sets of vital areas, as summarized in Section 7.

2. Policy Framework

Six policy considerations need to be addressed before VAI is performed at a facility:

- Explicit definition of unacceptable radiological consequences;
- Determination of operational states to be analyzed;
- Determination of a safe facility state at which the analysis of facility behavior is terminated;
- Treatment of random failures concurrent with malevolent acts;
- Treatment of maintenance outages;
- Vulnerability of equipment not located in vital areas; and
- Treatment of recovery actions and human errors.

These policy considerations are not unique to the method described here. However, this method presents the issues in a manner that helps ensure that they are explicitly addressed rather than being an implicit part of some aspect of the VAI approach.

The common theme of these policy considerations is risk acceptance. Unacceptable radiological consequences are the threshold of potential radiological harm to the health and safety of personnel, the public, and the environment that triggers requirements for special physical protection against sabotage. For potential radiological harm below this threshold, the risk that standard industrial security and the physical protection measures called out in INFCIRC/225/Rev 4. For non-vital areas (e.g., the physical protection measures recommended for protected areas) provide insufficient protection is accepted. Determining the facility operational states to be analyzed may involve the acceptance of risk if all such states are not analyzed. The decision not to analyze some possible operational states includes accepting the risk that sabotage will be attempted when the plant is in an unanalyzed state and that there are sabotage vulnerabilities in that state that differ from those in the state(s) analyzed. The tradeoff is between accepting that risk and the additional effort required to analyze the facility in all possible operational states.

Similarly, the determination of a safe facility state to terminate the VAI analysis involves the acceptance of the risk that a subtle aspect of facility behavior or an unanticipated combination of equipment failures may render this identified end state unstable or unsafe. The treatment of random failures during malevolent acts is based upon willingness to accept the risk of random events that would aid a potential adversary's sabotage attempt. The treatment of maintenance includes accepting the risks that a potential adversary or actual adversary will attempt sabotage when equipment is down for maintenance and that this will reduce the physical protection defense-in-depth by reducing the number of barriers an adversary must overcome to cause unacceptable radiological consequences. The treatment of the vulnerability of equipment not located in vital areas relates to the acceptance of the risk that actual adversaries may have characteristics that enable them to disable equipment more effectively than the potential adversaries considered in the VAI analysis.

The treatment of recovery actions and human errors involves also involves risk trade-offs. On one hand, the analysis may credit recovery actions that may not be achievable, which risks failing to designate enough areas as vital to protect against unacceptable radiological consequences. On the other hand, the analysis may fail to credit achievable recovery actions, which risks protecting an excessive number of areas leading to less effective protection and higher physical protection costs and operational impact. These risk acceptance decisions are part of the overall trade-offs that the competent authority of each State typically makes in the context of weighing the risks and benefits of activities. Thus, these policy decisions are typically the province of the competent authority of each individual State, but may be explicitly or implicitly delegated to individual facilities on some occasions.

2.1 Defining Unacceptable Radiological Consequences

The first and perhaps the most significant policy consideration that needs to be addressed is the explicit definition of "unacceptable radiological consequences" as discussed in Section 7.1.5 of INFCIRC/225/Rev. 4. This part of VAI answers the question identified in Section 1.2, "What is the specific meaning of unacceptable radiological consequences and what measure is to be employed to determine whether the consequences of acts by a potential adversary are unacceptable?" The competent authority generally establishes the explicit definition of this term. All aspects of the explicit definition of unacceptable radiological consequences, including dose or exposure thresholds and calculation assumptions and methods, should be clearly established before the analysis is begun.

In this discussion two basic approaches are presented for defining unacceptable radiological consequences. The first approach is based on one way that unacceptable radiological consequences are established for nuclear safety analysis wherein these consequences are defined by establishing prescribed and acceptable limits for radiation doses or releases for various categories of events. The safety analysis ensures that the facility design is capable of meeting these limits.[21] Similar prescribed and acceptable limits for radiation doses and releases can be established for malevolent acts. If these limits are exceeded, then the malevolent act has created unacceptable radiological consequences. In the establishment of these limits for malevolent acts, it is necessary to specify the location of dose receptors, the meteorological conditions, and other parameters (e.g., deposition velocity for particulates and plume buoyancy) needed to calculate the dose from a hypothetical radiological release just as these requirements are established for safety analyses. It may also be appropriate to specify a computer program or computational method for performing the dose dispersion calculation.

The competent authority may decide that the same limits should be employed for malevolent acts as are used for some class of accidents, such as design basis accidents. On the other hand, the competent authority may relate these limits to emergency exposure intervention guidelines or may select some other set of limits. Several IAEA publications include numerical emergency

[21] See Paragraph 5.69 of NS-R-1 (Reference 2) and Paragraph 4.1 of NS-G-1.2 (Reference 4).

exposure intervention guidelines.[22] These include recommending sheltering to avert a radiation dose of 10 mSv (1 rem) over a period not to exceed two days. They also recommend temporary evacuation to avert a radiation dose of 50 mSv (5 rem) over a period not to exceed one week. However, the competent authority may have good reasons for employing different standards from any of those cited above. The competent authority may also select the same numerical dose limits for malevolent events and design basis accidents but allow the dose calculations for malevolent events to be based upon less conservative assumptions about meteorological conditions and other dose estimation parameters. This is similar to the treatment of radiation dose limits for beyond design basis accidents. In order to employ a standard of this type for VAI, the individuals performing the VAI need to be able to calculate estimates of the dose resulting from hypothetical malevolent acts.

The second approach for defining unacceptable radiological consequences is based upon a safety analysis that ensures that design limits are met under postulated accident conditions.[23] Unacceptable radiological consequences for VAI can also be operationally defined as a situation in which design limits are exceeded. This is a more conservative definition than one based upon limits for radiation doses and releases. If the design limits are not exceeded, then the radiation dose or release limits will not be exceeded either. However, if the design limits are exceeded, the radiation dose or release limits may or may not be exceeded. Thus, a definition of unacceptable radiological consequences based upon design limits means that the class of events creating unacceptable radiological consequences is larger than the class of events that would cause radiation dose or release limits to be exceeded. This type of definition has the advantage that it is frequently simpler to determine whether a sequence of events would cause design limits to be exceeded than to determine whether it would cause limits for radiation doses or releases to be exceeded. The latter determination frequently requires evaluation of processes and physical phenomena that are poorly understood so there is considerable uncertainly about actual consequences.

However, the design limits-based approach has the disadvantage that it may exclude some accident mitigation systems from consideration in the analysis. For example, one design limits-based definition of unacceptable radiological consequences for a nuclear power reactor would be core damage. If the VAI analysis were based on protecting against core damage, then the containment function would not be modeled, unless there is an interaction between the containment functions and the systems that protect against core damage. Certainly the containment barrier itself would be expected to serve as a vital area barrier because the reactor pressure boundary would need to be in a vital area.[24] However, the locations of items that must function for the containment function to be performed might not be identified as vital. This would reduce physical protection defense-in-depth, because these items could provide a second line of defense that the potential adversary would need to overcome in order to directly or indirectly endanger the health and safety of personnel, the public, and the environment. This potential disadvantage of the design limits-based approach can be overcome in practice by using the methods discussed in Section 8.2 for enhancing defense-in-depth in the selection of vital areas.

---

[22] See, for example, Annex III of GS-R-2 (Reference 5) and Schedule V of SS 115 (Reference 6).

[23] See Paragraph 5.71(4) of Reference 2 and Paragraph 4.79 of Reference 4.

[24] Paragraphs 2.17 and 7.2.12 of Reference 1 require that vital areas be surrounded by physical barriers that provide penetration delay.

From a facility perspective, a combination of these two approaches may also be used. In this hybrid approach, a design limits-based approach is employed for radiological releases from certain locations (e.g., a reactor core), and a dose or release quantity-based approach is employed for releases from other locations (e.g., a spent reactor fuel storage area or gaseous radioactive waste storage tank). This approach is especially useful where safety analyses employing a design limits-based approach (e.g., a Level 1 PSA) have been completed for some potential release locations but not for others. It is also useful where the processes and physical phenomena associated with releases from some areas are well understood (e.g., radioactive waste storage area) and those from other areas are not as well understood (e.g., reactor core).

In using any of these approaches there is a conceptual and practical advantage to employing the same limits for radiation doses and releases or the same design limits for malevolent events and for accidents. The conceptual advantage is that use of the same limits treats malevolent events, which are expected to be quite unlikely, in a manner consistent with the class of unlikely random events considered in the facility safety analysis. The practical advantage of employing the same limits is that it makes it possible to use safety analysis results to decrease the analytical effort required for VAI. The way that the VAI method presented here makes use of the results and the models developed for DSA and PSA is discussed in Sections 4 and 5.

2.2 Facility Operational States

Some facilities may have more than one operational state during normal operations. These different facility operational states may rely upon different equipment to perform necessary safety functions. It is important that the method employed identify appropriate vital areas for all operational states. The first step in this process is defining the facility operational states.[25] The operational state definition should parallel the definition of operational states in the operational limits and conditions established for the facility. The identification of vital areas for all operational states can be accomplished by analyzing each operational state. Alternatively, if a bounding operational state can be identified, a VAI can be performed for that bounding operational state, and the resultant vital areas would be deemed vital during all operational states.[26] A third approach might be to address the normal operating state in detail using the method presented here and then to address other operating states qualitatively or in less detail to identify additional protection requirements for these states. This approach makes it possible to take advantage of information in the safety analyses, which frequently focus on normal operations, and the VAI for normal operations, to gain insights about possible additional protection requirements for other states at lower cost than for a VAI analysis covering all of the states. Regardless of the approach employed, the analysis of each operational state should consider the most vulnerable condition of the facility that is permitted during that operational state. Typically this would be accomplished by performing the analysis assuming that no equipment is down for maintenance and then addressing the maintenance activities permitted in

[25] It is also important to take care to define operational states clearly in terms of potential sabotage vulnerabilities. For example, for a power reactor, shutdown and refueling might be defined as different operational states because of the barriers to radioactive release that are removed to permit refueling.

[26] Depending upon the design of the facility, the bounding state may be a shutdown mode when safety systems could be unavailable or an operating mode where the demands on safety systems are greater. Care should be taken in analyzing the facility to determine the appropriate bounding state.

the operational state in the manner discussed in Section 2.5. After the analysis is completed, it may be desirable to establish one set of vital areas that are applicable for all or most operational states. Often, this is advantageous from a physical protection standpoint to minimize or eliminate the need for reconfiguring physical protection measures when the operational states change.[27]

2.3 Defining a Safe Facility State

When analyzing the consequences of postulated malevolent acts to determine whether they lead to unacceptable radiological consequences, the analysis must end at some point. 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 stable, safe state. One or more of these states needs to be defined as an acceptable termination point for the analysis. The state(s) accepted for this purpose should be a situation(s) where the necessary safety functions can be accomplished for an essentially indefinite period, either by the safety groups designed to perform those functions, by alternative arrangements, or by some combination of safety groups and alternative measures. In accepting one or more of these facility states as a termination point for the analysis, the competent authority should perform an analysis demonstrating the acceptability of the risk of additional sabotage acts or system failures that could result in unacceptable radiological consequences after the safe state is achieved. Where appropriate, this analysis should consider the attributes and capabilities of the potential adversary as well as the reliability of systems relied upon to perform safety functions. The defined facility safe state(s) may differ for analyses of different facility operational states, as discussed in Section 2.2.

2.4 Random Failures

Although VAI focuses on the consequences of malevolent acts, equipment failures could conceivably occur by chance concurrent with malevolent acts. The results of the VAI need to be deterministic; that is, an area is either vital or it is not. A method that designated areas as vital areas with a certain probability is not useful for physical protection purposes. Therefore, the method needs to include identifying which equipment failures will be assumed to occur concurrently with malevolent acts. The simplest approach is to assume that random failures do not occur concurrently with malevolent acts. This is a defensible assumption if threat assessment data indicates that malevolent events are unlikely and facility equipment failures are also unlikely.[28] Alternatively, the assumption can be made that each equipment item or combination of items with reliability below a set value, or failure probability above a set value, referred to as "the probability cut-off," will fail concurrent with a malevolent act. Such a failure would be

[27] There may be exceptions to this generalization. For example, a facility may need to be in a specific operational state for an extended period of time and a VAI may show that a specific area need not be designated as vital in that operational state. In such a case, the facility could choose to de-vitalize that area on a temporary basis. In such case, it would be necessary to carefully search the area for sabotage devices and verify the operability of vital equipment as a part of returning the area to its vital area status before changing the facility operational state to one that required the area to be vital.

[28] The assumption that random failures do not occur concurrently with malevolent acts is not as non-conservative as it might appear. In Section A.2.1, it is shown that random failures do not affect vital area configuration unless they cause the failure of an entire system or system train or a special component that affects the systems needed to respond to an MAIE. Therefore, the issue is not generally the reliability of individual components but the reliability of system trains and systems.

assumed to occur only if the failure would make the consequences of a postulated malevolent act more severe or permit a potential adversary to achieve the same consequences with fewer malevolent acts or malevolent acts in fewer locations.[29] To employ a rule of this type it would obviously be necessary to have or develop failure/reliability data for the facility equipment, the failure of which it might be appropriate to assume during VAI. Such data would generally be available if a Level 1 PSA[30] (see Reference 3) had been performed for the facility before the VAI. In setting a probability/reliability threshold for assuming that a random failure occurs concurrently with a malevolent act, care should be taken to establish consistent requirements for the design of physical protection systems.[31] It should be noted that, for facilities without a Level 1 PSA, the effort required to develop the random failure probabilities needed for this type of analysis could be commensurate with the effort required to perform a Level 1 PSA. Even for facilities where the data are available from a PSA, modeling of concurrent random failures may significantly increase the complexity and difficulty of VAI. (See Sections A.2.1 and A.2.3.4.)

Random failures of equipment in this context should not be confused with equipment failures that are indirectly caused by malevolent acts. For example, if a malevolent act disables the cooling system for a pump, the VAI should assume that the pump will fail unless there is appropriate evidence that the pump has sufficient design margin to continue to operate without the cooling system. Such an equipment failure is not random, but rather is the predictable indirect result of a malevolent act. In this example, a random failure would be a failure of the pump to operate, concurrent with a malevolent act that had no effect on the pump, its support systems, or operating environment.

It may be best to approach this policy decision through an iterative process, where the VAI is initially performed under the assumption that random failures do not occur concurrently with malevolent acts. This process would then be refined either by examining the reliability of the equipment, systems, and devices protected (see Section 8.1.3) or by examining the effect of accounting for the most likely random failures on vital area configuration. Based upon the considerations discussed in Section 8.2.3 and other considerations related to safety, emergency response, and the cost-effectiveness of any required additional physical protection measures, the competent authority or facility could determine the type of random failures that should be assumed to occur concurrent with malevolent acts.

2.5 Maintenance

As discussed above, VAI involves identifying "the minimum complement of equipment, systems, or devices to be protected against sabotage." At some time over the life of the facility at least some of this minimum complement of equipment, systems, or devices will need to be removed from service for maintenance (i.e., temporarily inoperable). During these periods,

---

29 The point is not an assumption that a potential adversary would be so foolish as to rely upon random failures, but rather that otherwise sufficient physical protection measures would fail to prevent unacceptable radiological consequences because of concurrent random failures. Random equipment failures that mitigate the consequences of malevolent acts are to be excluded from the VAI modeling by a corollary of the traditional fault tree analysis "no miracles rule." See Chapter V of NUREG-0492, "Fault Tree Analysis Handbook" (Reference 7).

30 A probabilistic safety analysis is a comprehensive, structured analysis that identifies accident scenarios and derives numerical estimates of risks.

31 For example, an intrusion detection system or a component of that system would be required to be designed so that its reliability was above the set value. .

additional equipment must be protected so that a sufficient complement of equipment, systems, and devices remain protected against sabotage. This may be accomplished using at least two strategies. The simplest strategy is to conduct the VAI without consideration of maintenance outages and, when these outages occur, take appropriate compensatory measures to ensure that an appropriate minimum complement of operable equipment, systems, or devices remains protected against sabotage. This can be accomplished by designating, as vital, additional areas that need protection only when specific safety systems are down for maintenance. These are referred to as temporary vital areas. These additional areas can be identified from the candidate vital area sets developed during the VAI. The policy issue associated with this strategy is the length of the maintenance outage that requires activation of these temporary vital areas. The competent authority should establish this outage time based upon an assessment of the capabilities of the potential adversary to take advantage of items being out of service for maintenance. Typically such capability would require that the potential adversary be able to obtain information (e.g., through an insider) and to gather and deploy the resources required for a sabotage attempt during the maintenance outage. Where there is a design basis threat applicable to the facility, the assumptions about the ability of the potential adversary to take advantage of items being out of service for maintenance should be consistent with the defined design basis threat. The capabilities of a potential adversary, related to establishing the length of the maintenance outage that would require protection be afforded to one more temporary vital area(s), are a very small part of the overall design basis threat. Therefore, this decision can be made quite well, based upon a general understanding of potential adversary capabilities, without completing the formal process for developing a design basis threat.

A second, more complex strategy for addressing maintenance outages is to designate facility vital areas so that the minimum complement of operable equipment, systems, or devices to be protected against sabotage would remain protected by being in vital areas even though some equipment was undergoing maintenance. If this approach is employed, care must be taken to ensure that extensive facility maintenance does not create a situation in which a minimum complement of operable equipment is no longer protected. The approach for accomplishing this during the VAI is discussed in Section A.2.3.5. The policy decision that must be made for this strategy is how much more than the minimum complement of equipment, systems, or devices should be protected by being included in designated vital areas. As discussed in Section 8.2.3, having too much equipment in vital areas can reduce physical protection effectiveness as well as increase related physical protection costs and potentially impact safety or emergency response. It may be useful to employ an iterative process that refines the amount of the equipment, systems, or devices to be protected, based upon the effect on the vital area configuration.

2.6 Vulnerability of Equipment Not Located in Vital Areas

Equipment, systems, or devices not located in vital areas are typically afforded physical protection because of their location within the protected area and in the facility. However, the conservative assumption is generally made that the potential adversary can disable these items because they are not afforded the special protection required for vital areas. This may not be an appropriate assumption in all circumstances. For example, if the equipment is difficult to locate

or hardened against attack by safety or other measures, this circumstance, in combination with the physical protection that is afforded items outside a vital area, may be judged to provide adequate protection against a potential adversary. For example, equipment that is difficult to locate might be the cable run for the control cabling or power cabling for a specific piece of equipment. If the facility has not maintained records of cable run locations, performed safety evaluations that require cable tracing (e.g., fire hazard evaluations), or traced and documented cable locations for some other purpose, it would be quite difficult for even knowledgeable insiders to locate specific cable runs. Unless documented evaluations containing cable run information had been made publicly available, it would be quite difficult for an external potential adversary to locate specific cable runs.

Equipment that might be both naturally hardened against attack and difficult to locate would be underground piping. Again, if the facility has not maintained records of underground pipe run locations or traced and marked or documented underground pipe run locations for some other purpose, it would be quite difficult for even knowledgeable insiders to locate underground pipe runs. And unless documentation containing underground pipe run information had been made publicly available, it would also be quite difficult for an external potential adversary to locate specific pipe runs. Furthermore, in the absence of manholes or other access points, the potential adversary would probably need to penetrate a meter or more of soil to gain access to the underground piping to disable it. Depending upon potential adversary capabilities, this could be as complex, time consuming, and likely to alert response forces as penetration of vital area barriers.

These are examples of situations in which it may be reasonable to credit the operability of equipment located outside of vital areas. Obviously, the decision about whether equipment outside vital areas may be assumed to be operable depends upon both the facility configuration and the capabilities that the potential adversary is deemed to have. Where there is a design basis threat applicable to the facility, the capabilities that the potential adversary is deemed to have should be consistent with those defined in the design basis threat. Note that the information needed to make such decisions is a very small part of the overall design basis threat. Therefore, these decisions can be made quite well, based upon a general understanding of potential adversary capabilities, without completing the formal process for developing a design basis threat. The competent authority should establish the conditions, if any, under which equipment outside vital areas may be considered sufficiently resistant to malevolent acts that it can be assumed to be operable even if it is outside of a vital area. These conditions should take appropriate account of facility configuration and the characteristics of the potential adversary. For example, even if it is decided that individual cable runs outside of vital areas can be assumed operable, it may be appropriate to require that locations through which a large number of cables run (e.g., the cable spreading room at a nuclear power reactor) be designated as vital areas.[32] Likewise, it may be appropriate to designate manways (small passageways) that provide access to underground piping as vital area access points if the underground piping is determined by VAI to be part of the minimum complement of equipment, systems, or devices required to be protected against sabotage.

[32] This approach provides protection for those areas where a potential adversary employing the generally inferior strategy of mindless destruction might “get lucky” and cause unacceptable radiological consequences.

Early identification of classes of items that do not require vital area protection can significantly reduce the cost and effort required for VAI. In principle, it is desirable to identify vital areas before determining whether specific classes of items require vital area protection. However, for some facilities, this approach can require significant effort to locate and model items (e.g., chasing cable runs and identifying the specific locations of underground piping) that turn out to be wasted when these items are later determined not to require vital area protection. In general, if there is not the potential for a significant savings in VAI cost or effort, vital areas should be identified before determining whether specific classes of items require vital area protection. This may be another situation where an iterative process can be useful. Determining whether specific classes of items require vital area protection may be refined based upon the effect of that determination on the vital area configuration.

2.7 Treatment of Recovery Actions and Human Errors

The safety analyses and other analyses that are used as a basis for VAI frequently contain explicit or implicit assumptions about personnel actions. These may relate to routine or emergency operator actions that are needed to maintain the facility in a safe state (see Section 2.3). They may also be implicit in the way that the facility response to events is modeled. The VAI team (see Section 3.2) should be careful to identify all implicit and explicit assumptions about personnel actions that are included in the safety and other analyses used as a basis for the VAI. After these actions have been identified, the VAI team needs to determine whether they should be credited as part of the facility response to sabotage. During the course of the VAI, the VAI team may also identify possible recovery actions to compensate for disabled equipment. In this case too, the VAI team needs to determine whether the recovery actions should be credited as part of the facility response to sabotage. It is useful to establish standards to assist in making these determinations. The following standards are recommended, as a minimum, for the crediting of personnel actions and proposed recovery actions:

- A realistic, best estimate analysis demonstrates that the facility will respond to the actions under consideration in the manner modeled. This analysis accounts for the anticipated environmental effects associated with the sabotage events (e.g., habitability of locations where the personnel actions must be performed), and for the likely effects of using equipment under circumstances for which it was not designed.[33]

- The actions under consideration are documented in facility procedures and facility personnel have been trained in taking them.

- The actions under consideration have been demonstrated to be practical under normal circumstances and are judged to be practical after or during the associated sabotage scenario(s), as appropriate. The judgment about practicality during the associated sabotage scenario(s) includes consideration of the effects of stress upon the performance of the personnel taking the actions under consideration.

[33] An example of the type of effects to be considered is the effect of two-phase flow on relief valves during their use in the "feed and bleed" alternative core cooling method for a pressurized water reactor.

The competent authority or facility may determine that it is appropriate to establish more stringent standards for crediting recovery actions or other personnel actions. The VAI team should document the rationale for crediting personnel actions, including recovery actions.

If the facility has a PSA meeting IAEA recommendations, it will include a human performance analysis[34] that will identify the human interactions most important to the safety of the facility and include estimates of the likelihood of human error in these interactions. The VAI team should review this information to determine whether the VAI analysis should include the assumptions that these errors will be made. With the additional stress associated with an assault on the facility or sabotage attempt, the likelihood of human error during a sabotage scenario is unlikely to be lower than it is during an accident. If random errors with a likelihood greater than an established probability cut-off are assumed to occur concurrent with malevolent acts, then human errors with likelihoods greater than this cut-off should also be assumed to occur concurrent with malevolent acts (so long as the combined likelihood of human errors and random failures exceeds the probability cut-off). The competent authority or facility may determine that a different approach to addressing the possibility of human error concurrent with malevolent acts is more appropriate, including the assumption that human errors do not occur concurrent with malevolent acts. Assuming no human error may be a good assumption if threat assessment data indicate that malevolent events are unlikely and the human errors that have the potential to affect VAI results are also unlikely.[35] In such a case the combined likelihood of malevolent events and human errors that affect VAI results is as low as the likelihood of other types of events that are not considered in physical protection system design. Examples of such events would include errors by security force personnel coincident with an attack by a potential adversary.

[34] See Section 4.3 of Reference 3.

[35] Human errors with the potential to affect VAI results are those that disable safety systems or trains of safety systems or affect the facility response so that different safety systems are required to respond to MAIEs.

3. VAI Management and Organization

The management and organization of VAI activities is critical to ensuring that the results are accurate and that the VAI can be completed on schedule and within budget. Establishment of a clearly defined project schedule and provision of an adequate budget is also key to successful VAI. The complexity of VAI logic models for many realistic facilities necessitates the establishment of a process for quality assurance. The schedule and budget required to perform a VAI are strongly dependent upon whether certain prerequisites are met.

In general, facility management will perform VAI under the oversight of the state competent authority and cognizant regulatory authorities. The competent authority or cognizant regulatory authority also may perform a VAI or portions thereof, in the course of discharging its responsibility to verify that the facility vital area designation complies with the recommendations of Reference 1 or other requirements. Selecting, training, and organizing the VAI team are other critical factors in the success of the effort. These aspects of the management and organization of the VAI process are discussed below.

3.1 Prerequisites

There are several prerequisites to performing VAI. The most important prerequisite is the resolution of the policy issues discussed in Section 2. Although the completion of facility safety analyses is a less important prerequisite, it is still quite valuable. Facility safety analyses, whether DSA or PSA, contain analyses of the response of the facility to initiating events (IEs) that could be caused by a potential adversary. Although a potential adversary may be able through malevolent acts to create IEs more severe than those considered in the safety analyses, the safety analyses provide a basis for addressing many of the possible malevolent acts considered. If the VAI cannot use analysis results from facility safety analyses that meet international standards, a significantly greater effort will be needed to analyze the response of the facility to malevolent acts.[36] (See Section 3.4.) Guidance for performing such analyses for power reactors may be found in Reference 4.

Establishing a design basis threat is not a prerequisite for VAI. However, the results will depend, to some extent, on the capabilities of the potential adversary. The relationship between the designation of vital areas and the capabilities of a potential adversary is discussed in Section 1.2.2 and alluded to in Sections 2.5 and 2.6. Potential adversary characteristics, such as the quantity and types of explosive that a potential adversary may be able to transport into the facility, will determine whether certain MAIEs are possible. Such characteristics may also determine whether specific equipment, components, or devices can be disabled and the locations from which it can be disabled. For example, large, thick-walled piping probably cannot be breached by a potential adversary without explosives or cutting torches. Similarly, the locations from which a potential adversary could breach a tank might depend upon whether the adversary

[36] International standards in this area are presented in IAEA NS-R-1 (Reference 2) and NS-G-1.2 (Reference 4) for nuclear power reactors; IAEA Safety Series No. 35-G1, "Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report," for research reactors; and IAEA-TECHDOC-1267, "Procedures For Conducting Probabilistic Safety Assessment For Non-Reactor Nuclear Facilities," for non-reactor nuclear facilities.

had appropriate standoff weaponry. The discussion in subsequent parts of the report will highlight areas where portions of the VAI model and results will depend upon characteristics of the potential adversary. If a design basis threat has been established, then the potential adversary characteristics employed should be consistent with the design basis threat.

3.2 Team Composition

The VAI team should be comprised of at least three members from three facility organizations: facility safety, physical protection, and facility operations. The team member from the facility safety organization should be familiar with the facility safety analyses. This individual should be knowledgeable of the assumptions that were made in the evaluations of facility response in the safety analyses and should be familiar with the types of safety issues affecting the facility. This may include familiarity with the design of fluid and electrical systems, operational aspects, and facility layout. This team member should also be knowledgeable of the capabilities of the facility safety and engineering organizations. This team member should know how to obtain expert technical support in mechanical, electrical, and instrumentation and control engineering to address specific issues. This individual serves as the leader of the safety specialists mentioned in Paragraph 7.1.5 of Reference 1.

The team member from the physical protection organization should be an expert in security engineering, physical protection system design, and vulnerability assessment. This individual should be experienced in evaluating security systems from the adversarial perspective ("black hatting") and have a good understanding of the capabilities and use of explosive devices and other tools that might be used by the potential adversary. This team member should also be knowledgeable of the capabilities of the facility security organization and their engineering support organization and should know how to obtain expert technical support to address specific issues. This individual serves as the leader of the physical protection specialists mentioned in Paragraph 7.1.5 of Reference 1.

The team member from the facility operating organization should have hands-on experience operating the facility, be familiar with equipment locations and operations, and be knowledgeable of routine and emergency operating procedures.[37] This team member should be knowledgeable of the capabilities of the facility operations, maintenance, and engineering support organizations and know how to obtain expert technical support to address specific issues. Although Reference 1 does not specifically mention the participation of the operating organization in VAI, the operating organization representative has a critical role on the team. This member helps the team understand overall facility operation, leads the VAI walkdowns to identify locations from which equipment can be disabled, and helps ensure that vital areas are selected so that their protection does not adversely affect facility safety and does not place an undue burden on facility operation.

An important collateral benefit of performing VAI is that it fosters communication and mutual understanding among the safety, physical protection, and operating organizations. For large, complex facilities this team will probably need to be augmented with additional staff from these

[37] For a nuclear power reactor, the desired level of experience and qualifications is that of a senior reactor operator.

disciplines. For small, simpler facilities, the team members may not need to work full time on VAI activities, although these activities should be team members' highest priority assignment for the duration of the analysis.

The VAI team will need to be supported by someone with expertise in fault tree analysis modeling and the specific computer programs (typically fault tree analysis or PSA programs) that will be used. For complex facilities this individual should be able to provide full-time support to the team. For simpler facilities, it may be possible for the safety organization representative to perform these functions.

For large, complex facilities, it may be necessary to have one or more additional team members who focus on the management of the overall project and liaison with other facility organizations to exchange information and resolve managerial, procedural, and technical issues. Although VAI has a strong safety component, the project should be managed by the physical protection organization because it is an integral part of facility physical protection. For smaller, simpler facilities, the security organization representative should lead the VAI team and manage the overall effort. All team members and support personnel should meet the information protection requirements for access to the categories of information that are required to perform, and that are generated during, the VAI analysis (see Section 9.1).

3.3 Team Training

A team performing VAI for the first time will require training to acquire the specific expertise needed to successfully conduct the analysis. Even though individual members of the team will already have some of the expertise required, it is strongly recommended that the team train together before the analysis is begun to achieve a common understanding of the objectives and methods used. As a minimum, the following four types of training should be given and attended by all team members.

1. *Facility system and operational procedures.* This course (typically 3 days to 1 week) should cover the basic aspects of the facility, including anticipated operational occurrences and accidents of concern, the safety groups and their functions to mitigate these occurrences and accidents, and operational procedures under normal and accident conditions.

2. *Physical protection basics.* This course (typically 1 to 2 days) covers the basic concepts of physical protection as they relate to vital area identification and protection. If the State competent authority has established a design basis threat applicable to the facility where the analysis is being performed this course should cover relevant aspects of the design basis threat. This training should also address the information protection requirements applicable to information generated (see Section 9.1).

3. *Fault tree analysis techniques.* This course (typically 3 days) should cover the basic principles of fault tree modeling, the input and output of the fault tree analysis or PSA software to be employed. The objective of this training is to give the team members a level of knowledge that will help them ensure that their insights about the facility design and

operation and potential adversary capabilities and characteristics are being faithfully incorporated into the fault tree model that is the basis of this approach.

4. *VAI method – comparative review of VAIs for similar facilities.* This course (1 week) should cover the VAI approach presented in this report. If the State competent authority has established policy to resolve the issues discussed in Section 2, these policy assumptions should be also be covered in this course. If these issues are to be resolved only for this specific VAI, this course should include a facilitated session that presents these issues and develops facility-specific resolutions. If analyses for facilities of similar design have been prepared and documented, and are available, these should be reviewed as part of this course. The purpose of this course is to ensure that team members have a common understanding of the VAI method, the assumptions that are appropriate for their facility, and their roles and responsibilities in the process.

3.4 Funding and Scheduling

The resources in terms of person-hours, time, and computer resources required to perform VAI depend greatly on the complexity of the facility being analyzed, the amount of applicable safety analysis information that is available, and the experience and expertise of the team. Significant reductions in the effort and time required can be achieved if VAI models for similar facilities are available for review and adaptation. Naturally, scheduling of activities is affected by the availability of personnel to serve on and support the VAI.

The following example may be of assistance in estimating the resources and time required to perform a VAI. For a facility of the complexity of a nuclear power reactor, an experienced three-person team working full time can complete and document a VAI analysis, using this method, in two to three months. This estimate assumes that the available safety analysis information is adequate to perform the VAI without additional engineering analyses of facility response to MAIEs or detailed analyses of equipment, component, or device reliability and availability. Additional time and resources would be required for a large number of dispersion and dose calculations or engineering evaluations of alternative facility response to malevolent acts, that rely upon design safety features or alternative accident management/damage control measures. Additional time would be required if the team were not experienced in applying the VAI method. The schedule can be compressed to some extent by enlarging the VAI team.

3.5 Quality Assurance

Quality assurance (QA) for VAI encompasses the activities necessary to achieve the appropriate quality in application of the method and those that are necessary for verifying that the required quality is achieved. For a VAI analysis, appropriate quality means an end product that is correct, useable, meets the recommendations of Section 7.1.5 of Reference 1, and can be shown to satisfy the requirements established by the competent authority of the State in which the facility is located.

QA is an essential aspect of "good management" (see Sections 201 and 202 of Reference 8). Good management contributes to achieving quality through thorough analysis of the tasks to be performed, identifying the skills required, selection and training of appropriate personnel, creation of a satisfactory environment where activities can be performed, and recognizing the responsibility of the individual who is to perform each task. Briefly stated, the QA activities should provide for a disciplined approach to all activities affecting the quality of the analysis, including verifying that activities have been satisfactorily performed, and, if not, instituting appropriate corrective actions. A critical aspect of this is appropriate documentation of activities, such as work papers, memoranda and correspondence, engineering calculations, computer files, computer output, and the final report, suitable for use by the appropriate personnel. All assumptions made in the analysis and any interpretations of policy guidance and requirements from the facility or State competent authority should be documented. Documents prepared and records generated during the analysis should be prepared, formatted, and retained in accordance with the policies and procedures established by the facility for quality records and any requirements established by the competent authority of the state in which the facility is located. Because of its possible value to a potential adversary, the documents prepared and records generated during the VAI analysis should be protected in accordance with the information protection requirements established by the competent authority and the implementing requirements and procedures established by the facility (see Section 9.1).

Information should be entered into computer programs so that fault tree model logic, calculation parameters, or other significant aspects of the calculation are evident and clearly presented. To the maximum extent practicable, the analysts must avoid shortcuts and computer programming tricks that obscure fault tree model logic, calculation parameters, and other significant aspects of calculations. The results of computer calculations must always be checked for reasonableness and any apparent discrepancies must be thoroughly investigated.

QA reviews should be conducted at the completion of the activities described in Sections 4, 5, 6, and 7 of this report. The individual(s) performing these reviews should be experienced in this method and should be independent of this particular VAI analysis so they are not reviewing their own work. The QA review conducted at the completion of the activities described in Section 4 should address the comprehensiveness of the identified MAIEs, front line systems, support systems, and the interdependencies among front line systems and support systems. The QA review conducted at completion of the activities described in Section 5 should address the clarity of the sabotage fault tree and its consistency with the information gathered and documented in the tasks described in Sections 4 and 5.

The QA review conducted at completion of activities described in Section 6 should address the accuracy of the location information gathered and the process for incorporating it into the sabotage fault tree. This review should also address the clarity of the sabotage fault tree and the associated documentation. QA reviews for the activities described in Section 7 should be conducted after the solution of the sabotage fault tree and the protection location tree.[38] The sabotage fault tree review should examine the solutions to understand the combination of MAIEs and disabling of safety systems that each term in the solution represents. These should be

[38] The protection location tree is the logical complement of the sabotage fault tree (sometimes referred to as the dual of the sabotage fault tree). This fault tree describes the systems, components, and locations that must be protected to prevent facility sabotage. The minimal path sets of this tree are candidate vital area sets.

checked for consistency with facility safety analyses and other safety documentation. The protection location tree review should examine the solutions to understand the combination of systems being protected and MAIEs being prevented that each term in the solution represents. These should be checked for completeness based upon the insights gained from the review of the solution to the sabotage fault tree. Corrective actions should be taken to address issues identified in each of these quality assurance reviews before performing the subsequent stage of the VAI analysis.

4. Identifying Sources of Radioactive Releases and Possible Malevolent Act Initiating Events

This section describes the first major step in performing the actual VAI analysis. This part of VAI answers two of the key questions identified in Section 1.2.1.

- "What are the sources of radioactive material that can be released to cause unacceptable radiological consequences?"

- What malevolent acts (referred to as malevolent act initiating events [MAIEs]) can a potential adversary commit that might cause radioactive material to be released, causing unacceptable radiological consequences?

The main purpose of this step is to produce a list of malevolent acts by which the potential adversary might initiate a chain of events leading to unacceptable radiological consequences (MAIEs). Many of these IEs will have already been identified and analyzed in facility safety documentation, such as a DSA or PSA report. However, there are three classes of MAIEs that are probably not addressed in facility safety documentation. The first class of MAIEs involves situations where there is no process or other energy normally present that could disperse radioactive material. Under these circumstances, malevolent 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 malevolent act. Because these IEs are not possible without a malevolent act, they are not analyzed in safety documentation.

The second, related class of MAIEs that may not have been analyzed in safety documentation is those IEs that are so unlikely to occur randomly that they may have been excluded from consideration. Such events typically include 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 tools.

The third class of MAIEs is those involving 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 only address 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 unacceptable radiological consequences (such as irradiated fuel and radioactive waste) also need to be considered in VAI.

When identifying the MAIEs, the team should maintain awareness of these three classes of events that may not be included in safety documentation. The specific events included in these classes will depend upon both the design of the facility and the capabilities, credited to the potential adversary, to damage equipment, components, and devices.

4.1 Selecting Malevolent Act Initiating Events

This part of VAI answers the question identified in Section 1.2.1, "What malevolent act initiating events can a potential adversary commit that might cause radioactive material to be released, causing unacceptable radiological consequences?" There are four approaches to the selection of MAIEs, each with its advantages and limitations. Because the objective is to produce a list that is as complete as possible, all of the approaches below should be followed, although one may be selected as the main approach.

1. *Review of safety documentation.* This should be the starting point for this part of the VAI, when the safety documentation is available. Lists of IEs in DSA and PSA, in fire analyses, seismic analyses, and other safety evaluation for the facility being analyzed and for similar facilities should be reviewed. Because any of the IEs that can occur randomly can also be caused by malevolent acts, this set of IEs should be included in the list of MAIEs. 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 possible malevolent acts and revised where appropriate.

2. *Reference to other VAIs.* Where other VAI analyses have been performed for similar facilities, lists of the MAIEs used should be reviewed. It is particularly important to identify MAIEs 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 see whether any consequences of malevolent 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 malevolent acts, to unacceptable radiological consequences. This approach should generally not be selected as the main approach for VAI unless the facility has very limited safety documentation. If the safety documentation is adequate, engineering evaluations should be limited to circumstances where they will provide a definite benefit, including consideration and analysis of classes of possible malevolent acts that are not addressed in safety analyses or documentation (see Section 4.3).

4. *Deductive analysis.* In this approach, unacceptable radiological consequences is the top event in a diagram that has the appearance of a fault tree, though it is not one. This top event is systematically decomposed into all possible categories of 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 MAIEs for the facility. The use of such diagrams can also assist in the definition of safety functions (see Section 4.2). This approach should generally not be selected as the main approach for VAI unless the facility has very limited safety documentation. Here again, the main benefit of this approach for facilities with adequate safety documentation is brainstorming about classes of possible malevolent acts that are not addressed in safety analyses or documentation.

Care should be taken to include MAIEs that may be accomplished from outside the facility. Depending upon the capabilities that the potential adversary is deemed to have, MAIEs of this type can range from attacks on electrical transmission components that isolate the facility from

the electrical grid to attacks on facility structures and large components (e.g., storage tanks or transformers) with stand-off weapons. Events in this classification will need to be treated differently from those that require the potential adversary to access areas within the facility.[39] The approach for treating such MAIEs is discussed in Sections 6.2 and A.3.3.

Care should also be taken to include MAIEs for each of the facility operational states that the VAI needs to address, as identified in Section 2.2. MAIEs should be cross-referenced to the facility operational state(s) for which they are applicable.

The list of MAIEs should be reviewed to remove any repetitions or overlaps and checked further for inadvertent omissions. Once identified, the MAIEs are normally listed in a systematic way. A simple example for a light water reactor might be:

1. Loss of Coolant Accident (LOCA) break sizes (beyond design basis, large, small);

2. Interfacing system LOCAs, and other LOCAs that affect mitigating systems;

3. Transients applicable to the facility;

4. Transients initiated by disabling support systems in ways that affect mitigating systems;

5. Combinations of the above (e.g., LOCAs with loss of offsite power); and

6. Malevolent acts directed against other radioactive material inventories, such as irradiated fuel or radioactive waste storage.

The list of MAIEs should be prepared in suitable format and retained as a VAI analysis record (see Section 3.5).

4.2 Determining Safety Functions and Associated Systems

This part of VAI answers the question identified in Section 1.2, “What safety groups must a potential adversary disable concurrent with MAIEs to cause unacceptable radiological consequences?” The determination of safety functions and the identification of associated facility systems are performed in this stage of the analysis because the MAIEs can be grouped based upon the demands that they place on safety functions: front line systems and support systems. This grouping of MAIEs significantly simplifies the subsequent development of the facility sabotage fault tree. The information developed in part of the analysis is also directly useable in the creation of the facility sabotage fault tree in Section 5.

For each MAIE, the safety functions that need to be performed in order to prevent unacceptable radiological consequences should be identified. Note that the safety functions that need to be performed in response to a specific MAIE may vary depending upon the facility operational

[39] This different treatment is required because these MAIEs cannot be protected against by designated the areas from which they can be caused as vital areas. Therefore, they are treated in a different manner where the events are linked to locations as described in Section 6.2 and A.3.3.

state, as discussed in Section 2.2. The concept of safety functions is discussed in References 2 and 3. The annex to Reference 2 lists the safety functions for light water reactors. Safety functions for light water reactors that are important for protecting against unacceptable radiological consequences are listed below.[40]

1. Control reactivity;

2. Remove core decay heat and stored heat;

3. Maintain integrity of primary reactor coolant boundary (pressure control);

4. Maintain primary coolant inventory;

5. Protect containment integrity;

6. Scrub radioactive materials from containment atmosphere;

7. Remove irradiated fuel decay heat;

8. Maintain integrity of irradiated fuel storage; and

9. Maintain integrity of radioactive waste storage.

These functions are illustrative of the functions to be considered in the analysis. However, it may not be necessary to protect all of them to achieve the level of protection identified as the baseline in Section A.2.

The safety functions required to maintain radiation doses and releases within prescribed and acceptable limits are typically described in safety analysis reports. The information in these reports may be presented in terms of the functions performed by safety systems rather than a specific listing of safety functions.[41] However, it is usually possible to infer the facility safety functions from the description of the functions performed by the corresponding safety system. For example a PWR containment cooling system cools the containment atmosphere during and following a loss of coolant accident to condense primary coolant that has blown out of the reactor, reducing the pressure in the containment. This reduces the load that the containment must bear to remain leak tight. Thus, the PWR containment cooling system supports the safety function of maintain containment integrity. These safety functions and safety systems are typically a superset of the safety functions and safety systems that provide protection against unacceptable radiological consequences. In addition to the safety functions and safety systems that protect against unacceptable radiological consequences, safety analysis reports and other safety documents include safety functions and safety systems that serve to maintain worker radiation exposure and routine radiological releases within appropriate limits during normal

[40] This list does not include maintenance of subcriticality of irradiated fuel based upon the implicit conclusion that a criticality in the irradiated fuel storage area would not cause unacceptable radiological consequences. The validity of this conclusion depends upon the definition of unacceptable radiological consequences as discussed in Section 2.1. As spent fuel storage is configured at most reactors, if the definition of unacceptable radiological consequences is based upon dose to the off site public, a criticality in the irradiated fuel storage area would not cause unacceptable radiological consequences.

[41] This is typically the case where a PSA has not been performed for the facility. Where a PSA has been performed, the PSA will identify the facility safety functions and the safety and, in some cases, non-safety systems that can be employed to perform them.

operations and anticipated operational occurrences. Frequently, the safety functions and safety systems that serve these latter purposes do play a role in protecting against unacceptable radiological consequences. Thus, the safety functions that provide protection against unacceptable radiological consequences can generally be obtained directly from the facility safety analysis report or inferred from them.

The next stage of the analysis is to identify the systems that are directly or indirectly required for the performance of each safety function. Here again, the specific systems that perform a particular safety function may differ depending upon the facility operational state. The systems that directly perform a safety function are defined to be front line systems and those required for proper functioning of the front line systems are defined to be support systems. Table 4-1 shows safety functions and the corresponding front line systems for a typical pressurized water reactor.

Table 4-1. Pressurized Water Reactor Safety Functions and Corresponding Front Line Systems

Safety Function	Front Line System
Control reactivity	(a) Reactor protection system (b) High pressure injection system
Remove core decay heat and stored heat	(a) Power conversion system (b) Emergency feedwater system (c) High pressure injection system and pressurizer relief valves (feed and bleed) (d) Low pressure injection system (e) Residual heat removal system
Maintain integrity of primary reactor coolant boundary (pressure control)	Pressurizer safety relief valves
Maintain primary coolant inventory	(a) High pressure injection system (b) Low pressure injection system
Protect containment integrity (isolation, overpressure)	(a) Containment spray system (b) Containment cooling system
Scrub radioactive materials from containment atmosphere	(a) Containment spray system (b) Containment ventilation system
Remove irradiated fuel decay heat	Spent fuel pool cooling system
Maintain integrity of irradiated fuel storage	Spent fuel pool
Maintain integrity of radioactive waste storage	(a) Gaseous waste processing system (b) Liquid waste processing system (c) Solid waste processing system

The objectives of this activity are (1) to obtain all necessary information about the front line systems and support systems that will determine facility response to a specific MAIE; and (2) to identify and assess dependencies in a preliminary way. As with the safety functions listed above, these front line systems are illustrative of the types of systems that should be considered for a pressurized water reactor. It may not be necessary to protect all of them to achieve the level of protection identified as the baseline for VAI in Section A.2.

For each safety function that provides protection against unacceptable radiological consequences, the set of front line systems that perform this function alone or in combination with other systems, should be identified and catalogued (see Table 4-1). As discussed above, this information can typically be obtained from the facility safety analyses. The list of all front line systems to be considered should be developed and the associated information about these systems should be located in safety analyses and other safety documents.

In this analysis, the VAI team prepares a dependency table or spreadsheet linking front line systems with the support systems that they are dependent upon. The initial dependency table/spreadsheet is then used to produce a list of support systems. The team identifies all systems required for the functioning of these support systems. These additional support systems are added to the list of support systems. The team repeats this process until all systems that affect the operation of the front line systems through this chain of dependencies have been identified and their dependencies documented. The analyst also makes a dependency table/spreadsheet illustrating the dependencies among these support systems. If a PSA has been prepared for the facility, this information should be readily available from the PSA or supporting documentation (see Reference 3). If only a DSA is available, then the analyst 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 extremely helpful in identifying front line systems and their dependencies. The analyst then revises the front line system dependency table/spreadsheet to reflect the second and higher order dependencies shown in the support system dependency table/spreadsheet.

These dependencies relate to the direct hardware and functional dependencies. There may be other dependencies that relate to specific malevolent acts or sabotage scenarios. For example, explosive breaching of a cooling water pipe may cause flooding that disables equipment near the pipe breach. Such location dependencies will be analyzed later in the VAI process and should not be included in the dependency tables/spreadsheets developed in this activity.

The final results of this activity are:

1. A list of the safety functions needed to respond to each MAIE[42] and a table/spreadsheet of safety functions and combinations of front line systems that can perform each function;

2. A list of front line systems;

3. A list of support systems (all inclusive);

[42] There are likely to be some MAIEs for which there are no safety functions designed to respond or for which the design of the systems performing the safety functions is inadequate to respond. These are usually MAIEs that are in the three classes, discussed in Section 4, that are not addressed in safety documentation.

4. A dependency table/spreadsheet among front line systems and support systems;

5. A dependency table/spreadsheet among support systems.

This information should be recorded in the appropriate VAI analysis document or record format and retained as VAI analysis documents or records. (See Section 3.5.) The systems identified in this activity are modeled in the facility sabotage fault tree.

4.3 Assessing System Requirements

This part of VAI begins to answer the question identified in Section 1.2, "What equipment must be disabled to disable the facility safety groups needed to respond to MAIEs?" The required performance of a front line system depends, in general, on the MAIE. Required performance of a front line system means the minimum performance needed for the successful fulfillment of the system's safety function under the specific conditions created by the MAIE. These success criteria for front line systems are of particular importance for the VAI analysis because they define the top events or starting points for the subsequent modeling of the system sabotage scenarios in the development of the facility sabotage fault tree branches[43] (see Sections 5.2 and A.2.3).

Success criteria can be defined unambiguously for front line systems for which clear success or failure in the performance of a safety function can be recognized. In addition to a performance definition (e.g., flow rate, response time, trip limits), the success criteria must be expressed in hardware terms, such as the number of required flow paths, power trains, etc.

Defining success criteria for support systems may be more complex. 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 function. A particular support system state could therefore lead to a safety function success or failure depending on the particular state of the front line system that it is supporting.

Relevant information for developing front line system and support system success criteria is given in facility safety analyses. PSAs generally provide realistic success criteria, while those derived from assumptions in DSAs may be conservative. If the VAI is based on a DSA, more realistic success criteria may be considered appropriate for use, if available from other safety documents or special analyses. These more realistic criteria should be supported by documented analyses that demonstrate their validity. Existing analyses for the particular facility or for other similar facilities can be used to derive success criteria that are more realistic than those derived from the assumptions in the facility DSA. These analyses should be clearly referenced in the documentation and should be included in the documentation if the references are not accessible.

In developing success criteria for front line systems, care should be taken to assess the effects of any special conditions that MAIEs create. Such special conditions may affect support systems,

[43] Because the potential adversary wants to disable the system, these top events are defined in a negative sense. That is, what malevolent acts must be accomplished to ensure that the success criteria are not met.

symptoms displayed to the operator, or automatic actuation systems as well as creating environmental conditions that cause additional systems to fail. For example, an arson fire may destroy not only the front line system in the location where the fire was started, but smoke from the fire may cause the failure of other "independent" front line systems or support systems. These special conditions should be used in grouping the MAIEs into equivalent classes.

Special analyses should be performed to develop more realistic system success criteria for VAI analyses when the possibility exists that the success criteria in DSA and other available safety documentation may be overly conservative. Realistically, such analyses are expensive and time consuming to perform—as expensive and time consuming as the VAI analysis, and should be undertaken only when the long-term physical protection benefits are likely to be commensurate with the costs of the analysis. Thus, sensitivity analysis of potential physical protection benefits are performed after the VAI analysis has been performed using the existing, more conservative system success criteria. This analysis should be considered if the VAI analysis identifies as vital locations for which protection is difficult, costly, or likely to have substantial adverse affects on safety or operations. In this case, the team should examine the systems being protected in these locations and do sensitivity analyses to determine whether less conservative success criteria or consideration of employing additional systems to perform the associated safety function are appropriate. Where plausible alternatives are identified, the fault tree model should be used to determine the effect of the alternative on the analysis results. If the results indicate significant possible long-term benefits, then a special analysis should be performed to determine whether the plausible alternative approach can, in fact, be technically justified.

This analysis produces a table/spreadsheet that lists the associated front line systems and support systems for each MAIE, as identified earlier (i.e., the safety group, as defined in Reference 2); their success criteria for that MAIE; references to supporting documentation; and any special characteristics of that MAIE that affect the success criteria. If a PSA has been done for the facility, the PSA documentation should provide this information for the MAIE for which corresponding safety IEs were analyzed. The table/spreadsheet developed should be documented in the appropriate VAI analysis document or record format and retained as a VAI analysis record (see Section 3.5).

4.4 Grouping of MAIEs

Once the system success criteria have been established, the MAIEs can be grouped so that all MAIEs in the same group require that front line systems and support systems meet essentially the same success criteria to prevent unacceptable radiological consequences and cause the same special conditions. Thus, the same sabotage fault tree branch can model sabotage scenarios beginning with any of the MAIEs in a group. Through the process of grouping, it will be clear that some categories of MAIEs need to be subdivided. For nuclear power reactors, one example may be the need to divide LOCAs by break size. Other categories of MAIEs may require similar division. If a PSA has been performed for the facility, the PSA documentation should contain the grouping of safety IEs, which can be employed for the MAIEs that correspond to safety IEs. Relatively few MAIEs do not correspond to safety IES, and 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 safety IEs from other safety documentation or another source. For example,

the groupings of safety IEs for boiling water reactors, pressurized water reactors, and CANDU reactors (provided in Reference 3) are an excellent starting point for grouping nuclear power reactor MAIEs. However, MAIE groupings depend upon the design of the facility, so groupings taken from other sources must be carefully validated to be certain that they are appropriate for the facility being analyzed. The MAIE that is used to represent the group in the subsequent sabotage fault tree development (typically the MAIE in the group that places the most stringent demands on safety systems), is defined to be the "bounding MAIE." The remaining MAIEs in the group are defined to be the "bounded MAIEs."

It is often useful to group together MAIEs that evoke the same general type of facility response but for which the front line system success criteria are not identical. The success criteria applied to this group should then be the most stringent for any member of the group. This introduces some additional conservatism, but generally has little effect on the analysis result. This simplification has no effect on the analysis result under the following circumstances: (1) one or more of the MAIEs in the specific group (e.g., loss of offsite power) may be initiated from outside the facility by a potential adversary; (2) the front line system and support system success criteria for at least one of these MAIEs is at least as stringent as those for the remaining MAIEs in that group.[44] Under such circumstances, this simplification may always be made when performing a VAI analysis.

With some insights into facility design, it may also be possible to do additional grouping to simplify the analysis for VAI. For example, although small and large LOCAs in nuclear power reactors actually require different front line systems for initial response, they can be grouped together into a composite LOCA MAIE for analysis of a nuclear power plant. This MAIE "requires" all of the front line systems required for both large and small LOCAs and has the most stringent of the system success criteria for the two classes of MAIE.

Care must be taken in making simplifications of this nature to ensure that important aspects of the behavior of the facility front line systems and support systems and possible credited recovery actions are not lost. In general, the possible simplifications described in the previous paragraphs are probably not worth the effort when a PSA is available to simplify the construction of the facility sabotage fault tree. However, they are worth considering when the only basis available for the development of the facility sabotage fault tree is a DSA and related safety documentation.

The result of this activity is the development of a set of bounding MAIEs and associated system success criteria that can be used for developing the facility sabotage fault tree. The VAI documentation should record the MAIEs that are "bounded" by the MAIEs used in the sabotage fault tree development. This record is needed to verify completeness and, as important, to ensure that when the bounding MAIEs are linked to locations, the location set includes those locations from which the potential adversary can accomplish the bounded MAIEs as well as those from which the bounding MAIE can be accomplished. The documentation developed should be in a suitable format and retained as VAI records (see Section 3.5).

[44] When MAIEs are linked to locations in the sabotage fault tree, the MAIEs that the potential adversary can accomplish from outside the facility are assumed to always occur because there is no onsite location that can be designated as vital to protect against them. (See Sections 6.2 and A.3.) Therefore, the areas containing the systems needed to ensure that these MAIEs do not create unacceptable radiological consequences must be designated as vital and protected. Once this is done the locations from which other on-site MAIEs that evoke the same general type of facility response (with front line system success criteria that are no more stringent than those for the MAIE that can be accomplished from offsite) need not be further considered with respect to this group of MAIEs.

This page intentionally left blank.

5. Sabotage Fault Tree Modeling

The second major step in performing VAI analyses is constructing a logic model (i.e., a fault tree) that models the set of possible sabotage scenarios for the facility that would lead to unacceptable radiological consequences. This completes the answer to the question identified in Section 1.2.1, "What equipment must be disabled to disable the facility safety groups needed to respond to MAIEs?" General sabotage scenarios are defined that consist of a bounding MAIE and malevolent acts to disable specific systems in manner that leads to unacceptable radiological consequences. These general sabotage scenarios are made more specific by modeling the disabling of systems in terms of representative malevolent acts to disable combinations of system components to prevent the system from meeting its success criteria. Representative malevolent acts to disable system components are modeled in sufficient detail to permit them to be linked to facility locations. However, these representative malevolent acts are generally surrogates for tens to hundreds of specific malevolent actions that a potential adversary could employ to disable the system component. The details of these various malevolent acts are considered when the representative malevolent acts are linked to locations in Section 6.

Because PSA models employ a combination of event trees and fault trees, the need for conversion of these logic models into a single sabotage fault tree may not be apparent where a PSA has been performed. However, there are two important VAI steps that most PSA software is not designed to perform on a combined event tree–fault tree model. The first of these is linking MAIEs (e.g., model IEs) to locations, as discussed in Section 6 and Section A.3. The second step is taking the Boolean complement of the sabotage fault tree model to derive a protection model, as discussed in Section 7 and Section A.4. Appendix A describes the way that these steps can be accomplished with virtually any fault tree analysis software. Where a PSA has not been performed, a sabotage fault tree can be constructed as described in Appendix A.

This sabotage fault tree is developed from information provided in the facility safety analysis and other safety documentation. Typically, this is accomplished in two stages. The first stage is developing the facility sabotage fault tree relating unacceptable radiological consequences to the bounding MAIEs and disabling front line systems. This is accomplished using information gathered in Section 4 and information from the facility safety analysis. The second stage is developing sabotage fault tree branches for individual front line systems and the support systems they are dependent upon. This activity is performed either by modifying existing fault tree models from the facility PSA, if one has been prepared, or by developing fault trees using facility system configuration information and the success criteria and dependency information developed in Section 4. The details of both stages of the construction of this fault tree are described in Section A.2.

This process produces a facility sabotage fault tree developed to the level of disabling of equipment, components, and devices. This sabotage fault tree links the bounding MAIEs and the disabling of equipment, components, and devices that are part of the front line systems and support systems that must respond to the bounding MAIEs to prevent unacceptable radiological consequences. This sabotage fault tree will have the MAIEs and the events in which equipment, component, and devices are disabled as basic events. The next stage in the analysis is identifying

and documenting facility locations from which the MAIEs can be initiated, and actions to disable equipment, components, and devices can be accomplished.

6. Collecting and Modeling Location Data

This next step in the VAI analysis process is identifying and documenting the locations from which a potential adversary could accomplish the set of MAIEs and malevolent acts that could disable the equipment, systems, and devices causing the failure of associated safety functions. This step answers the question identified in Section 1.2.1, "What plant areas must the potential adversary gain access to in order to perpetrate the MAIEs and disable equipment, shutting down the safety groups needed to respond to the MAIEs?" The information about these locations and areas is collected through a structured walkdown process described in Section 6.1.1. After the location information has been collected, it is entered into the facility sabotage fault tree as discussed in Section 6.2 and Section A.3. This sabotage fault tree can then be solved to determine the set of combinations of locations from which malevolent acts could cause unacceptable radiological consequences.

6.1 Collecting Location Data

The first step in collecting location data is to subdivide the facility into areas. Because some or all of these areas may be designated as vital areas, it must be practicable to provide them with the protection specified for vital areas in Reference 1. Therefore, it must be feasible to employ existing structures or new construction to establish a physical barrier around each defined area.[45] It must also be feasible to control access to each area and to minimize the number of entries to and exits from it,[46] and to alarm and to secure appropriately all points of access to the area.[47] To increase the effectiveness of data collection, these areas should be defined to be as small as feasible. The actual configuration of the vital areas will be determined based upon the analysis results. Therefore, the VAI team should consult with the organization responsible for physical protection system design when subdividing the facility into areas for VAI. Once the location data has been collected, it is possible to aggregate two or more locations into a larger area without collecting additional data. However, it is necessary to conduct an additional walkdown to split a larger area into two or more smaller areas. Thus, collection of location data is likely to be more efficient if performed on the basis of area divisions that are as small as could be feasibly designated as vital areas.

Once area divisions are established, they should be documented by marking them on facility elevation drawings or other facility design and layout documents to define clearly the area boundaries. Each area should be assigned a name and assigned an abbreviation that could be used as an event name in the computer software employed for fault tree analysis. To reduce errors in collecting location data, the area names should be as consistent with the names in common use at the facility as practicable. The documented names and abbreviations of areas and the definitions of area boundaries should be provided to each VAI walkdown team collecting information.

---

45 See Paragraph 7.2.12 of Reference 1.

46 See Paragraph 7.2.11 of Reference 1.

47 Ibid.

6.1.1 VAI Walkdowns

The main objectives of the VAI walkdowns are:

- To identify the set of areas from which a potential adversary could accomplish each bounding MAIE identified in Section 4.4, and the set of areas from which the potential adversary could accomplish each of the MAIEs that are "bounded" by the bounding MAIE.

- To identify the set of areas from which a potential adversary could accomplish each of the actions to disable equipment, components, or devices that are identified in the facility sabotage fault tree developed in Section 5.

As discussed in Section 3.2, a representative from the operating organization should serve as leader of the VAI walkdown team. At least one member of the team must be familiar with the design and operation of the system, equipment, components, or devices being walked down. This may require support from several technical disciplines, such as facility mechanical, electrical, and instrumentation and control engineering organizations. This may also necessitate a strategy of walking the facility down on a system by system basis rather than an area by area basis. The system by system basis walkdown will require fewer people on the team and maintain the team's focus on specific systems. However, that approach is likely to require that each area be walked down several times (one for each system in the area). The area by area basis walkdown requires larger teams (to address every system in the area) but walks down each area only once. It may also benefit from interaction among the representatives of the larger set of technical disciplines participating.

In preparation for the VAI walkdown, the team should be provided with appropriate drawings of the systems with components in the areas to be walked down.[48] Typically these will include piping and mechanical drawings, equipment layout drawings, and conduit layout drawings and other diagrams, as appropriate for the system being walked down. The team should also establish a standard approach for marking up these drawings to indicate which equipment, components, or devices are located in each area. Marking up appropriate drawings (e.g., piping and instrumentation drawings) has been found to be an efficient way of documenting information while walking down facility areas. Obviously, these drawing markups and the notes made while walking down the areas should be expanded and documented in a suitable format and retained as VAI records after the areas have been walked down (see Section 3.5). An example of the type of drawing markup that might be developed is shown in Figure 6-1. Where equipment locations have been documented in safety studies such as safe shutdown analyses and fire and seismic probabilistic safety analyses, it may be possible to prepare drafts of the VAI walkdown documentation before performing the VAI walkdowns. In such cases, the focus of the VAI walkdowns will be validating this data and considering possible malevolent acts that have no counterparts in the safety documentation.

[48] Information about the locations of system components, equipment, and devices for safety systems may be found in safety documentation, such as seismic safety analyses and fire safety analyses. Facility drawings and other facility design documentation may also identify the locations where system components, equipment, and devices are located.

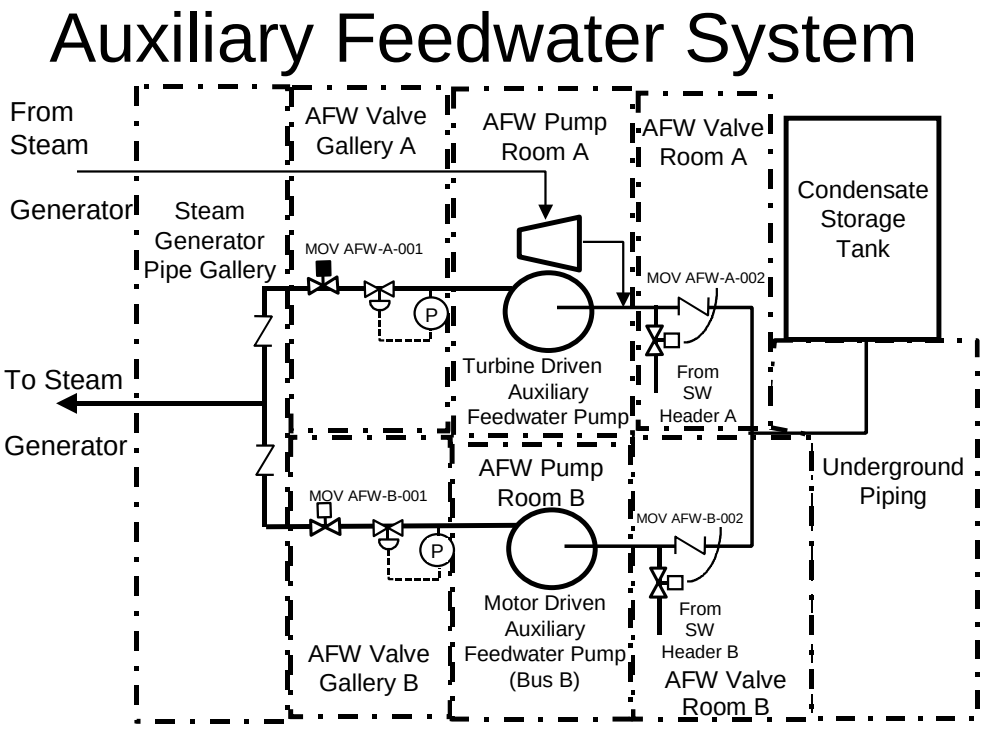

Figure 6-1. Example Drawing Markup

During the VAI walkdown, the team leader should orient the VAI walkdown team to the equipment, components, and devices in an area when the team enters. Team members should mark appropriate diagrams to indicate the items that are located in the area. The representative of the security organization should lead a discussion of the manner and areas from which these items could be disabled. If a location from which an item can be disabled is identified (that has not been previously established as an area), a new area should be established that contains this location. The team should look for ways that malevolent acts in other nearby areas could disable the item. These may include drainage paths from other areas where fluid line or tank breaches could flood the area, and airflow paths from which smoke, steam, or other environmental contaminants could enter the area. They may also include fire paths and combustible loading that might permit a fire to spread into the area if fire protection/suppression systems were disabled. Another way that malevolent acts could disable items in nearby areas would be to destroy related supports and structures that could directly cause items to fail or cause debris to strike the items disabling them. During the VAI walkdown, the team needs to be especially alert for these area linkages that are not evident from system diagrams (piping and mechanical drawings and conduit layout drawings may be good sources to identify some of these linkages). The VAI walkdown team should also be attentive to other ways of remotely disabling items, such as disabling motors and valves by cutting cables or from motor control centers.[49] However,

[49] When looking at remote disabling of valves, the team should determine whether a valve that has been placed remotely in the position that disables a system train could be restored to a position that would permit the system train to operate by local operator action. If that is the

these sabotage scenarios are more obvious and generally can be identified before the areas involved are walked down. The focus during the VAI walkdowns should be to validate the feasibility of these scenarios rather than to identify them.

The VAI walkdowns should also identify the areas from which a potential adversary could accomplish the MAIEs identified in Section 4.1. Although the main focus of this effort will be on the "bounding" MAIEs identified in Section 4.4, VAI teams should be careful to identify any "bounded" MAIEs that a potential adversary might be able to accomplish from areas other than those from which the corresponding "bounding" MAIE could be accomplished. In such cases, the walkdown team needs to document the linkage between these areas and the "bounding MAIE" so that the facility sabotage fault tree can correctly represent sabotage scenarios involving the "bounded" MAIEs.

In addition to walking down the facility areas identified in Section 6.1, the VAI walkdown team should walk the facility perimeter to identify any MAIEs or actions to disable equipment, components, or devices that can be accomplished by a potential adversary from outside the facility boundary. These should be documented in the same manner as the information collected during the VAI walkdowns of facility areas.

The result of this activity is documentation indicating which MAIEs and actions to disable equipment, components, or devices can be accomplished by a potential adversary from each area in the facility and from outside the facility. This documentation should be prepared as the VAI walkdowns are performed so that the information is fresh in the minds of the VAI walkdown participants. The entire VAI walkdown team should review the documentation for accuracy and completeness. This documentation should be prepared in a suitable format and retained as VAI records (see Section 3.5).

6.1.2 Data Preparation

The data collected in the walkdowns should be organized into a table or spreadsheet that lists the location(s) from which it can be accomplished for each basic event in the sabotage fault tree (i.e., each "bounding" MAIE or event in which equipment, components or devices are disabled). Where the disabling of an item is the result of an event that affects multiple areas (e.g., arson with the fire suppression system disabled), this should be noted. Likewise, the table should also include notes in the case that an area is linked to a "bounding" MAIE, not because the "bounding" MAIE can be accomplished from there but rather because a "bounded" MAIE can be accomplished from there. This documentation should be prepared in a suitable format and retained as a VAI record (see Section 3.5).

case, then the decision whether to include remote disabling of the valve in the facility sabotage fault tree should be made based upon the considerations, discussed in Sections 2.7 and A.2.3.3, related to crediting operator action.

6.2 Incorporating Location Data in the Sabotage Fault Tree

Incorporating location information into the facility sabotage fault tree links the MAIEs and the acts of disabling equipment, components, or devices that are already represented in the sabotage fault tree, with the locations from which they can be accomplished. This is accomplished in a slightly different manner depending upon whether:

1. the equipment can be disabled, or the MAIE accomplished, from one or more on-site locations, without the initiation of an event that affects multiple areas.

2. the equipment can be disabled, or the MAIE accomplished, through a sabotage scenario affecting equipment in multiple areas (e.g., an arson fire with the fire suppression system disabled); or

3. the equipment can be disabled, or the MAIE accomplished, from off-site (i.e., outside of the locations under the physical protection control of the facility). An example of a MAIE that can be accomplished from off-site would be isolating the facility from the electrical grid. An example of disabling a component from off-site would be breaching a water or fuel storage tank with a light anti-tank weapon.

The methods employed for these three situations reflect the differences in the ways that the corresponding sabotage scenarios can be protected against. In the first case, protecting the locations from which the MAIEs can be accomplished or the equipment can be disabled prevents the malevolent act. In the second case, there may be an additional system involved, such as the fire suppression system in the example. This additional system needs to be included in facility sabotage fault tree, so that the VAI results will include the option of protecting it. In the third case, the on-site physical protection measures generally will not provide protection against such a malevolent act.[50] Therefore, the facility sabotage fault tree needs to be constructed in a way that will require the protection of those systems needed to respond to the malevolent act and their support systems in order to prevent unacceptable radiological consequences. Detailed fault tree analysis techniques for incorporating the location information into the facility sabotage fault tree are described in Section A.3.

The result of this task is a modified facility sabotage fault tree that links the MAIEs, acts to disable items, and malevolent acts affecting multiple locations with the locations from which they can be accomplished. Depending upon this PSA software, this may be accomplished by some type of linking table or by modifying the sabotage fault tree itself so that:

1. All bottom level events are either basic events or house events, and

2. All basic events are area locations.

[50] In some cases, it may be possible to employ physical protection measures to prevent equipment from being destroyed from off-site. Typically, these measures include hardening of the components, providing shielding against stand-off weapons, or reconfiguring the protected area or site. These measures usually differ from those required for vital areas in Reference 1. However, where such measures are feasible, they should be considered and evaluated for cost-effectiveness in facility physical protection system design.

The sabotage fault tree model should be preserved in electronic format (e.g., as an input file or set of input files to the fault tree software program) and retained as a VAI analysis record (see Section 3.5).

This page intentionally left blank.

7. Identifying Candidate Sets of Vital Areas

This part of VAI answers the question identified in Section 1.2, "What are the minimum sets of areas (referred to as candidate vital area sets) that, if protected, will prevent the potential adversary from carrying out any combination of MAIEs and disabling of safety groups that would cause unacceptable radiological consequences?" Identifying candidate sets of vital areas is accomplished in two stages. First the facility sabotage fault tree is solved to obtain minimal cut sets, each of which identifies a combination of areas from which malevolent acts could cause an unacceptable radiological release. The process for accomplishing this first step is detailed in Section A.4.1. The combinations of areas from which malevolent acts could cause an unacceptable radiological release can be useful in configuring and evaluating the facility physical protection program. These combinations of areas can be reviewed to identify potential adversary targets as a basis for development of sabotage scenarios for physical protection program design and evaluation. These area combinations should be documented in the VAI report, which should also briefly discuss the MAIEs and acts to disable systems that are associated with area combinations. This can be most effectively accomplished by grouping the area combinations by the underlying MAIE and mitigating systems disabled. In order to prevent malevolent acts leading to an unacceptable radiological release, the facility must protect at least one area in each of these area combinations. The next step in the process is a systematic method for identifying possible combinations of areas to be protected.

The second step is to take the Boolean complement of the facility sabotage fault tree (referred to in Reference 7 as the dual of the fault tree). This Boolean complement of the facility sabotage fault tree is referred to as the facility protection location tree, because it identifies the equipment and areas that can be protected to prevent unacceptable radiological consequences. The facility protection location tree is solved to identify minimal path sets (as indicated in Reference 7, the minimal cut sets of the Boolean complement of a fault tree are referred to as minimal path sets). The process for accomplishing this step is detailed in Section A.4.2. Each of the minimal path sets in the solution of the facility location protection tree identifies a set of areas that contain the minimal complement of equipment, systems, or devices that, if protected against sabotage, will prevent unacceptable radiological release. Thus, each of these sets is a candidate for the set of vital areas that contains the minimum complement of equipment, systems, or devices to be protected against sabotage. Protection of each area in any one of these sets provides protection of the minimal complement of equipment, systems, or devices that, if protected against sabotage, will prevent unacceptable radiological release. The collection of candidate vital area sets is the product of this stage in the VAI process.

This page intentionally left blank.

8. Selecting Vital Areas

This final stage of VAI analysis answers the question identified in Section 1.2.1, "Which of the candidate vital area sets is it best to designate as the set of facility vital areas?" The final selection of vital areas is typically accomplished as a part of physical protection system design rather than as a part of the VAI analysis. Typically, this stage of the VAI includes close coordination with the facility organization responsible for physical protection system design and the VAI report provides recommendations in this area, but does not actually select a vital area set. The VAI report and supporting documents should also provide sufficient supporting information to serve as a resource for the facility physical protection system design organization. The entire process for selecting the set of vital areas is discussed here for completeness, recognizing that the activities performed during the VAI and those conducted as a part of physical protection system design will depend upon facility-specific considerations. These considerations include the design of the facility, the facility life-cycle stage in which the VAI is being conducted, and the feasibility of making of significant configuration changes as a part of physical protection system design. These considerations highlight the close, natural inter-relationship between VAI and physical protection system design.

This stage of the VAI / physical protection system design consists of the actual selection of one of the candidate vital area sets to serve as the basis for the set of areas designated as facility vital areas. Considerations that apply to the final selection of areas to be designated as vital fall into two basic categories: (1) considerations that relate to the selection of a set of areas from the facility protection location tree minimal path set; and (2) considerations for the addition of areas to the selected minimal path set to increase the number of vital area barriers that a potential adversary must overcome to cause unacceptable radiological consequences (i.e., to increase defense-in-depth). Although considerations in these two categories are discussed separately below, they should be jointly considered in the selection of vital areas. That is, the considerations discussed in Sections 8.1 and 8.2 should be addressed in a combined or an iterative fashion to select a set of vital areas that is best from all of the perspectives described in both sections.

8.1 Path Set Selection Considerations

Each of the minimal path sets of a facility protection location tree meets the recommendation in Section 7.1.5 of Reference 1 for a set of facility vital areas. Thus, the reasons for selecting one set over another relate to factors other than selecting areas that contain "the minimum complement of equipment, systems, or devices to be protected against sabotage." Major considerations in the selection of one of the minimal path sets as the set of vital areas include the following:

1. Ease, effectiveness, and cost of protecting the vital areas;

2. Impacts on safety and emergency response; and

3. Reliability of protected components, equipment, and devices.

It is unlikely that one candidate vital area set will receive the highest rating in each of these areas. Thus, it will be necessary to make trade-offs between the ratings in the various areas and select the candidate vital area set that is the overall best choice. This can be done using engineering judgment, or a more structured analytical approach can be employed. Reference 9 describes the multi-attribute utility theory technique for making such decisions. Reference 10 describes the analytical hierarchy process, which is another analytical technique for structured decision making and analysis of alternatives. Either approach provides a structured method for choosing alternatives. The following sections provide more detailed discussions of the three major considerations in selecting one minimal path set as the set of facility vital areas.

8.1.1 Ease, Effectiveness, and Cost of Protection

Recommendations for measures to protect vital areas are discussed in Sections 7.2 and 7.3 of Reference 1. It may be easier or less expensive to apply these protection measures to the areas in one minimal path set (candidate vital area set) than to those in another. The following examples illustrate considerations that should be applied in rating candidate vital area sets with respect to the ease, effectiveness, and cost of protection. Paragraph 7.2.11 of Reference 1 recommends that vital areas not be sited near public thoroughfares. Accordingly, preference should be given to candidate vital area sets that do not contain areas close to public thoroughfares or the boundary of the facility's site. In general, preference would be given to candidate vital area sets that did not contain structures that are separated from the main facility buildings (e.g., the intake structure of a nuclear power reactor). Paragraph 7.2.3 of Reference 1 recommends that access to vital areas be kept to a minimum. Accordingly, preference should be given to candidate vital area sets for which the minimum number of facility personnel require routine access. Paragraphs 7.2.3 and 7.2.11 of Reference 1 recommend that the number of entries and exits to vital areas be minimized. Accordingly, preference should be given to candidate vital area sets that have the minimum number of entries and exits, or for which the number of entries and exits can be minimized without unduly affecting facility and worker safety and facility operations. Paragraph 7.2.12 of Reference 1 recommends that vital areas provide penetration delay. Accordingly, preference should be given to candidate vital area sets with the most substantial walls and other barriers, or where penetration delay can be increased with minimal effect on facility safety and operations at reasonable cost. Paragraph 7.2.7 of Reference 1 recommends that operators monitor equipment, systems, and devices in vital areas to detect tampering. Accordingly, preference should be given to candidate vital area sets containing vital equipment where tampering can be readily detected.

Other protection cost and effectiveness issues not specifically related to the recommendations in Reference 1 include, for each candidate vital area set:

1. the estimated cost of installing required physical protection measures; and

2. the feasibility of establishing tactical positions to preclude potential adversary entry into the vital areas.

The review for ease, effectiveness, and cost of protection should be documented in a systematic manner using a table or spreadsheet. The table/spreadsheet should show how the candidate vital

area sets score against each of the physical protection considerations related to the Reference 1 recommendations as well as any additional physical protection considerations deemed significant by facility management or the competent authority. The scoring process can be developed based upon engineering judgment, multi-attribute utility theory, the analytical hierarchy process, or another established method.

8.1.2 Safety and Emergency Response Impacts

Selecting a candidate vital area set can affect facility and personnel safety and emergency response in three ways. First, the access control measures recommended for vital areas can degrade emergency response by lengthening the time required for operators to reach facility equipment in vital areas. Although mitigating actions can be taken (e.g., dropping vital area access controls during an emergency), this may actually aid a potential adversary by granting him access to the remainder of the facility once he has initiated a sabotage scenario. Therefore, in selecting vital areas, preference should be given to candidate vital area sets for which access controls would not unduly impede operator emergency response actions. This may be accomplished by selecting candidate vital area sets containing areas to which operators would need to respond in only a very small number of emergencies or areas to which rapid operator response was not generally required. If a PSA has been performed, the effects of controls on candidate vital areas can be incorporated into the PSA recovery analysis to obtain qualitative and quantitative insights regarding the effect of the selection of specific vital area sets on accident risk.

Second, physical protection access controls can degrade personnel safety by hindering personnel evacuation in an emergency. This concern is less serious than the previous one because it can largely be eliminated by the use of appropriate access control hardware (e.g., crash bar doors) that does not impede emergency evacuation. However, care must be taken in limiting the number of exit and entrances to vital areas that the personnel exit paths do not become so long or so complex as to preclude safe egress in an emergency. Therefore, in selecting vital areas, preference should be given to candidate vital area sets for which minimization of entrances and exits would not unduly impede personnel egress during an emergency. In evaluating impediments to emergency egress, the VAI team should consider the accident environment (e.g., lighting, visibility, and walking surfaces) under which personnel may need to exit an area.

Third, physical protection measures may require the use of firearms to prevent a potential adversary from entering a vital area. Discharging firearms in a nuclear facility can pose a number of hazards to facility and personnel safety. The hazards to facility safety include inadvertent disabling of equipment or instrumentation. The hazards to personnel safety include rupturing of lines containing hazardous materials (e.g., steam, acids, caustics, or pressurized water or chemicals). These hazards should be reviewed in the development of tactics to respond to attempted or actual intrusions into vital areas and the configuration of defensive positions. As discussed in Section 1.1.3, the discussion of protection measures is beyond the scope of VAI. Nevertheless, in the selection of vital areas, preference should be given to candidate vital area sets for which the hazards associated with firearm discharges are less serious or can be minimized without undue impact on facility operations or safety.

Here again, the review should be documented in a systematic manner using a table or spreadsheet. The table/spreadsheet should show how the candidate vital area sets score against each of these considerations as well as any additional similar considerations deemed significant by facility management or the competent authority. The scoring process can be developed based upon engineering judgment, multi-attribute utility theory, the analytical hierarchy process, or other established method.

8.1.3 Component, Equipment, and Device Reliability

Where facilities have diverse means of accomplishing safety, the systems in different candidate vital area sets may have different reliability. In such cases, preference in the selection of vital area sets should be given to candidate vital area sets that contain higher reliability systems. This reduces the likelihood that the systems protected in vital areas would experience random failure concurrent with a malevolent act.

This review should be added to the table/spreadsheet used to document the reviews of the other considerations.

8.1.4 Results

The results of this analysis are the following:

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 rating of each of the candidate vital area sets.

2. A recommended vital area set with the best score or rating.

8.2 Additional Possible Vital Areas

The minimal path set identified in Section 8.1 meets the recommendations in Section 7.1.5 of Reference 1 for a set of facility vital areas. The method by which the vital areas were identified is structured to ensure that a potential adversary will need to overcome at least one vital area barrier in order to cause unacceptable radiological consequences. This section addresses the feasibility and desirability of augmenting the set of vital areas with additional areas so that a potential adversary will have to overcome more than one vital area barrier to cause unacceptable radiological consequences. In general, there will always be some situations in which a potential adversary can commit acts that result in unacceptable radiological consequences in a single area. In nuclear power reactors, these areas typically include reactor containment and the control room. Obviously designating additional areas as vital areas will not increase the number of vital area barriers that a potential adversary must penetrate to cause release from these areas. However, it can increase the number of vital area barriers that a potential adversary must penetrate to cause releases from other facility areas. The following two approaches can be taken to augment the initial vital area set:

1. Include accident management equipment.

2. Include both areas where MAIE(s) can be initiated and those where response systems can be disabled.

These are discussed separately below.

8.2.1 Accident Management Equipment

Paragraph 5.31 of Reference 2 requires that the design of nuclear power reactors incorporate measures for mitigating severe accidents. These accident management measures may involve use of some systems (i.e., safety systems and non-safety systems) beyond their originally intended function and anticipated operational states and use of additional temporary systems to return the facility to a controlled state or to mitigate the consequences of a severe accident. The designs of nuclear facilities other than power reactors may also include such features. Typically, many of these systems would not be considered in the VAI analysis because they are not the systems relied upon to prevent or mitigate design basis accidents. The accident management measures should be reviewed to determine whether it is prudent to expand the set of vital areas to include the areas where they are located. Note that the accident management measures that perform a specific safety function should not be protected in lieu of the safety system(s) relied upon to perform that safety function. Rather, consideration should be given to the feasibility and benefit of protecting the accident management measures in addition to the corresponding safety systems. In augmenting the vital area set, care should be taken to include all accident management measures required to perform a specific safety function. In determining whether to augment the vital area set in this manner, the applicable factors discussed in Sections 8.1 and 8.2.3 should be considered. These considerations should be documented as necessary to demonstrate that adequate consideration has been given to augmenting the vital area set to include areas containing accident management measures and to present the rationale for the decision reached.

8.2.2 MAIE(s) and Response Systems

For those sabotage scenarios in which a potential adversary requires access to an area on site to accomplish an MAIE and the MAIE is not beyond the capability of the front line systems to mitigate, the candidate vital area sets may provide two options for protection against the sabotage scenario: (1) include the areas where the MAIE can be accomplished in the candidate vital area set; and (2) include, in the candidate vital area set, the areas needed to maintain the capability of the front line systems and support systems needed to mitigate the MAIE. Consideration may be given to designating both of these sets of areas as vital to achieve greater physical protection defense-in-depth.[51]

[51] These augmented candidate vital area sets can be derived by modifying the facility protection location tree, replacing the OR gates that link the MAIEs and front line systems with AND gates. The minimal path sets of this modified facility protection location tree will contain both the locations from which the MAIEs can be accomplished and the locations from which the associated front line systems can be disabled.

Alternatively, consideration may be given to designating as vital two or more (if there are more than two) of the redundant trains of the front line systems and support systems that could serve to mitigate the MAIE to increase redundancy.[52] Obviously, this will be of limited effectiveness when there are single areas from which both redundant trains can be disabled. In facilities where there is substantial physical separation of these redundant trains (e.g., the redundant trains are located in separate structures) this approach may form the basis for using zoned access controls to enhance protection against the insider threat. The zoned access controls could be structured to prevent a single individual from having access to all trains of the front line systems and support systems. Alternatively, the zoned access controls could be structured to prevent a single individual from having access to both the locations where an MAIE could be accomplished and the locations from which the corresponding front line systems or support systems could be disabled. In determining whether to augment the vital area set in this manner, the applicable factors discussed in Sections 8.1 and 8.2.3 should be considered. These considerations should be documented as necessary to demonstrate that adequate consideration has been given to augmenting the vital area set to include areas containing accident management measures and to present the rationale for the decision reached.

8.2.3 Other Vital Area Designation Considerations

Initial appearances indicate that increasing the number of vital areas increases the level of protection against sabotage resulting in unacceptable radiological consequences. More equipment is protected by being in vital areas, providing the facility with additional options to respond to sabotage attempts. However, frequently, as the number of vital areas increases, the level of protection afforded each individual vital area decreases. Consider, for example, a facility that declares all areas within the protected area to be a single vital area. This vital area contains all facility equipment important to safety. However, by moving the vital area access controls, physical barriers, and intrusion detection out to the protected area, the physical protection benefits of designating vital areas have largely been lost. Indeed, the physical protection measures at such a facility are very similar to what they would be if there were no vital areas at that facility. In other words, when everything is vital, nothing is vital. Thus, the main purpose of identifying vital areas is to focus physical protection measures and attention on those areas that require protection in order to protect against malevolent acts by a potential adversary that could cause unacceptable radiological consequences. Increasing the number of vital areas beyond the minimum set of areas that require protection for this reason may dilute the focus of physical protection measures and attention and ultimately reduce actual overall physical protection effectiveness.

The VAI analysis team needs to be aware of this trade-off when identifying vital areas. The team member representing the physical protection organization should take the lead in working with the physical protection system design organization to analyze any decrease in the effectiveness of individual vital area barriers and intrusion detection measures that may occur as

[52] These augmented candidate vital area sets can be derived by modifying the facility protection location tree, replacing the OR gates that link the various trains of the front line systems with AND gates. Note, if the facility protection location tree was derived from a sabotage fault tree that accounted for maintenance or random equipment failures concurrent with malevolent acts, as discussed in Sections 2.5 and 2.4, respectively, then multiple trains of redundant systems may already be protected. In that case, there is no need to modify the facility protection location tree in this manner.

the number of areas designated as vital areas increases (see Paragraphs 7.2.11 and 7.2.12 of Reference 1). This team member should also take the lead in working with the physical protection system design organization to analyze any decrease in response force tactical effectiveness that may occur as the number of areas designated as vital areas increases (see Paragraph 7.2.14 of Reference 1). The team member representing the operating organization should take the lead in analyzing increases in the number of facility personnel that will require vital area access as the number of areas designated as vital areas increases (see Paragraphs 7.2.9 and 7.2.12 of Reference 1). This team member should also take the lead in analyzing the increase in difficulty of having operators monitor all vital areas to detect tampering or interference with equipment as the number of areas designated as vital areas increases and the increase in effort required to accomplish operations and maintenance tasks (see Paragraph 7.27 of Reference 1). The team member representing the safety organization should take the lead in determining where adding areas to the vital area set would have greatest benefit to the facility in responding to MAIEs and preventing unacceptable radiological consequences. As stated in Section 1.1.3, the discussion of appropriate protection measures for vital areas and the design of physical protection systems is beyond the scope of the VAI analysis. However, the analysis team needs to be aware of the relationship between physical protection effectiveness and vital area configuration in order to achieve the primary objective of VAI: the identification of a set of facility vital areas that is most effective in protecting against malevolent acts by the potential adversary that could result in unacceptable radiological consequences.

8.2.4 Results

The results of this stage of the VAI analysis are the:

1. Documented considerations of options to include additional areas containing accident management measures in the vital area set;

2. Documented considerations of options to include additional areas in the vital area set to increase physical protection defense-in-depth; and

3. Recommendation for the set of vital areas to be identified for the facility and the rationale for this recommendation.

This page intentionally left blank.

9. Documenting Results

This step includes all aspects of documentation of the VAI analysis. "Documentation" here is understood in its broad sense; that is, related subjects that influence directly or indirectly the form and handling of the documentation are also considered. This discussion is mainly focused on the form of documentation of the analysis. The suggested format for the report is adapted from Reference 3. Three topics need to be addressed in the context of documenting the analysis.

9.1 Protecting Information

The analysis process, by its nature, generates information that could be quite valuable to a potential adversary. Accordingly, appropriate information protection requirements and procedures should be developed and applied to both the analysis report and other documentation generated during the course of this study. The specific nature of these requirements and procedures will depend upon the legal system in the state where the facility is located. These requirements and procedures should be established by the competent authority and the facility, as applicable, before the analysis begins. All team members should receive training in these measures as a part of the team training discussed in Section 3.3.

9.2 Objectives and Principles of Documentation

The primary objective of the analysis documentation is to demonstrate that the analysis meets the recommendations of Section 7.1.5 of Reference 1, and that it satisfies the requirements established by the competent authority of the state in which the facility is located. The analysis documentation should be well structured, clear, and easy to follow, to review, and to update. In addition, means should be provided for possible updates or extensions of the analysis. These include updates or extensions to reflect changes in the capabilities credited to a potential adversary that relate to the types of MAIEs it can accomplish and the locations from which it can accomplish MAIEs or disable facility components, equipment, or devices. These also include updates or extensions to reflect modifications to the facility, its operations, its safety systems and measures, and the locations of facility components, equipment, or devices. The documentation should explicitly present the assumptions made in the policy framework topics discussed in Section 2.

9.3 Organizing Documentation

The first step in organizing the analysis documentation is to determine the nature and amount of information that will comprise the analysis report. That is, what information will be published in the analysis report and what information will only be retained as internal documentation. This determination will depend, in part, upon the explicit and implicit documentation requirements established by the competent authority of the state in which the facility is located.

In the report (or by reference to available material), the documentation should provide all the necessary information to reconstruct the results of the analysis. Other documentation considerations may apply if the competent authority of the state in which the facility is located requires that the analysis report be submitted for review and approval. The facility management should have a clear understanding of the elements of the report that are viewed as facility commitments by the competent authority and that will require, their approval for changes. This can create difficulties if the competent authority requires, for its review, information addressing topics where the facility must be able to make changes for operational flexibility. In such cases, the facility and the competent authority must establish a process, which may include preparation of supplemental documents, so that the change control requirements on the VAI report do not unduly constrain facility operations. In this case, the VAI analysis report submitted for review and approval, in combination with the remainder of the submittal package, should supply sufficient information to permit the competent authority reviewer to reconstruct the analysis.

All intermediate analyses, assumptions, and other significant information that will not be published in the report or supplemental documentation should be retained as notes, working papers, or computer outputs. This is very important for future reconstruction and updates of the analysis. This information should be retained in the form of well-organized computer and word processor files, and a process established for updating this material to ensure that it remains accessible as computer media change over time and newer versions of computer programs are developed.[53]

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. That is:

    - Identification of MAIEs;
    - Facility level sabotage fault tree development;
    - System sabotage fault tree branch development;
    - Sabotage location determination;
    - Identification of area combinations from which malevolent acts can cause unacceptable radiological consequences;
    - Identification of candidate vital area sets; and
    - Recommendation of a set of vital areas.

[53] For example, data stored 15 years ago on 5.25-inch computer disks might be inaccessible today if it had not been migrated to different media. Likewise, word processor or fault tree analysis program data files might not be readable by the current versions of these computer programs if they are not periodically migrated to newer versions of the software.

The published documentation should be organized into the report and appendices or supplementary reports. The report should provide a clear and traceable presentation of the analysis, including:

- brief facility description,
- description of the VAI analysis method,
- MAIEs considered,
- facility sabotage fault tree development,
- sabotage location determination,
- candidate vital area sets, and
- vital areas recommended and the methods employed to develop the recommendation.

The appendices or supplemental reports should contain detailed data, detailed fault tree branch models, summaries of location walkdown results and assumptions, etc. While it is impossible to specify what detailed information should generally be provided in the appendices and supplementary reports, the functional and regulatory requirements for the report should provide the necessary guidelines (e.g., put information in the appendices or supplementary reports if the competent authority does not require that it be in the body of the report and most users will not need it or will not need to consult it regularly). The appendices or supplemental reports should be constructed to correspond directly to the section and subsections of the report to the extent practicable. An example outline of a report is shown in Figure 9-1.

I. Executive Summary

A. Introduction
B. Summary of Policy Framework Assumptions
C. Vital Areas Selected
D. Overview of VAI Method

II. Introduction

A. Purpose of VAI study
B. Scope of VAI study
C. VAI Analysis Team, Qualifications, and Training
D. VAI Method Summary
E. Report Organization

III. Policy Framework Assumptions

A. Assumptions Established by Competent Authority
B. Assumptions Established by Facility

IV. Facility Description

A. Overall Facility Characteristics
B. Facility Safety and Process Systems
C. Facility Layout

V. Identification of Sources of Radioactive Releases and Possible Malevolent Act Initiating Events

A. Radioactive Material Sources
B. Selection of Malevolent Act Initiating Events
C. Safety Functions And Associated Systems
D. System Requirements
E. Grouping of Malevolent Act Initiating Events

VI. Sabotage Fault Tree Development

A. Facility Sabotage Fault Tree
B. System Sabotage Fault Tree Branches

VII. Collection and Modeling of Location Data

A. Collection of Location Data
B. Incorporation of Location Data in the Sabotage Fault Tree

VIII. Identification of Candidate Sets of Vital Areas

A. Solution of the Facility Sabotage Fault Tree
B. Development and Solution of Facility Protection Location Tree

IX. Recommended Vital Areas

A. Recommended Path Set Selection
B. Additional Areas Recommended for Designation as Vital

Figure 9-1. Example VAI Report Outline

10. Conclusions

The method presented here provides a structured, logical approach to identifying the minimum complement of equipment, systems, or devices to be protected against sabotage, as recommended in Paragraph 7.1.5 of Reference 1. It identifies the risk acceptance policy decisions that must be made, either implicitly or explicitly, by the competent authority or individual facility in order to identify vital areas. The method provides for the selection and training of a team qualified to perform a correct and insightful analysis. The method incorporates information from facility safety documentation, including DSAs and PSAs in a structured and efficient manner that lends consistency to the protection against accidents and sabotage. It employs fault tree analysis to deal with the complexity of complex facilities and to document the logic employed in the identification of vital areas. The methodology also employs insights about the effectiveness of various physical protection options to select the set of facility vital areas that is most effective in protecting against malevolent acts by the potential adversary that could result in unacceptable radiological consequences. Finally, the recommended documentation approach provides the necessary information to reconstruct the results of the analysis. It also would enable a reviewer to determine the precise basis for the identification of specific facility areas as vital areas.

This page intentionally left blank.

References

1. INFCIRC/225/Rev. 4, “The Physical Protection of Nuclear Material and Nuclear Facilities,” International Atomic Energy Agency, Vienna, Austria, 1999.

2. NS-R-1, “Safety of Nuclear Power Plants: Design,” International Atomic Energy Agency, Vienna, Austria, 2000.

3. 50-P-4, “Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1),” International Atomic Energy Agency, Vienna, Austria, 1992.

4. NS-G-1.2, “Safety Assessment and Verification for Nuclear Power Plants,” International Atomic Energy Agency, Vienna, Austria, 2001.

5. GS-R-2, “Preparedness and Response for a Nuclear or Radiological Emergency,” International Atomic Energy Agency, Vienna, Austria, 2002.

6. Safety Series (SS) 115, “International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources,” International Atomic Energy Agency, Vienna, Austria, 1996.

7. NUREG-0492, “Fault Tree Analysis Handbook,” U.S. Nuclear Regulatory Commission, Washington D.C., USA, 1981.

8. 50-C/SG-Q, “Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations,” International Atomic Energy Agency, Vienna, Austria, 1996.

9. Keeny, R. L. and Raiffa, H., *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*, Wiley, New York, 1976.

10. Saaty, Thomas L., *Decision Making for Leaders,* Vol. II, AHP Series, RWS Publications, Pittsburgh, PA, 2001.

11. 1AEA-TECDOC-967 (Rev.1), “Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities,” International Atomic Energy Agency, Vienna, Austria, 2000.

This page intentionally left blank.

Glossary

Accident conditions — Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents. (Glossary of Reference 2.)

Accident management — The taking of a set of actions during the evolution of a beyond design basis accident:

- to prevent escalation of the event into a severe accident;
- to mitigate the consequences of a severe accident; and
- to achieve a long term stable state. (Glossary of Reference 2.)

AND Gate — A symbol indicating a relationship where the output event occurs if and only if all input events occur. (Adapted[54] from Reference 7.)

Anticipated operational occurrence — An operational process deviating from normal operation that is expected to occur at least once during the operating life time of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions. (Glossary of Reference 2.)

Area — For the purpose of vital area identification, a location that has four walls, a ceiling, and floor or any component, such as a motor control center or electrical rack, or location for which an enclosure or other means of providing penetration delay, access control, and intrusion detection could feasibly be constructed. (Adapted from paragraphs 7.2.11 and 7.2.12 of Reference 1.)

Basic event — An event that requires no further development for the specific fault tree. (Adapted from Reference 7.)

Boolean complement — The Boolean complement of a logical expression is the application of the logical NOT operator to that expression. The minimal cut sets of the Boolean complement of a fault tree are the events that need to be presented to prevent the top event from occurring. The Boolean complement of a fault tree is referred to as the dual of the fault tree and the minimal cut sets of the dual of the fault tree are referred to as the minimal path sets of the fault tree dual. (Adapted from Reference 7.)

Candidate vital area set — A minimal path set (or complement cut set) for a sabotage fault tree that incorporates equipment locations or the minimal path sets of a facility protection location tree. Sabotage cannot be accomplished unless the saboteur can enter at least one area in the protection set.

[54] Adapted definitions were developed where the cited source document used a term without providing an explicit definition of the term and no other readily available source documents contained an explicit definition of the term. The adapted definition is intended to reflect the definition of the term that is implicit in its usage in the referenced source document. There is no intent to revise or amend the definition in the referenced source document. The phrase “adapted from” simply means that the definition stated is implicit in the referenced document rather than explicit and therefore cannot be quoted. Where definitions are cited from sources without stating that they are adapted, the definition is drawn verbatim from the cited source.

Competent Authority — The organization(s) empowered under the legislative authority of a State to establish and ensure the proper implementation of the State's system of physical protection. If the elements of the State's system of physical protection are divided between two or more authorities, competent authority in this document refers to that authority responsible for establishing and ensuring the proper implementation of the requirements for VAI. (Adapted from paragraph 4.2.3.2 of Reference 1.)

Defense-in-depth — Safety: A concept, applied to all safety activities – whether organizational, behavioral, or design related – that ensures that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. (Adapted from paragraph 2.9 of Reference 2.)

Defense-in-depth — Security: A concept used to design physical protection systems that requires an adversary to overcome multiple obstacles, similar or diverse, in order to achieve his objective. (Paragraph 2.3 of Reference 1.)

Design basis accident (DBA) — Accident conditions against which a nuclear facility is designed according to established design criteria, and for which the damage to fuel and the release of radioactive material are kept within authorized limits. (Glossary of Reference 2.)

Design basis threat — The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is evaluated. (Paragraph 2.4 of Reference 1.)

Deterministic safety analysis (DSA) — A comprehensive, structured analysis that assesses the performance of the facility against a broad range of operating conditions, postulated IEs, and other circumstances, demonstrating that normal operation can be carried out safely, in such a way that facility parameters do not exceed operating limits. It can also demonstrate that, for anticipated operational occurrences and design basis accidents, the safety systems are able to fulfill the safety requirements in that they can:

- Shut down the reactor and maintain it in the safe shutdown condition during and after DBA conditions.
- Remove residual heat from the core after reactor shutdown from all operating states and all DBA conditions.
- Reduce the potential for release of radioactive material and ensure that any releases are below prescribed limits during operational states and below acceptable limits during DBA conditions.

It can also demonstrate that a degree of defense-in-depth is provided for beyond design basis accidents and severe accidents. (Adapted from paragraphs 4.8 through 4.105 of Reference 4.)

Event tree — A graphic model that orders and reflects events according to the requirements for mitigation of each group of IEs. Events or "headings" of an event tree can be a safety function's status, a system's status, basic events occurring, or operator actions. The event tree headings are normally arranged in either chronological or causal order. Chronological ordering means that events are considered in the chronological order in which they are expected to occur in an

accident. Causal ordering means that events are arranged in the tree so that the number of omitted branch points is maximized (i.e., the number of event tree branch points is minimized). (Adapted from paragraph 4.1.1 of Reference 3.)

Fault tree — A graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, maintenance or test unavailabilities or any other pertinent events that can lead to the undesired state. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, which is the top event of the fault tree. The top event and these basic events are linked by a complex of entities known as gates that show the relationships of events needed for the occurrence of a "higher" event (an event "nearer" to the top event). The gate symbol denotes the type of logical relationship (typically AND or OR) of the input events required for the output event. (Adapted from paragraph 4.2.1 of Reference 3.)

Fault tree solution — The solution to a fault tree is the complete listing of minimal cut sets for that fault tree.

Front line system — A system that directly performs a facility safety function. See also the definition of support system. (Paragraph 3.7 of Reference 3.)

House event — A primary event that is assumed either always to occur or never to occur. (Adapted from Reference 7.)

Initiating event (IE) — An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. Referred to in Reference 2 as a postulated IE. (Glossary of Reference 2.)

Item — A structure, system, or component. (Glossary of Reference 2.)

Malevolent Act Initiating Event (MAIE) — A malevolent act by which the potential adversary might initiate a chain of events leading to unacceptable radiological consequences.

Minimal cut set — A minimal cut set is the smallest combination of primary events (usually basic events) such that, if they all occur, will cause the top event to occur. In such a minimal cut set all of the primary events must occur for the top event to occur. (Adapted from Reference 7.)

Minimal path set (or minimal complement cut set) — A minimal path set is the smallest combination of primary events (usually basic events) such that, if none of them occurs, will prevent the top event from occurring. In such a minimal path set, each primary event must be prevented from occurring if the top event is to be prevented from occurring. The collection of minimal path sets for a specific fault tree dual may be obtained by taking the Boolean complement of the collection of minimal cut sets for that fault tree. (Adapted from Reference 7.)

OR gate — A symbol indicating a relationship where the output event occurs if and only if any of the input events occurs. (Adapted from Reference 7.)

Protection location tree — The protection location tree is the logical complement of the sabotage fault tree (sometimes referred to as the dual of the sabotage fault tree). This fault tree describes the systems, components, and locations that must be protected to prevent facility sabotage. The minimal path sets of this tree are candidate vital area sets.

Potential adversary — An individual or a group, some of whom may have authorized access to the facility (i.e., insiders), who might attempt sabotage. The term also refers to the attributes and characteristics of such individuals that relate to the types of malevolent acts that they are capable of once they gain access to areas within the facility. Where a design basis threat has been established, these attributes and characteristics are defined as a part of the design basis threat.

Protected area — An area under surveillance, containing Category I or II nuclear material, and/or vital areas surrounded by a physical barrier. (Paragraph 2.10 of Reference 1.)

Primary event — An event in a fault tree that has only an output. Typically primary events are basic events, undeveloped events, or house events. (Adapted from Reference 7.)

Probabilistic safety analysis (PSA) — A comprehensive, structured analysis that identifies accident scenarios and derives numerical estimates of risks. PSAs for nuclear power plants are normally performed at three levels as follows:

> **Level 1 PSA**, which identifies the sequence of events that can lead to core damage, estimates the core damage frequency, and provides insights into the strengths and weaknesses of the safety systems and procedures provided to prevent core damage.
>
> **Level 2 PSA**, which identifies the ways that radioactive releases from the plant can occur and estimates their magnitude and frequency. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures such as reactor containment.
>
> **Level 3 PSA**, which estimates public health and other societal risks, such as the contamination of land or food. (Adapted from paragraphs 4.123 through 4.126 of Reference 4.)

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 Reference 1.)

Sabotage fault tree — A fault tree that describes the ways in which systems and components can be disabled to sabotage the facility leading to unacceptable radiological consequences. This fault tree may incorporate the physical locations from which systems and components can be disabled. In this case, the sabotage fault tree minimal cut sets identify the combinations of areas from which sabotage resulting in unacceptable radiological consequences can be committed.

Safety group — The assembly of equipment designated to perform all actions required for a particular postulated IE to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded. (Glossary of Reference 2.)

Safety system — A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. (Glossary of Reference 2.)

Severe accidents — The very low probability event sequences, which may include multiple failures of safety systems leading to significant core degradation, that result in facility states, beyond design basis accident conditions, that may jeopardize the integrity of many or all of the barriers to the release of radioactive material. (Adapted from paragraph 5.1 of Reference 2.)

Sievert — A radiation dose equivalent to an absorbed gamma ray dose of one joule per kilogram. (Adapted from the definition of equivalent dose in Reference 6.) Sievert is abbreviated Sv and millisievert (.001 Sv) is abbreviated as mSv.

Special Component — An item that is challenged during a sabotage scenario or an accident sequence and that, if it fails to function properly, affects the number or type of front line systems required to prevent unacceptable radiological consequences. Typically, the responses of special components during accident sequences are shown on the event tree for an accident in a PSA that employs the small event tree/large fault tree modeling approach.

Success criteria — The minimum system performance that will allow for performance of the system safety function under the specific conditions created by an IE. (Adapted from paragraph 3.8 of Reference 3.)

Support system — A system required for the proper functioning of one or more front line system(s). (Paragraph 3.7 of Reference 3.)

Temporary Vital Area — An area that needs to be designated and protected as a vital area only when a system component or device is undergoing maintenance or is otherwise unavailable for a period of time in excess of an established de minimus period. The process for providing physical protection to a temporary vital area (i.e., activating the temporary vital area) should typically proceed as follows:

1. Area access controls, including physical barriers and intrusion detection systems, are activated (see Paragraphs 7.2.3, 7.2.11, and 7.2.12 of Reference 1);

2. The area is inspected by an operator to verify that no tampering or interference with vital equipment has taken place (See Paragraph 7.2.7 of Reference 1) and, where practicable, the operability of vital equipment is verified; and

3. If no tampering or interference has taken place or when the effects of any tampering or interference have been repaired, the vital area is considered activated.

Top event — The single event in a fault tree that does not input to another event. This is the specific undesired event that the fault tree relates to a set of primary events. The top event is almost always a gate and is customarily shown at the top of the fault tree. (Adapted from Reference 7.)

Unacceptable radiological consequences — A possible result of sabotage that is deemed, by the facility or competent authority, to be sufficiently serious that the facility for which VAI is being performed is required to employ special physical protection measures to protect against it.

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 consequences. (Paragraph 2.17 of Reference 1.)

Vital area identification (VAI) — The process of evaluating the consequences of malevolent 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 (vital items), by designating as vital the areas from which they could be sabotaged. (Adapted from Paragraph 7.1.5 of Reference 1.)

VAI walkdown — The process of systematically determining and documenting the areas from which identified MAIEs can be accomplished or equipment, systems, and devices that are part of front line or support systems can be disabled. The VAI walkdown concentrates on determining and documenting the areas from which each of the basic events of the facility sabotage fault tree can be accomplished.

Vital equipment — Nuclear material or equipment, systems, or devices that are important to safety, or the sabotage of which could lead to unacceptable radiological consequences. (Adapted from Paragraph 7.2.2 of Reference 1.)

Appendix A
Fault Tree Analysis Details

A.1 Introduction

This appendix provides detailed instructions for performing the fault tree model development and analysis necessary to identify vital areas. Section A.2 presents a detailed approach for constructing the sabotage fault tree model as described in Section 5. Section A.3 provides detailed guidance for incorporating location equipment into the fault tree model as discussed in Section 6.2. Finally, Section A.4 provides the details about how the fault tree model is to be transformed and solved to identify candidate sets of vital areas, as summarized in Section 7. The details presented in this appendix are designed to assist the VAI team in understanding the specific steps involved in constructing and solving the facility sabotage fault tree and the facility protection location tree to obtain candidate vital areas. In addition, the detail presented is intended to provide sufficient guidance to enable the expert in fault tree development and analysis who is supporting the VAI team to solve the difficulties and deal effectively with the complexities that arise in the analysis of complex nuclear facilities. The discussions in this appendix assume that the reader is familiar with basic probabilistic safety analysis (PSA) methods, terminology, and tools.

A.2 Facility Sabotage Fault Tree Development

The facility sabotage fault tree basically aggregates the set of sabotage scenarios that could cause unacceptable radiological consequences. The top event (first level) in the facility sabotage fault tree is "Sabotage with Unacceptable Radiological Consequences." The second level of facility sabotage fault tree events typically identifies the radioactive material locations from which radioactive material could be released to cause the unacceptable radiological consequences. For a nuclear power reactor, these could include the reactor core, the irradiated fuel storage, and the radioactive waste storage. These events are linked by an OR gate, because a potential adversary could cause unacceptable radiological consequences by releasing radioactive material from any of these locations.

The third level of the facility sabotage fault tree typically identifies the facility operating states being considered in the VAI (see Section 2.2). Once again, the events are linked by an OR gate, because a potential adversary could cause unacceptable radiological consequences by sabotaging the facility in any of the operating states considered.[55] For some sources of radioactive material the bounding malevolent act initiating event (MAIE) front line system combinations are the same for all of the facility operating states under consideration and this level of events may be omitted.[56] In such case, the fourth level events are linked directly to the second level events discussed above (i.e., the radioactive material locations).

---

55 This approach to VAI analysis results in the identification of a single set of vital areas that, if protected, will prevent unacceptable radiological consequences from sabotage attempts during any of the facility operating states considered. If the objective of the VAI analysis is to identify a set of vital areas for each facility operating state, different facility sabotage fault trees should be developed for each facility operating state. In this case, the top event would be sabotage with unacceptable radiological consequences during normal operations, etc.

56 An example would be explosive dispersal of spent fuel from the spent fuel pool. This is the reason that the radioactive material release locations are modeled at the second level of the facility sabotage fault tree. This has the potential to make the fault tree smaller and less complex.

Figure A-1 shows an example of the top three levels of the sabotage fault tree for a pressurized water reactor. The fourth level of the facility sabotage fault tree is developed from the bounding MAIEs and associated front line systems developed in Section 4. This level includes the bounding MAIEs that cannot be mitigated by facility front line systems. Each of the remaining bounding MAIEs appears in an event with the associated front line systems disabled.[57] For a nuclear power reactor, an example could be "Small Loss of Coolant Accident (LOCA) with Mitigating Systems Disabled." These events are linked by an OR gate because a potential adversary could cause unacceptable radiological consequences employing any of these sabotage scenarios. These events are further developed based upon the success criteria developed in Section 4.3. The simplest technique for the further development of these events depends upon whether a PSA has been performed for the facility. The technique for preparing this part of the facility sabotage fault tree from PSA is discussed in Section A.2.1. Section A.2.2 provides a description of the technique for preparing this part of the facility sabotage fault tree from a deterministic safety analysis (DSA). The general techniques for constructing and manipulating fault trees are described in Reference 7.[58]

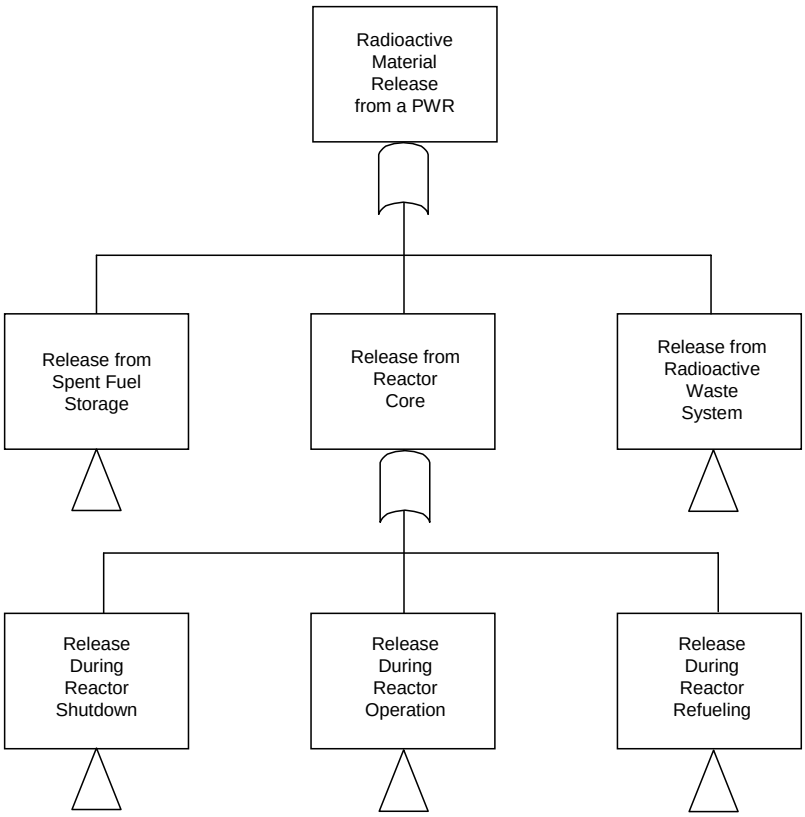

Figure A-1. Example of Top Three Levels of Pressurized Water Reactor Sabotage Fault Tree

57 There will probably be some MAIEs that the front line systems are incapable of mitigating; that is, MAIEs that exceed the design bases of the front line systems. These MAIEs are included at this level as events that lead directly to unacceptable radiological consequences without other systems being disabled.

58 NUREG-0492, Fault Tree Handbook, is cited in Paragraph 4.2.1 of IAEA 50-P-4, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), as describing the "general techniques for constructing, manipulating, and quantifying fault trees."

A.2.1 Using PSA Event Trees in Developing the Sabotage Fault Tree

If a PSA has been performed, the PSA event trees illustrate the combinations of safety initiating events (IES) and front line system failures that cause specific facility damage states.[59] This information is used in developing portions of the facility sabotage fault tree in the following three basic steps:

1. For each bounding MAIE that has a corresponding safety IE, review the event tree that illustrates the facility response to the IE.

2. If several facility damage states fall within the definition of unacceptable radiological consequences, the event tree should be simplified by aggregating those facility damage states that meet the definition of unacceptable radiological consequences. After these end states have been aggregated, then the event tree should be simplified by removing branching events where both branches lead to the same state; i.e., unacceptable radiological consequences. (See Figures A-2, A-3, and A-4 for an example. In this example, core damage is defined as unacceptable radiological consequences so both core damage and radiological release from the core meet the criteria for unacceptable radiological consequences. Figure A-3 shows the event tree shown in Figure A-2 with aggregated facility damage states. Figure A-4 shows the event tree in Figure A-3 with the branching event containment integrity removed since both branches lead to the unacceptable radiological consequences state.)

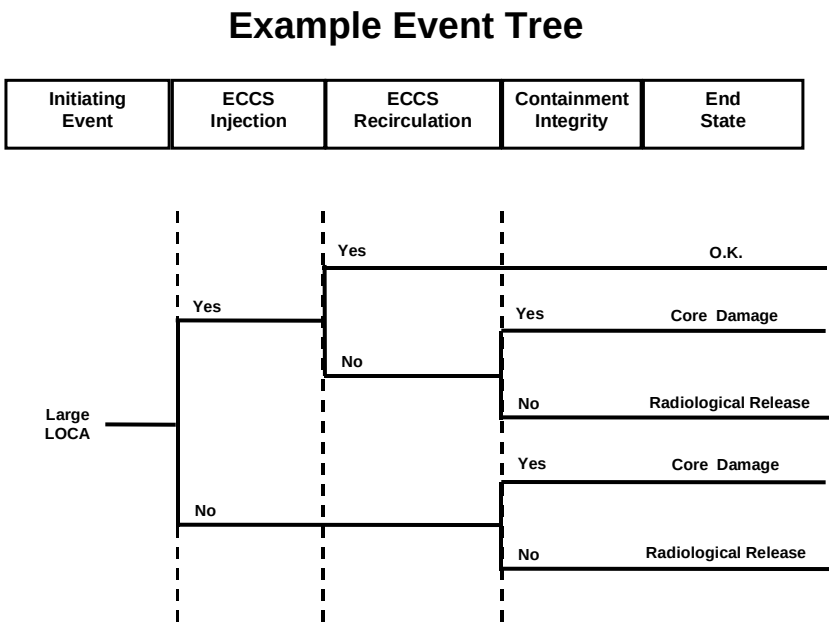

Figure A-2. Example of Event Tree

59 For a discussion of event trees and their use in PSA, see Section 4.1 of Reference 3.

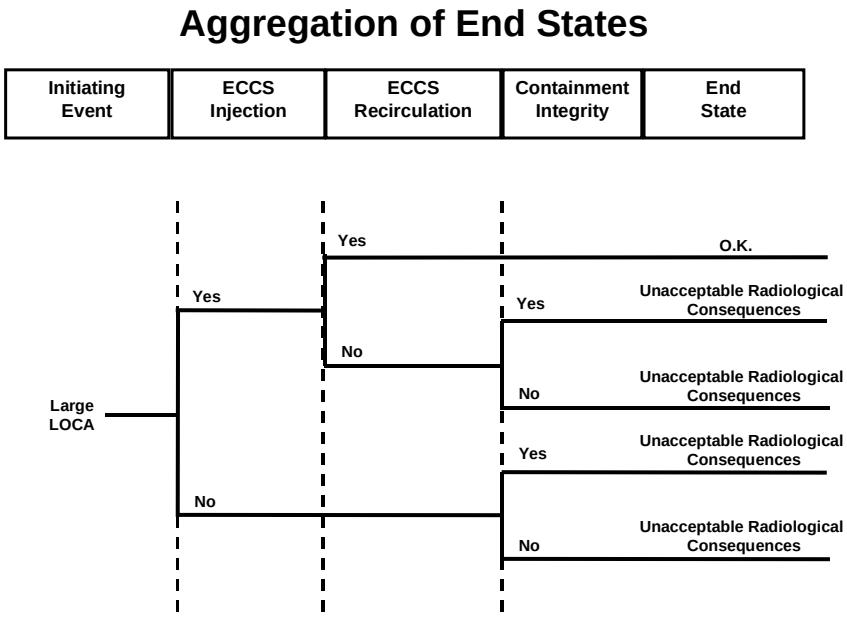

Figure A-3. Event Tree With Aggregated Facility Damage States

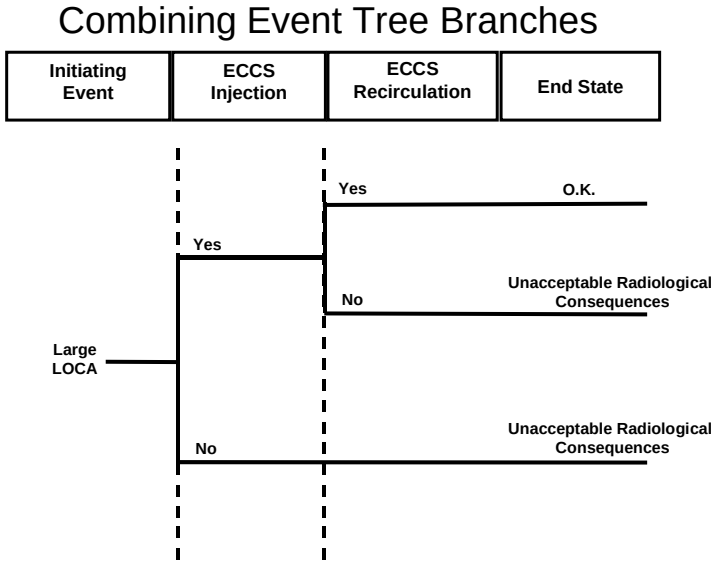

Figure A-4. Event Tree With Branching Event Containment Integrity Removed

3. Once the event trees have been simplified, convert them into fault tree branches by linking together the various event tree branches leading to unacceptable radiological consequences with an OR gate and then linking the events along each of the branches with an AND gate.[60] (Figure A-5 illustrates the fault tree branch constructed from the simplified event tree in Figure A-4.) For VAI analysis, the sabotage fault tree branch in Figure A-4 can be simplified further by combining the events "Disable ECCS Start" and "Disable ECCS Run" into a single event "Disable ECCS." When the fault tree for this event is developed, as discussed in Section A.2.3, care needs to be taken to ensure that the sabotage actions that would disable the start of the ECCS and keep it from running are both modeled. If the PSA from which the VAI analysis is being developed contains fault trees for both "ECCS Fails to Start" and "ECCS Fails to Run" it may be simpler to link and modify these fault trees, as discussed in Section A.2.3, than to develop a new, combined fault tree. These two approaches are logically equivalent and will not affect the VAI analysis results.

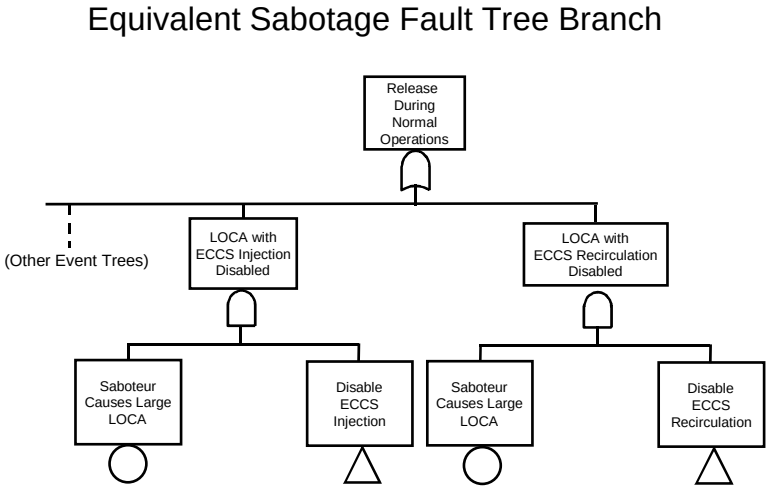

Figure A-5. Equivalent Sabotage Fault Tree Branch

These three basic steps are supplemented by two additional "rules" to address specific issues related to the differences between PSA graphic models of facility response and sabotage fault tree branches. The first "rule" relates to event tree branches that do not correspond to equipment failures. If the event tree contains branches that do not correspond to on-site equipment failures (e.g., operator recovery actions, human errors, or restoration of off-site power), determine which branch of the event tree is appropriate for sabotage modeling. Then, trim out the inappropriate branch and all branches coming off of it before developing the corresponding sabotage fault tree branches.[61] For example, if the event tree includes recovery of offsite power within a specific time period, the VAI team should determine, based upon the postulated adversary characteristics and facility contingency measures, whether the recovery of off-site power within the expected time is sufficiently likely that it should be credited. If this is the case, then the event tree branch

[60] The conversion of event trees to fault trees is usually necessary because of the limitations on PSA tools discussed in Section 5. If the PSA tools without these limitations are available, then the VAI can be accomplished employing an approach that uses both event trees and fault trees.

[61] These probabilistic events must be resolved into a deterministic sabotage scenario. Therefore, the VAI team needs to determine whether they will be credited as occurring during the sabotage scenario.

where off-site power is not recovered should be ignored when developing the sabotage fault tree branch. Similar considerations apply to operator recovery actions and human errors. These should be addressed in a manner consistent with the policies established in the topics discussed in Section 2.7.

The second "rule" relates to random failures of equipment concurrent with malevolent acts. The sabotage fault tree constructed in accordance with the rules given so far does not consider random failure of equipment in conjunction with sabotage events. If the policy decision is made to consider random equipment failures, with likelihoods above a probability cut-off, in conjunction with sabotage scenarios, as discussed in Section 2.4, the sabotage fault tree needs to be modified. There are several approaches that can be employed to account for random failures, depending upon the capabilities of the fault tree analysis software. In some cases, it may be possible to include both random failures and malevolent acts in the sabotage fault tree model and the fault tree analysis software can easily compute the Boolean complement of cut sets and path sets. If the fault tree analysis software can include random failures and readily take the Boolean complement of results that include random failures, these two capabilities then these features may be used to simplify this part of the analysis.[62]

If the fault tree analysis software does not have such features, then the following approach can be used. Identify from the PSA the random equipment failure events with probabilities in excess of the cut-off probability. The probabilities should be examined from the system level down. In other words, first assess the probability that a system will fail to operate due to random failure(s) to determine whether it exceeds the cut-off probability. If the failure probability at the system level does not exceed the cut-off probability, then assess the probability that one train of the system will fail to determine whether it exceeds the cut-off probability. In general, if the random failure probabilities of all of the trains of a system are below the cut-off probability, there is no need to review the failure probabilities of individual components within the system trains because random failures at this level will not affect the VAI analysis results.[63] Note that this analysis needs to include support systems as well as front line systems.

The one exception to this generalization is when a random failure of a component or device affects the progression of a sabotage scenario in a way that requires additional front line systems in order to prevent unacceptable radiological consequences. In this discussion, components of this type are referred to as special components. For example, during the facility response to a loss of off-site power transient, a pressurized water reactor may vent steam through the pressurizer power-operated relief valve (PORV). If the PORV malfunctions and sticks open, it provides a potential loss of coolant path if the flow cannot be stopped by closing the block valve. In this case, the stuck open PORV has created a small LOCA, which requires the small LOCA

---

62 If both malevolent acts and random events can be included in the sabotage fault tree model, then the malevolent acts should be represented by the locations from which they can be accomplished, as discussed in Section A.3, and assigned a "failure probability" of 1. Solution of the sabotage fault tree with a probability cut-off equal to the probability cut-off for random events established in Section 2.4 will yield the minimal cut sets for releases with unacceptable radiological consequences due to malevolent acts combined with random failures that are more likely than the probability cut-off. These minimal cut sets then need to be simplified by removing the random failure terms (assuming that they always occur; i.e., setting them to Omega) and doing a Boolean reduction. Taking the Boolean complement of these minimal cut sets yields the minimal path sets developed in Section A.4.2.

63 Because the potential adversary is assumed to be able to disable all equipment in an area once he gains access to it and it is virtually always possible to disable an entire system train from a single location, a random failure or combination of failures that does not disable the entire train does not reduce the number of areas to which a potential adversary would require access to cause unacceptable radiological consequences.

front line systems to respond, in addition to those needed for the loss of offsite power transient.[64] Fortunately, the circumstances where a random component failure could affect the progression of a sabotage scenario in this manner are relatively obvious because the failure creates an event tree branch. Thus, the event tree branches that do not correspond to failures of front line systems or trains also need to be examined to see whether the probability of the random failure of the special component(s) involved exceeds the probability cut off.[65]

Once the random system failures of front line systems or random special component failures whose failure probabilities exceed the probability cut-off have been identified, branches need to be added to the facility sabotage fault tree to reflect the possibility that these items will fail concurrently with a malevolent act. For a system failure, this is accomplished by adding a copy of each fault tree branch that includes disabling the system modified to assume that the system has failed (due to a random failure or fault). This fault tree branch is linked to the fault tree branch without the system failure by an OR gate.[66] For a special component failure, the fault tree branch that needs to be added is developed from the PSA event tree, as described above, but taking the event tree branch that corresponds to the failure of the special component (i.e., assuming that the special component fails). The random failure of the special component is not developed further in the facility sabotage fault tree because it is not part of the sabotage scenario.

Where the probability of random failure of a single train of a front line system, a support system, or a single train of a support system exceeds the probability cut-off, the possibility that these failures will occur needs to be reflected in the system sabotage fault trees discussed in Section A-2.3. In modeling these possible random failures, the team needs to take care to ensure that the sabotage fault tree does not inadvertently include multiple random failures, when the probability of such multiple random failures does not exceed the probability cut-off. This will be addressed further in the discussion of reflecting the possibility of random failures for the system sabotage fault tree branches in Section A.2.3.4.

If the PSA does not model all of the operating states being considered in the analysis, fault tree branches should be constructed for the operating states not modeled in the PSA employing the approach discussed in Section A.2.2. However, these fault tree branches should reflect any additional information about front line system performance and front line system success criteria that is available from the analyses performed as a part of the PSA.

The final result of this activity is a facility sabotage fault tree that is developed to the level of bounding MAIEs and the front line systems that a potential adversary must disable in combination with accomplishing the MAIE in order to cause unacceptable radiological consequences. The next stage in this activity is the development of the sabotage fault tree

---

64 This sequence of events is familiar from the accident that happened at Unit 2 of the Three Mile Island Plant near Harrisburg, Pennsylvania, in 1979. (See NUREG/CR-1250-V, "Three Mile Island: A Report To The Commissioners and the Public," United States Nuclear Regulatory Commission, Washington, D.C., 1980.)

65 Note that these random component failures affect the VAI analysis in a different manner than the disabling of the same component by the potential adversary. Disabling of the component by the potential adversary requires access to one or more plant areas and, therefore, can be protected against by designating these locations as vital areas. Security measures cannot protect against random component failures.

66 The approach of adding a new fault tree branch in which the system is assumed to fail randomly is employed instead of modifying the original branch to reflect the random failure. This approach is employed to ensure that such random failures are modeled to occur only if the failure would be to the advantage of the potential adversary, as discussed in Section 2.4.

branches for each front line system and the support systems upon which the front line systems depend. This is discussed in Section A.2.3.

A.2.2 Developing the Sabotage Fault Tree from DSA Information

If there is no PSA available for the facility, then the facility sabotage fault tree is developed from information in the facility DSA and other safety studies. The information developed in Section 4 about system success criteria and the linkages between MAIEs and the front line systems that must respond to the MAIEs to prevent unacceptable radiological consequences provides the information needed to construct the fourth level of the facility sabotage fault tree. (See the introductory material in Section A.2, from which this discussion continues.) In constructing this level of the fault tree, the MAIEs are linked to the disabling of these front line systems using AND gates. That is, the saboteur must cause an MAIE **and** disable the front line system that responds to it in order to create unacceptable radiological consequences. These various combinations of MAIEs and disabling front line systems are linked to the level above by an OR gate, since unacceptable radiological consequences will result if a saboteur succeeds in accomplishing any one of these combinations. Events containing all of the "bounding MAIEs" identified in Section 4.4 should be included at this level of the facility sabotage fault tree. Where multiple operating states are being modeled, care should be taken that the appropriate MAIEs and the disabling of the appropriate front line systems are modeled for each operating state.

The final result of this activity is a facility sabotage fault tree that is developed to the level of bounding MAIEs and the front line systems that a potential adversary must disable in combination with accomplishing the MAIE in order to cause unacceptable radiological consequences. The next stage in this activity is the development of the sabotage fault tree branches for each front line system and the support systems upon which the front line systems depend. This is discussed in Section A.2.3.

A.2.3 System Sabotage Fault Tree Branches

The next step in the VAI analysis is the construction of sabotage fault tree branches for each of the front line systems in the facility sabotage fault tree developed in Sections A.2.2 or A.2.3 and the support systems with which they have dependencies. (See Section 4.2.) These sabotage fault tree branches are similar to the corresponding fault trees used in PSAs. However, there are some differences because sabotage fault tree branches are designed to model sabotage scenarios while PSA fault trees model system failure logic. These differences between modeling sabotage scenarios and system failure logic affect the construction of the sabotage fault tree branches in the following manner:

1. System sabotage fault tree branches need to be comprehensive in identifying the locations from which items can be disabled, but need not reflect all item failure modes or all mechanisms for disabling the item.

2. System sabotage fault tree branches need to reflect sabotage events that are so unlikely to occur randomly that they need not be considered in PSAs, such as destruction of passive components.

3. Operator recovery actions and other events in PSA system fault trees that affect system availability, such as test and maintenance outages, but do not correspond to action in a sabotage scenario need to be treated in a special manner. These events need to be treated as events that can always be accomplished or as events that cannot be relied upon to occur during or in response to a malevolent act. (See the related discussions in Sections 2.7 and A.2.3.3.)

The implications of these three differences are discussed in the contexts both of developing system sabotage fault tree branches and of modifying PSA fault trees to develop system sabotage fault tree branches.

A.2.3.1 Location Focus

The VAI sabotage fault tree branches are designed to identify the locations from which a potential adversary can disable systems. Therefore, it is extremely important that the basic events in the sabotage fault tree branch be sufficiently comprehensive that the location linkages developed in Section A.3 reflect all locations and combinations of locations where a potential adversary could disable the system. On the other hand, there is no need for the system sabotage fault tree branch basic events to reflect all of the ways in which the system can be disabled from a single location. Therefore, the sabotage fault tree model is typically developed to the point where a piece of equipment, a component, or a device is disabled, but no further, so that the fault tree does not specify the means by which the item is disabled. However, when there are means of disabling an item from remote locations, the fault tree should be developed to show all of these remote means of disabling the item. Examples of means of sabotaging components from a remote location include disabling a valve from the associated motor control center or disabling a pump motor by cutting its control or power cable. These methods of disabling components should be shown in the system sabotage fault tree branches. Generic sabotage fault trees (see Section A.2.4) or reviews of VAI analyses for similar plants (see Section 3.3) can be helpful in ensuring that sabotage scenarios are not overlooked in the development of the system sabotage fault tree branches.

Therefore, PSA system fault trees can be simplified to develop system sabotage fault tree branches by combining multiple failure modes of a single component, such as “Component Fails to Start” and “Component Fails to Run,” into a single event, e.g., “Component Disabled.”[67] This single event should then be developed to show the areas from which the component can be disabled. Figure A-6 gives an example of the way that the sabotage fault tree branch for disabling a motor-driven pump is developed. (Note that this branch only includes the pump and does not include piping.) Likewise, events in a single area, such as manipulation of manual valves or check valves located in the same area as a pump, can be combined into a single event, such as disabling the pump locally.

[67] Alternatively, the fault tree can be left unmodified and the redundant events can be linked to the same locations or set to φ (i.e., a zero probability event that does not occur). This approach requires less fault tree manipulation but may reduce the clarity of the model. If the event name is unchanged, it may also obscure some of the possible sabotage scenarios complicating the location linking. Whichever approach is taken must meet the standard for clarity of fault tree model logic discussed in Section 3.5.

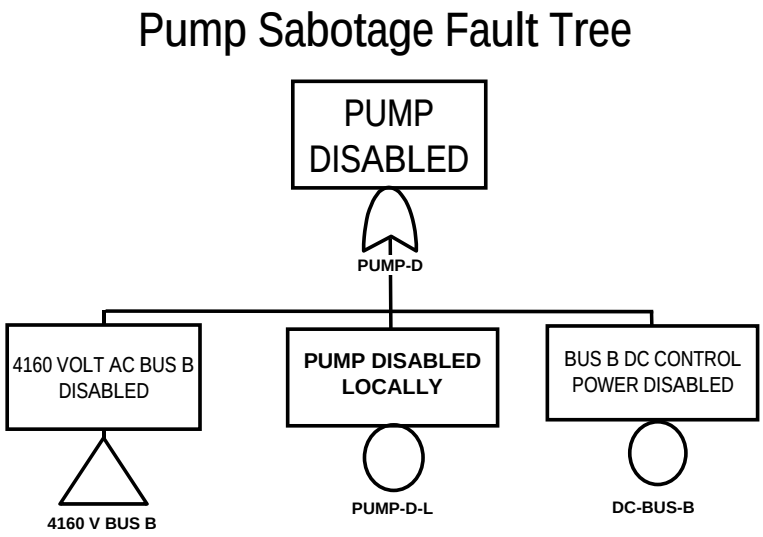

Figure A-6. Fault Tree Branch for Disabling a Motor-Driven Pump

A.2.3.2 Low Probability Events

The fault trees in PSAs are simplified by not including component failures of such low probability that they do not contribute to risk. However, a potential adversary may be able to intentionally cause such failures as a means of disabling a system. Failures of this type include spontaneous catastrophic failures of passive components. Thus it is necessary to add such malevolent acts as disabling a system by breaching piping, breaching tanks or reservoirs, and cutting cables.[68] For events in fluid systems where a piping is breached, it is also necessary to consider situations in which the breach creates an alternate flow path that seriously degrades or fails the system. In general, unless safety studies provide evidence to the contrary, if the pipe diameter of the diversion flow path is one third or greater than the pipe diameter of the primary flow path, then the system is disabled.[69] In addition, fluid from pipe breaches or tank ruptures may cause local flooding that disables or degrades the performance of nearby equipment.[70] Two additional events involving valve position are frequently not considered in PSAs: (1) spurious control faults after initial operation where the component is not expected to receive an additional signal during the course of the accident to readjust or change its operating state; and (2) position faults before an accident if the component receives an automatic signal to return to its operable state under accident conditions. However, a potential adversary could certainly create a spurious control fault to disable a component from, for example, a motor control center. Likewise, a saboteur at a motor control center or the valve itself could induce a position fault before an

---

68 Here again, the locations from which these events can be accomplished can be linked to *basic events* in the existing *fault tree* (i.e., surrogate events). This reduces the required amount of *fault tree* manipulation at the risk of obscuring the logic associated with the location linkage and making it more difficult to assure quality because the event names may no longer be representative of all of the sabotage events being considered.

69 See Paragraph 4.2.1(10) of Reference 3.

70 Interrelationships of this type will frequently be identified during the walkdowns. (See Section 6.1.1.) They may be modeled as sabotage events affecting multiple areas. (See Section A.3.2.)

accident and disable cabling to ensure that the valve never receives the automatic signal to return to its operable state under accident conditions. Possible malevolent acts of this type need to be addressed in the system sabotage fault tree branches.

A.2.3.3 Non Fault Events Affecting System Availability

The system fault trees developed for PSAs frequently include events that do not involve equipment, component, or device faults, but affect system reliability or availability. Non-fault events of this type include operator recovery actions, test and maintenance outages, and human errors. Fault tree events that involve equipment, component, or device faults generally translate quite directly into sabotage scenario events, although several different types of faults may translate into the same sabotage scenario events. However, these non-fault events do not translate directly into sabotage scenario events. Test and maintenance outage events should be deleted from PSA fault trees when they are translated into system sabotage fault tree branches. As discussed in Sections 2.5 and A.2.3.5, the effects of test and maintenance outages on the designation of vital areas are treated in a different manner. For other events of this type, the team should determine, based upon the expected conditions during the execution of the sabotage scenario, whether the event is sufficiently likely to succeed to credit in the analysis. For recovery actions and human errors, modeling decisions should be made in a manner that is consistent with the policy guidance regarding human recovery actions and human error in Section 2.7. In either case, the system sabotage fault tree branches developed should reflect either the assumption that these events always occur or that they never occur.

A.2.3.4 Random Component Failures

As discussed in Section 2.4, the policy decision may be made to include random failures whose likelihood exceeds a probability cut-off in the vital area analysis. An approach for fault tree analysis software that permits inclusion of both random failures and malevolent acts in the sabotage fault tree model and that can easily compute the Boolean complement of minimal cut sets and minimal path sets is described in Section A.2.1. That approach requires no modifications of the system sabotage fault tree branches. If the fault tree analysis software does not have these capabilities, then the approach, discussed in Section A.2.1 for treating random failures of special components and random failures of systems, must be supplemented with modifications of the system sabotage fault tree branches. As the discussion in Section A.2.1 demonstrates, in situations where the failure probabilities of systems, system trains, or special components do not exceed the probability cut-off, the consideration of random failures has no effect on VAI. In developing the facility sabotage fault tree model to reflect these random failures, care needs to be taken to ensure that the model accurately reflects the probability cut-off. The particular concern is the possibility of inadvertently including multiple concurrent random failures of systems or system trains where the likelihood of the combination of failures does not exceed the probability cut-off even though the probabilities of the individual failures exceed the probability cut-off. In order to model these random failures correctly, the VAI team should do the following:

1. Develop the complete facility sabotage fault tree without consideration of random failures.

2. Identify the sabotage fault tree branch that depends, either explicitly or implicitly, on systems where the random failure probability of one or more train of the system exceeds the probability cut-off.

3. Replace the top event of this branch in the facility sabotage fault tree with an OR gate.

4. Make multiple copies of the branch, modifying each copy to reflect the failure of one of the systems or system trains for which the random failure probability exceeds the probability cut-off. Link each of these modified copies along with the original branch with no random failure to the OR gate inserted in Step 3.[71]

This process is illustrated in Figure A-7 for a situation in which trains A and B of the system each have random failure probabilities in excess of the probability cut-off, but the random failure probability for the total system is less than the random failure probability cut-off. The undeveloped events labeled "Train A Random Failure" and "Train B Random Failure" are modeled as always occurring (i.e., set to Omega) when the fault tree is solved.

This modified facility sabotage fault tree incorporates the random failures of systems and system trains in manner that yields a solution accounting for the possibility of random failures occurring concurrently with a malevolent act.

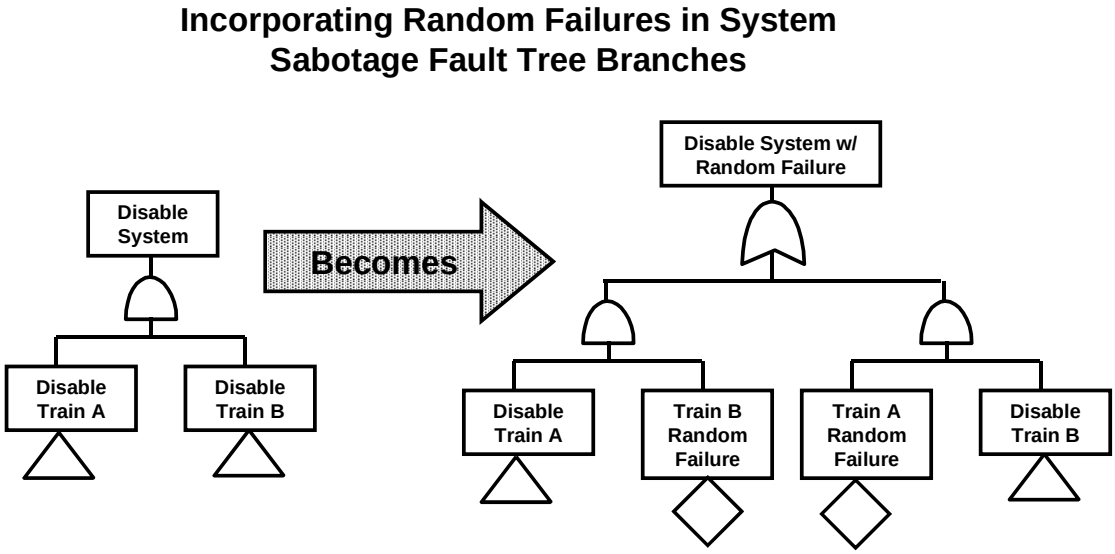

Figure A-7. System Sabotage Fault Tree Branch Modifications

[71] Should the system or train failure probabilities be sufficiently large that the likelihood of concurrent failure of two systems or trains exceeds the probability cut-off, copies of the fault tree branch that have been modified to reflect the concurrent failures of the trains or systems should be added to the OR gate inserted in Step 3.

A.2.3.5 Maintenance

As discussed in Section 2.5, it is necessary to identify vital areas in a manner that accounts for the possibility that system trains may be out of service for maintenance. This issue can be addressed either by establishing additional temporary vital areas that are afforded vital area protection only when equipment in related vital areas is out of service for maintenance. Alternatively, facility vital areas can be designated so that that the minimum complement of operable equipment, systems, or devices to be protected against sabotage would remain protected by being in vital areas even though some equipment was undergoing maintenance. This can be done systematically by considering the possibility that system trains will be out of service for maintenance concurrent with a malevolent act by the potential adversary. However, this is logically equivalent to considering the possibility that system trains will be out of service because of a random failure concurrent with a malevolent act by the potential adversary. Therefore, the approach discussed in Section A.2.3.4 can also be employed to address the need to account for maintenance during the VAI analysis. This approach modifies the VAI analysis to ensure that the vital areas identified will contain the requisite minimum complement of equipment, systems, or devices to ensure that protection is provided against unacceptable radiological consequences even when equipment is out of service due to maintenance. In using the approach discussed in Section A.2.3.4, care must be taken to limit the amount of equipment assumed to be out of service for maintenance to the maximum amount permitted by facility safety documents containing the operational limits and conditions. These documents are frequently referred to as technical specifications or technical safety requirements.

A.2.3.6 Results

The final result of the activities discussed in this section is a facility sabotage fault tree that is developed to the level of disabling of equipment, components, and devices. This sabotage fault tree links the bounding MAIEs and the disabling of equipment, components, and devices that are part of the front line systems and support systems that must respond to the bounding MAIEs to prevent unacceptable radiological consequences. This sabotage fault tree will have the MAIEs and the events in which equipment, components, and devices are disabled as basic events.

A.2.4 Generic Sabotage Fault Trees

Where VAI analyses are contemplated for many facilities of similar design (in terms of safety functions and safety systems), it may be beneficial to develop generic facility and equipment sabotage fault trees. The advantages of using generic sabotage fault trees are that they (1) make it unlikely that a sabotage event will be overlooked in the development of sabotage fault trees for specific facilities; (2) reduce the time required to develop the specific trees; and (3) make it possible for someone with minimal knowledge of fault tree analysis to develop the detailed trees efficiently. In using generic sabotage fault trees for VAI, care must obviously be taken to ensure that the design of the facility being analyzed is consistent with the assumptions made in developing the generic sabotage fault trees. The generic sabotage fault trees may also need to be modified as discussed in Sections A.2.3.4 and A.2.3.5 to address issues associated with random component failures and the unavailability of equipment due to maintenance. Generic sabotage

fault trees have been developed for the pressurized water reactor and boiling water reactor design of nuclear power reactors, but the results have not been published.[72]

A.3 Incorporation of Location Data in the Sabotage Fault Tree

The next step in fault tree development is incorporating location information, collected in the manner discussed in Section 6, into the facility sabotage fault tree. This is accomplished in three slightly different ways depending upon the specific sabotage scenario being modeled. The three approaches are discussed separately below.

A.3.1 On-site MAIEs or Disabling of Equipment

For situations in which an MAIE or the disabling of equipment, components or devices is accomplished from one or more on-site locations, without the initiation of an event that affects multiple areas, the sabotage scenario is modeled in the sabotage fault tree in one of two ways. If the fault tree analysis software has a feature for linking basic events to locations, that feature may be used. Alternatively, the fault tree may be modified as follows:

1. Change the basic event that represents the MAIE or item being disabled into an OR gate.

2. Add new basic event(s) under the OR gate that represent the area(s) from which the MAIE can be accomplished or the item can be disabled. The new location basic event(s) should be named in accordance with the abbreviation(s) established when the areas were defined. (See Section 6.1.)[73]

Figure A-8 illustrates this process for the malevolent act of disabling control power to an emergency diesel generator.

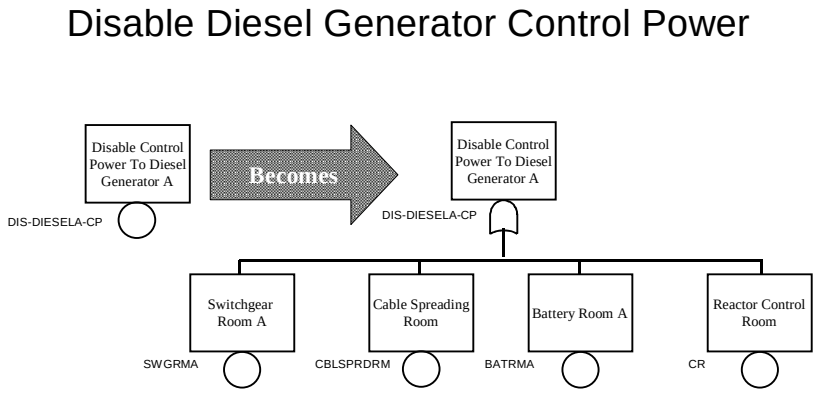

Figure A-8. Location Modeling Example for On-site

[72] However, generic sabotage fault trees can be readily developed from the fault tree analysis modular logic presented in such reports as SAND83-0963, *Modular Fault Tree Analysis Procedures Guide*, Sandia National Laboratories, Albuquerque, NM, August 1983.

[73] Some fault tree analysis or PSA computer programs may make it possible to link basic events with areas without making these modifications to the facility sabotage fault tree. If these features are used, the linkage should be performed in a manner that is clear and traceable.

A.3.2 Modeling Sabotage Events Affecting Multiple Areas

Sabotage scenarios that create an event affecting multiple areas (e.g., arson with the fire suppression system disabled) are modeled in the sabotage fault tree in the following manner:

1. Add a transfer event to each OR gate to which the basic events for disabling each component, equipment item, or device disabled by the event are inputs. These transfer events should be labeled with the name of the event created by the malevolent act (e.g., arson fire with fire suppression system disabled).

2. Create the fault tree branch to which these transfer events will be linked. The top event of the fault tree branch should have the same name as the transfer event. The fault tree branch should be developed down to the basic events in the sabotage scenario. In the example of the arson fire with the fire suppression system disabled, the basic events would be (i) igniting the fire and (ii) the basic events from a fault tree branch for disabling the fire suppression system.

3. Change the basic events in the fault tree branch created in Step 2 above into OR gates and add new basic events that represent the area(s) from which the basic events can be accomplished. In the example of the arson fire with the fire suppression system disabled, the areas would be those in which the fire could be started and those where components of the fire suppression system could be disabled.

A.3.3 Off-site MAIEs or Disabling of Equipment

Sabotage scenarios in which an MAIE can be accomplished from off site (e.g., isolating the facility from the electrical grid) or a component can be disabled from off site (e.g., breaching a water or fuel storage tank with a light anti-tank weapon) are modeled in the sabotage fault tree in the following manner:

1. Convert the basic events corresponding to each of the MAIEs and component disabling events to a House Event (also referred to as an External Event in Reference 7.)[74]

2. Set the value of each of these events in the fault tree software to “True,” “Omega,” or whatever nomenclature represents an event that always occurs. This models the obvious point that malevolent acts that can be accomplished from off site cannot be protected against by designating onsite areas as vital areas and providing protection for them.

A.3.4 Results

The result of these tasks is a facility sabotage fault tree that reflects the locations from which MAIEs can be accomplished, items can be disabled, and malevolent acts affecting multiple locations can be performed. As discussed above, depending upon the fault tree analysis software

[74] This first step is specified only to enhance the clarity of the fault tree model and to permit the type of quality assurance check discussed in Section A.3.4. The basic event probabilities may also be modified without changing the event type.

capabilities, this sabotage fault tree may look very similar to a PSA fault tree with the location linkages accomplished through software features or may be modified to explicitly show the location linkages. If the facility sabotage fault tree is modified to explicitly show the location linkages as discussed above, then it will have the following properties:

1. All bottom level events are either basic events or house events, and

2. All basic events are area locations.

The sabotage fault tree model should be preserved in electronic format (e.g., as an input file or set of input files to the fault tree software program) and retained as a VAI analysis record (see Section 3.5).

A.4 Identification of Candidate Sets of Vital Areas

The next step in fault tree development and analysis is the solution of the fault tree and its dual to identify candidate sets of vital areas. The identification of candidate sets of vital areas is accomplished in two stages. First the facility sabotage fault tree is solved to obtain minimal cut sets, each of which identifies a combination of areas from which malevolent acts could cause an unacceptable radiological release. The second step is to take the Boolean complement of the facility sabotage fault tree (referred to in Reference 7 as the dual of the fault tree). This fault tree is solved to identify minimal path sets (as noted in Reference 7, the minimal cut sets of the Boolean complement of a fault tree are referred to as minimal path sets). Each of these minimal path sets identifies a set of areas that contain the minimal complement of equipment, systems, or devices that, if protected against sabotage, will prevent unacceptable radiological release. Thus, each of these sets is a candidate for the set of vital areas that contains the minimum complement of equipment, systems, or devices to be protected against sabotage. This process is discussed in greater detail below.

A.4.1 Solution of the Facility Sabotage Fault Tree

The first stage of the identification of candidate sets of vital areas is the solution of the facility sabotage fault tree to obtain the minimal cut sets. This is typically accomplished by employing fault tree analysis software. The software should be configured to obtain an untruncated qualitative solution to the fault tree with no probability cut-off.[75] Each minimal cut set is a minimal set of areas from which a potential adversary could perform actions that would create unacceptable radiological consequences. These area combinations should be reviewed to identify the MAIEs and malevolent acts against front line systems that correspond to each area combination. This review may be incorporated into the quality assurance reviews in discussed in Section 3.5.

Where the VAI analysis model incorporates the possibility that random failures or maintenance activities will occur concurrently with malevolent acts, as discussed in Sections 2.4 and 2.5,

[75] As discussed in A.2.1, one approach for addressing random failures concurrent with malevolent acts employs a fault tree analysis solution that truncates the minimal cut sets on the random failure probability.

respectively, it is possible that the facility sabotage fault tree will have one or more minimal cut sets that involves no areas within the facility. This may mean one of two things. First, it may mean that the extent of maintenance outages modeled exceeds that permitted by the facility safety documentation containing the operational limits and conditions. The model developed should be checked against these operational limits and conditions.[76] Second, it may mean that the likelihood of random failure of the systems needed to respond to one or more MAIEs that can be initiated by a potential adversary from off site exceeds the probability cut-off established in Section 2.4. This situation needs to be addressed before proceeding to the identification of vital areas. There are three ways in which the situation can be resolved. First, the probability cut-off should be reviewed to ensure that it provides a consistent level of risk acceptance. The first stage in such a review is determining whether the IE(s) that correspond to the MAIE(s) have been analyzed in safety analyses and the associated risks have been deemed acceptable. If that is the case, then the risk associated with the MAIE(s) should be acceptable unless the likelihood of a potential adversary accomplishing the MAIE(s) is judged to be greater than the likelihood of a corresponding IE(s) occurring by chance. If this review indicates an inconsistent level of risk acceptance, then the probability cut-off, established in Section 2.4, should be revised upward until a consistent level of risk acceptance is achieved. Second, it may be possible to revise the design of the facility systems that respond to these MAIEs so that their random failure probability no longer exceeds the probability cut-off established in Section 2.4. Such a redesign would also improve the safety of the facility by decreasing the likelihood of unacceptable radiological consequences if the IE(s) that correspond to the MAIE(s) occur(s) by chance. However, the requisite facility modifications may be quite expensive for operating facilities and facilities in the advanced stage of construction. Third, depending on the MAIE(s), it may be possible to impose security measures to prevent a potential adversary from initiating the MAIE(s) from off site. These measures may include shielding or hardening facility components (e.g., storage tanks or transformers) to preclude effective standoff attacks. In other cases, the measures may be designed to ensure that a potential adversary cannot obtain the tools necessary to initiate the MAIE(s) from off site.[77] Once action is taken to eliminate all minimal cut sets that involve no areas, the candidate vital area sets can be identified using the approach in the next section.

A.4.2 Development and Solution of Facility Protection Location Tree

The next step in the VAI process is constructing the dual of the facility sabotage fault tree. This is the Boolean complement of the facility sabotage fault tree and, therefore, represents the fault tree for the locations that must be protected to prevent the top event of the sabotage fault tree (i.e., unacceptable radiological consequences).[78] This Boolean complement of the facility sabotage fault tree is referred to as the facility protection location tree. Most fault tree analysis

---

[76] Note that the combination of one system or train down for maintenance, a concurrent random failure in an associated train or system, and a concurrent malevolent act is almost certainly sufficiently unlikely that it need not be considered in the VAI analysis. If this is not the case, the facility design should be carefully re-examined from a safety perspective and the reliability of the safety systems should be improved before proceeding with VAI.

[77] These measures, by their nature, are virtually always the responsibility of the State rather than the facility. However analyses of this nature can highlight need for the State to take such measures. For example, enhanced airport security might prevent the potential adversary from using a hijacked aircraft to cause an MAIE from off site. Such measures typically feed back into the VAI analysis via changes in the characteristics of potential adversaries.

[78] See Chapter VII of Reference 7 for a discussion of dual fault trees and minimal path sets.

computer programs have features that make it possible to take the Boolean complement of a fault tree. If this feature is not available, the facility protection location tree can be derived directly from the facility sabotage fault tree by complementing all events and interchanging OR and AND gates. When solving the facility sabotage fault tree, the areas in the minimal cut sets mean that a potential adversary enters the area to commit a malevolent act. When solving the facility protection location tree, the complemented areas in the minimal path sets mean that a potential adversary is prevented from entering the area. Thus, the minimal path sets for the facility protection location tree are the sets of areas that contain "the minimum complement of equipment, systems, or devices to be protected against sabotage" that are to be identified as vital areas under the recommendation in Section 7.1.5 of Reference 1. Thus any one of these minimal path sets is a candidate to be selected as the set of vital areas for the facility. The complete collection of minimal path sets of the facility protection location tree is the universe of candidate vital area sets. This collection of candidate vital area sets is the product of this stage in the VAI process. The selection of the facility vital areas based on this collection of candidate vital area sets is discussed in Section 8.

Distribution

1 XE Corporation
Suite 307
4611 Greene Ave. NW
Albuquerque, NM 87114

1 David Foster
115 Main Street South, Suite 202
Georgetown, Ontario
L7G3E5, Canada

1 Andrei Glukhov
P.O. box 999
M/S K7-65
Battelle Blvd.
Richland, WA 99352

1 James J. Johnson
7 Essex court
Alamo, CA 94507

1 Iain McNair
Nuclear Installation Inspectorate
404 St. Peter's House
Bootle, Merseyside
L20 3LZ, United Kingdom

1 G. Grint
Nuclear Installation Inspectorate
404 St. Peter's House
Bootle, Merseyside
L20 3LZ, United Kingdom

1 MS 0748 J. LaChance, 6864
1 0748 T. Wheeler, 6864
1 0759 J. Blankenship, 4154
1 1361 J. C. Matter, 6923
1 1361 D. F. Beck, 6923
1 1361 D. Ek, 6923
1 1371 L. Ehart, 6929

1 9018 Central Technical Files, 8945-1
1 0899 Technical Library, 9616
1 0612 Review and Approval Desk, 9612
For DOE/OSTI