SANDIA REPORT
SAND2008-5644
Unlimited Release
Printed September, 2008

Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants

G. Bruce Varnado and Donnie W. Whitehead

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 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's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2008-5644
Unlimited Release
Printed September, 2008

Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants

G. Bruce Varnado
International Security Projects Department

Donnie W. Whitehead
Security Risk Assessment Department

P.O. Box 5800
Albuquerque, NM 87185-0758

Abstract

U.S. Nuclear Regulatory Commission nuclear power plant licensees and new reactor applicants are required to provide protection of their plants against radiological sabotage, including the placement of vital equipment in vital areas. This document describes a systematic process for the identification of the minimum set of areas that must be designated as vital areas in order to ensure that all radiological sabotage scenarios are prevented. Vital area identification involves the use of logic models to systematically identify all of the malicious acts or combinations of malicious acts that could lead to radiological sabotage. The models available in the plant probabilistic risk assessment and other safety analyses provide a great deal of the information and basic model structure needed for the sabotage logic model. Once the sabotage logic model is developed, the events (or malicious acts) in the model are replaced with the areas in which the events can be accomplished. This sabotage area logic model is then analyzed to identify the target sets (combinations of areas the adversary must visit to cause radiological sabotage) and the candidate vital area sets (combinations of areas that must be protected against adversary access to prevent radiological sabotage). Any one of the candidate vital area sets can be selected for protection. Appropriate selection criteria will allow the licensee or new reactor applicant to minimize the impacts of vital area protection measures on plant safety, cost, operations, or other factors of concern.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of the NRC, in particular, Albert Tardiff, for helping to produce this document. We also gratefully acknowledge the work of Dr. John Hockert on vital area identification for U.S. nuclear power plants and international training course materials development. Muck of the text rests upon Dr. Hockert's contributions to these areas. Inez Atencio and Betty Biringer provided invaluable assistance in the review of the report.

Contents

Figures

Tables

Error! No table of figures entries found.

NOMENCLATURE

DBT	design basis threat
IEs	initiating events
LOCA	loss-of-coolant accident
IEMOs	initiating events of malicious origin
MOX	mixed oxide
NRC	U.S. Nuclear Regulatory Commission
PRA	probabilistic risk assessment
QA	quality assurance
SSC	systems, structures, or components
VAI	vital area identification

1. INTRODUCTION

1.1 Background

Nuclear power plants contain large inventories of radioactive materials that could, if released, cause radiological hazards to workers, the public, and the environment. Any deliberate act directed against a nuclear power plant that could directly or indirectly endanger public health and safety by exposure to radiation is defined in 10 CFR 73.2 as radiological sabotage. [Ref. 1] 10 CFR 73.55 specifies requirements for protection of nuclear power plants against radiological sabotage, including the location of vital equipment in vital areas and protection measures to be applied to vital areas. [Ref. 2] It is therefore necessary for each nuclear power reactor licensee and new reactor applicant to identify the vital areas to which the required protection measures will be applied. This document provides guidance on a method that can be used by licensees and new reactor applicants to identify nuclear power reactor vital areas.

The initial basis for vital area identification was U.S. Nuclear Regulatory Commission (NRC) Review Guideline 17, which required that essentially all safety-related equipment be considered vital. The review guideline referenced NRC Regulatory Guide 1.29, "Seismic Design Classification," and suggested that all equipment that required seismic protection should be designated as vital and enclosed within a vital area. However, the Review Guideline 17 standards were not uniformly applied during the reviews of some of the initial facility and license applicant vital area designations. The NRC initiated research studies to develop systematic methods for identifying vital areas at nuclear power reactors. [Ref. 3, 4] The key concepts that emerged from those studies include the use of logic models (fault trees) to determine the events that can cause release from a plant, replacing the events in the fault trees with the locations from which they can be accomplished, and solving the fault trees to generate (1) the combinations of locations which must be visited to complete sabotage scenarios (target sets) and (2) the combinations of locations that, if protected, will prevent all possible sabotage scenarios (prevention sets). The methods were applied to all U.S. nuclear power plants during the late 1970s and early 1980s. [Ref. 5] In 1985 an NRC committee issued its recommendations and basic assumptions for vital area identification in NUREG-1178. [Ref. 6] The NUREG-1178 approach recommended that vital areas be defined as the set of areas that must be protected to prevent radiological sabotage rather than as the set of areas containing all safety-related equipment as specified in Review Guideline 17. This approach was considered by NRC but was not formally adopted at that time.

The NRC reconsidered the approach recommended in NUREG-1178 in 1999. At that time, the Commissioners directed the NRC staff to develop a plan to modify the regulations to require power reactor facilities to identify sets of equipment that must be protected to maintain safe operation or for safe shutdown of the plant. [Ref. 7] The NRC developed a plan to accomplish this rule with a scheduled completion date in 2002.[1] The progress of this regulatory initiative was disrupted by the terrorist attacks on September 11, 2001, which caused the NRC to:

[1] The identification of such equipment sets was incorporated into the NRC Operational Safeguards Response Evaluation program as specified by NRC Inspection Procedure 81110, "Operational Safeguards Response Evaluation (OSRE)," dated September 8, 2000.

1. issue Federal Orders and advisories to its facilities to strengthen their capabilities and readiness to respond to a potential attack on a nuclear facility;
2. assess the adequacy of security measures specified in the Code of Federal Regulations (CFR) and implemented at licensed facilities;
3. conduct a comprehensive review of its safeguards and security programs; and
4. codify the measures listed above and lessons learned from the reviews in a revision of 10 CFR 73.55.

As of 2008, the NRC has received an increase in design certification applications for nuclear power plants and has also received over 20 combined license applications. With this renewed emphasis in building new facilities and the revised provisions of 10 CFR 73.55, the NRC deemed it appropriate to update its guidance for identifying vital areas at nuclear power plants. This document provides the updated guidance.

1.2 Purpose

The purpose of this document is to describe a structured process that can be used to identify the areas of a nuclear power plant that should be designated as vital areas. The set of vital areas identified using this process should be provided with the protection measures specified in 10 CFR 73.55 to reduce the risk of radiological sabotage. The vital area identification process is based on the information contained in the following documents:

- NUREG-1178 (*Vital Equipment/Area Guidelines Study: Vital Area Committee Report*) [Ref.6],
- Draft IAEA-NUCLEAR SECURITY SERIES-XXXX (*Identification of Vital Areas at Nuclear Facilities*) [Ref. 8]
- SAND2004-2866 (*A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities*) [Ref. 9],
- NUREG/CR-0809 (*Fault Tree Analysis for Vital Area Identification*) [Ref. 4], and
- *Nuclear Power Plant Security Assessment Format and Content Guide* [Ref. 10].

1.3 Scope

The process described in this document deals with the identification and selection of vital areas for commercial nuclear power plants; however, the basic approach could be applicable to other nuclear facilities (e.g., a fuel reprocessing facility). The focus of this document is on updating, consolidating, and integrating the information already contained in the documents identified in Section 1.2 above.

1.4 Report Organization

Section 1 provides an introduction to the document. Section 2 presents the set of assumptions that are used in the performance of a Vital Area Identification (VAI) analysis for commercial nuclear power plants. Section 3 describes the VAI process in detail. Section 4 describes the

documentation requirements for VAI. Section 5 provides a brief conclusion. References are listed in Section 6.

2. VITAL AREA IDENTIFICATION ASSUMPTIONS

This section provides the assumptions upon which licensees should base their VAI analyses.

1. In order to prevent radiological sabotage of a nuclear power plant it is necessary to prevent significant core damage and spent fuel sabotage. Vital areas should be identified so as to protect a minimum set of the systems, personnel, and equipment needed to prevent significant core damage and spent fuel sabotage.

   The radiological sabotage criterion for inventories of material other than the reactor core and the spent fuel pool is a release of radioactive material in excess of 10 CFR Part 100 [Ref. 11] limits.[2] A minimum set of equipment needed to prevent releases in excess of Part 100 limits from inventories of radioactive material other than the core and the spent fuel pool must also be protected in vital areas.

2. All distinct operating states (power operation, hot standby, cold standby, and refueling) must be addressed in the vital area identification process. Different operational states may rely on different equipment to perform safety functions and may require protection of different areas to ensure protection against sabotage. A set of vital areas may be identified for each operational state or a bounding set of vital areas that provides protection during all operating states can be selected. The latter approach may be advantageous from a physical protection standpoint to minimize or eliminate the need for reconfiguring physical protection measures when the operational states change.[3]

3. In building logic models for the VAI analysis, it is not necessary to assume that a vital equipment maintenance outage occurs concurrently with an attack. Vital equipment maintenance outages that occur during operations should be addressed as specified in Reference 10, Volume 3 and may require the implementation of compensatory measures such as designating and protecting alternate vital areas containing redundant equipment.

4. It is not necessary to assume that a random failure of vital equipment occurs concurrently with an attack.

5. Credit can be taken for operator actions if all of the following conditions are met:

   a. There is sufficient time to implement the actions between the sabotage act(s) and the onset of core damage or spent fuel melting.

[2] The dispersal of unirradiated mixed oxide (MOX) fuel may or may not produce exposures that exceed 10 CFR Part 100 limits depending upon the Pu concentration and other factors. However, because unirradiated MOX fuel could be a target for theft, the area in which any inventory of such fuel is stored should be protected in the same manner as vital areas, regardless of the potential for a release exceeding 10 CFR Part 100 limits.

[3] 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 remove that area from the vital area set 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.

b. Environmental conditions in the area where the actions must be performed allow access of personnel.

c. Adversary interference with the completion of the actions is precluded.

d. Any equipment needed to complete the actions is available and ready for use. (This may require that the equipment is secured in a vital area.)

e. Approved procedures for the actions exist.

f. Training is conducted on the procedures covering the actions under conditions similar to the scenarios for which the actions are credited.

6. Spurious actuation of equipment (as might occur as a result of fire) must be addressed.

7. The effects of cyber attacks on equipment performance must be addressed.

8. The inability of an adversary to identify cable trays containing power or control cables should not be used as a criterion to remove the cable trays from the vital area identification process if cutting the cables would disable the equipment to which the cables are connected.

9. Loss of coolant incidents and main steam line breaks must be considered credible adversary acts unless access to all locations from which such acts could be performed are inaccessible because of disabling radiation levels or environmental conditions so severe that an attacker would not be able to carry out the required acts before being incapacitated.

10. Assume that loss of offsite power occurs concurrent with an attack.

11. Assume that all equipment outside the protected area of the plant is lost unless continued operation of the equipment makes the situation worse.

3. VITAL AREA IDENTIFICATION PROCESS

Vital Area Identification (VAI) is the process of identifying the areas of a nuclear facility that must be protected to prevent malicious acts that could directly or indirectly endanger the public health and safety by exposure to radiation. Exposure of the public to unacceptable levels of radiation can occur only if radioactive material is dispersed from the facility. In order to disperse the material by sabotage, an adversary must cause some form of dispersal energy to be applied to the radioactive material. The adversary may do this directly by applying energy from an external source (such as explosives or incendiary devices) or indirectly by using the thermal or mechanical energy stored in the material or its related process systems to cause dispersal. Direct sabotage attacks generally require the attacker to gain physical access to the area in which the material is used or stored. Indirect sabotage attacks may be possible without gaining direct access to the material, such as through attacks on cooling or other process or safety systems.

VAI involves the use of logic models to systematically identify all of the malicious acts or combinations of malicious acts that could lead to radiological sabotage. The models available in the plant probabilistic risk assessment (PRA) and other safety analyses provide a great deal of the information and basic model structure needed for the sabotage logic model. The probabilities of occurrence of events used in the PRA are not considered in the VAI process; only the PRA logic models are of use. Also, as discussed in a later section of this document, there are events that are not generally considered in a PRA that could be caused by an adversary (for example, malicious acts that disable or destroy systems, structures, or components (SSC) not susceptible to random failure), and care must be taken to include those types of events in the sabotage logic model.

The purpose of VAI is to identify the areas of the plant that must be protected against sabotage. Consequently, once the sabotage logic model is developed, the events (or malicious acts) in the model are replaced with the areas in which the events can be accomplished. This sabotage area logic model is then analyzed to identify the target sets (combinations of areas the adversary must visit to cause radiological sabotage) and the candidate vital area sets (combinations of areas that must be protected against adversary access to prevent radiological sabotage). Any one of the candidate vital area sets can be selected for protection. Appropriate selection criteria will allow the licensee to minimize the impacts of vital area protection measures on plant safety, cost, operations, or other factors of concern.

The steps in the VAI process are as follows:

1. Identify the inventories of radioactive material for which radiological sabotage is a concern. Include sabotage of these inventories as events in the sabotage logic model.
2. Determine whether direct dispersal of each inventory of concern is possible; if so, include direct dispersal of the each such inventory as an event in the sabotage logic model.
3. Identify any initiating events (IE) [Ref. 12] that can, alone or in combination with other malicious acts, lead indirectly to radiological sabotage of each inventory of concern. Identify the systems required to mitigate those IEs (if mitigation is possible) and the success criteria for those mitigating systems.

4. Using the information obtained in step 3, develop the portions of the sabotage logic model that represent the combinations of events that could lead indirectly to radiological sabotage.
5. Eliminate from the sabotage logic model any events that the design basis threat (DBT) does not have the capability to perform.
6. Identify the areas corresponding to sabotage logic model events; that is, areas in which direct dispersal, IEs, and the mitigating system disablement events in the sabotage logic model can be accomplished. Replace the events in the sabotage logic model with their corresponding areas.
7. Solve the sabotage area logic model to identify the target sets – the combinations of areas to which the adversary must gain access in order to cause radiological sabotage. [Ref. 13, 14, 16]
8. Find the prevention sets of the sabotage area logic model (or find the Boolean complement of the result of step 7) to identify the candidate vital area sets – the combinations of areas that must be protected to prevent radiological sabotage. [Ref. 16, 18]
9. Select the VA set that will be protected to prevent radiological sabotage.

Each of these steps is discussed in detail in the sections that follow.

3.1 Identify Inventories of Radioactive Material

The first step in the VAI process is to identify all of the inventories of radioactive material at the facility that could be subject to radiological sabotage. For nuclear power reactors, the core and the spent fuel pool are the primary focus of concern for radiological sabotage. If there are any other significant inventories of material the release of which might exceed 10 CFR Part 100 limits, they should be identified and addressed in the steps that follow.

3.2 Assess Possibility of Direct Dispersal

The licensee should determine whether it is possible for an adversary to cause direct dispersal of each inventory of concern. This will depend upon the capabilities and resources of the DBT, the structural characteristics of the plant, the environmental conditions in the area where the inventory is located, and perhaps other factors. Because of the massive structures surrounding the core and the spent fuel pool (and the extreme environmental conditions in locations from which the core might be directly attacked), it is unlikely that either of these inventories could be directly dispersed. However, if direct dispersal of one or both of these inventories is deemed possible, the direct dispersal of the appropriate inventory should be included as an event in the sabotage logic model. For any other inventories of concern, the licensee should perform a conservative analysis to determine whether the complete release of the inventory of radioactive material could exceed 10 CFR Part 100 limits. A conservative analysis considers that 100% of the inventory converts into respirable-sized particles during a direct attack. The analysis should be performed without consideration of physical protection or mitigation measures present at the facility. If the potential radiological consequences calculated for an inventory under these conservative analysis conditions are below Part 100 levels, the identification of vital areas need not be considered for this inventory. Such inventories may be protected in accordance with prudent management practice. If the release of a complete inventory could exceed the Part 100 limits, the possibility of direct dispersal of the inventory must be considered. The direct dispersal of the

inventory should be included in the sabotage logic model as a potential malicious act leading directly to unacceptable consequences, and the remaining steps of the vital area identification process should be performed for the inventory. The feasibility that the threat could cause direct dispersal of the inventory is addressed when the threat characteristics are considered later in the process.

3.3 Assess Possibility of Indirect Dispersal

Malicious acts that lead indirectly to release are ones that use the potential energy (i.e., heat or pressure) contained in the nuclear or radioactive material or in a process system to disperse the material. Indirect sabotage attacks do not require that the adversary gain access to the area in which the material is located; instead, they involve attacks against SSC or operator actions that normally maintain the facility in a safe state. To determine the areas that must be protected to prevent acts that lead indirectly to radiological sabotage, two types of sabotage attacks must be considered, namely those in which the adversary:

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

An IE that is deliberately caused by an adversary in an attempt to cause a radioactive release from a facility is called an initiating event of malicious origin (IEMO).

3.3.1 Identify IEMOs

Many of the IEs that can lead to release of radioactive material will have already been identified and analyzed in the plant PRA or other safety analyses. However, there are two classes of IEMOs that are probably not addressed in the plant PRA. The first class of IEMOs that may not have been analyzed in the safety analyses includes those IEs that are so unlikely to occur randomly that they may have been identified but 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 an adversary equipped with explosives or other tools (depending on the specifics of the DBT being applied). The second class of IEMOs includes those involving sources of radioactive material releases that may not have been within the scope of the plant PRA. For example, Level 1 PRAs at nuclear power reactors address only events with the potential to lead to core damage and, thereby, the release of radioactive material from the reactor core. Other inventories of radioactive material that might be the source of release leading to radiological sabotage also should be considered in the VAI. There are four approaches that can be used to identify IEMOs. Because the objective is to produce a list that is as complete as possible, all of the approaches listed below should be followed, although one may be selected as the main approach.

1. *Review of risk assessment documentation.* This should be the starting point for this part of the VAI. Lists of IEs in the full-power PRA, in the fire PRA (or other fire analyses), in the seismic PRA (or other seismic analyses), and any other safety evaluation for the plant being analyzed and for similar facilities should be reviewed. Because any of the IEs that can occur randomly can also be caused by malicious acts, this set of IEs should

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

2. *Reference to other VAIs.* Where other VAI analyses for similar facilities are available, the IEMOs identified in those analyses should be reviewed. It is particularly important to identify any IEMOs that were not considered in plant PRA (or safety) documentation.

3. *Engineering evaluation.* The plant systems (operational and safety) and major components should be systematically reviewed to see whether any malicious acts (e.g., disabling, causing to operate spuriously, breaching, disrupting, collapsing, or igniting) could lead directly, or in combination with other malicious acts, to radiological sabotage. This approach should generally not be selected as the main approach for VAI. If the risk assessment (and 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 malicious acts that are not addressed in risk or safety analysis documentation.

4. *Deductive analysis.* In this approach, the VAI analyst should attempt to identify all IEMOs that could lead to radiological release without regard to the operation of mitigating systems and other preventive actions. The safety functions that must be performed to maintain each inventory of concern in a safe state, the systems that perform those safety functions, and the malicious acts that would lead to failure of those systems should be identified. The malicious acts that lead to failure of the systems are then candidates for the list of IEMOs for the plant. This approach should generally not be selected as the main approach for VAI. The main benefit of this approach for facilities with adequate risk assessment (and safety) documentation is brainstorming to identify classes of possible malicious acts that are not addressed in risk or safety analyses.

Care should be taken to include IEMOs that may be accomplished from outside the plant. Depending upon the adversary capabilities (as defined in the applicable DBT that may include insider actions), IEMOs of this type can range from attacks on electrical transmission components that isolate the plant from the electrical grid (loss of offsite power) to attacks on plant SSC (e.g., storage tanks or transformers) and operator actions that can be completed from offsite. Events in this classification will need to be treated differently from those that require an adversary to access areas within the plant.[4]

Care should also be taken to include IEMOs for each of the plant operational states that the VAI needs to address, as identified in Section 2. IEMOs should be cross-referenced to the plant operational state(s) for which they are applicable.

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

[4] This different treatment is required because these IEMOs cannot be protected against by designating 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 a later section.

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 plant;

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. Malicious acts directed against other radioactive material inventories, such as the spent fuel pool.

The list of IEMOs should be prepared in suitable format and retained as part of the VAI document of record.

Each IEMO should be assessed to determine whether there are systems capable of mitigating it. Every IEMO that exceeds mitigating system capacity should be included in the sabotage logic model as a potential malicious act leading to radiological sabotage. The feasibility that the threat could cause an IEMO that exceeds mitigating system capacity is addressed when the threat characteristics are considered later in the process. The steps described in the next two sections should be performed for IEMOs that can be mitigated.

3.3.2 Identify Mitigating Systems

This part of VAI answers the question, "For IEMOs that can be mitigated, what mitigating systems (including operator actions) must an adversary disable concurrent with the IEMOs to cause radiological sabotage?" For each IEMO, the safety functions that must be performed in order to prevent radiological sabotage should be identified. Note that the safety functions that need to be performed in response to a specific IEMO may vary depending upon the plant operating state. The concept of safety functions is discussed in References 12, 13, and 14. The safety functions for light water reactors that are important for protecting against significant core damage and spent fuel sabotage are listed below.[5]

1. Control core 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. Remove irradiated fuel decay heat; and

6. Maintain integrity of irradiated fuel storage.

[5] This list does not include maintenance of subcriticality of irradiated fuel based upon the implicit conclusion that a criticality event in the irradiated fuel storage area would not cause exposures in excess of 10 CFR100 limits.

The safety functions required to maintain the core and spent fuel pool within prescribed and acceptable operating limits are typically described in safety analysis reports. The PRA will identify the plant safety functions and the safety and, in some cases, non-safety systems that can be employed to perform 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 plant operating 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 shows safety functions and the corresponding front line systems for a typical pressurized water reactor.

Table 3-1. 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 set of front line systems that perform each safety function alone or in combination with other systems should be identified and catalogued (see Table). As discussed above, much of this in-

formation can be obtained from the plant-specific PRA. Other information, if needed, may be obtained from various safety analysis reports.

The VAI analyst should prepare a dependency table or spreadsheet linking front line systems with the support systems and operator actions that successful performance of the front line systems depend upon. The initial dependency table/spreadsheet is then used to produce a list of support systems. The analyst identifies all systems required for the functioning of these support systems. These additional support systems are added to the list of support systems. This process is repeated 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. A majority of this information should be readily available from the plant-specific PRA or supporting documentation.

These dependencies relate to the direct hardware and functional dependencies. There may be other dependencies that relate to specific malicious acts or sabotage scenarios. For example, explosive breaching of a cooling water pipe may cause flooding that disables equipment near the pipe breach. Such 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 IEMO 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);

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

5. A table/spreadsheet for dependencies among support systems and operator actions.

This information should be recorded in the appropriate standard record format and retained as part of the VAI document of record. The systems identified in this activity are modeled in the plant sabotage fault tree.

3.3.3 Determining Mitigating System Success Criteria

The required performance of a front line system depends, in general, on the IEMO. 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 IEMO. 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 development of the plant sabotage fault tree branches[6] (see Section 3.4.2).

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, or 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 the plant safety analyses. The plant-specific PRA generally provides realistic success criteria. The bases for all success criteria should be clearly referenced in the documentation and should be included in the documentation if the references are not accessible.

This analysis produces a table/spreadsheet that lists the associated front line systems and support systems for each IEMO, as identified earlier; their success criteria for that IEMO; references to supporting documentation; and any special characteristics of that IEMO that affect the success criteria. The PRA documentation should provide this information for the IEMOs for which corresponding safety IEs were analyzed. The table/spreadsheet should be documented in the appropriate standard record format and retained as part of the VAI document of record in the licensee or applicant document system.

3.3.4 Grouping of IEMOs

Once the system success criteria have been established, the IEMOs can be grouped so that all IEMOs in the same group require that front line systems and support systems meet essentially the same success criteria to prevent radiological sabotage and cause the same special conditions. Thus, the same sabotage fault tree branch can model sabotage scenarios beginning with any of the IEMOs in a group. Through the process of grouping, it will be clear that some categories of IEMOs need to be subdivided. For example, LOCAs may need to be divided by break size. An example LOCA grouping is provided in Table 3-2. Other categories of IEMOs may require similar division. The plant-specific PRA documentation should contain the grouping of safety IEs, which can be employed for the IEMOs that correspond to safety IEs. Relatively few IEMOs do not correspond to safety IEs, and those generally must be categorized in separate groups.

The IEMO that is used to represent the group in the subsequent sabotage fault tree development (typically the IEMO in the group that places the most stringent demands on safety systems), is defined to be the *bounding IEMO*. The remaining IEMOs in the group are defined to be the

[6] Because the adversary wants to disable the system, these top events are defined in a negative sense; that is, failure of the system to meet the success criteria.

bounded IEMOs. Examples of IE grouping for various reactor types can be found in Reference 15.

Table 3-2. Example LOCA Size Grouping

Initiating Event Name	LOCA Size	Front Line Systems	Success Criteria
Small LOCA	Up to 2 inches	High Pressure Injection System	1 of 3 Pumps
Medium LOCA	2 to 8 inches	High Pressure Injection System Accumulators	1 of 3 Pumps 2 of 3 Accumulators
Large LOCA	> 8 inches	Low Pressure Injection System Accumulators	1 of 2 Pumps 2 of 3 Accumulators

The result of this activity is the development of a set of *bounding IEMOs* and associated system success criteria that can be used for developing the plant sabotage fault tree. The VAI documentation should record the IEMOs that are "bounded" by the IEMOs used in the sabotage fault tree development. This documentation is needed to verify completeness and to ensure that when the *bounding IEMOs* are linked to locations, the location set includes those locations from which the adversary can accomplish the bounded IEMOs as well as those from which the *bounding IEMO* can be accomplished. The documentation developed should be retained as part of the VAI document of record.

3.4 Develop Sabotage Logic Model

The next step in performing VAI analyses is constructing a logic model that represents the set of possible sabotage scenarios for the plant that could lead to radiological sabotage. Direct dispersal events and IEMOs that exceed mitigating system capacity should be included in the logic model as noted in Sections 3.2 and 3.3. Other sabotage scenarios that lead indirectly to radiological sabotage consist of a *bounding IEMO* combined with malicious acts required to disable specific systems needed to mitigate that IEMO.

The sabotage logic model is developed from information provided in the plant-specific PRA (and other safety) documentation. Typically, this is accomplished in two stages. The first stage is developing the top-level sabotage logic model to record each type of sabotage attack that is of concern. The second stage is developing the system sabotage logic models, the branches for individual front line systems and the support systems they are dependent upon. This activity is performed by modifying existing PRA models. Because PRAs use fault trees to describe system failures, the remainder of this document assumes that the sabotage logic model will be a fault tree. The details of sabotage fault tree development are presented in the following section.

3.4.1 Top-Level Sabotage Fault Tree Development

The top-level sabotage fault tree aggregates the set of sabotage scenarios that could cause radiological sabotage. Although all operating states of concern could be addressed in a single fault tree, the following discussion assumes that a separate tree will be developed for each operating state. The top event (first level) in the plant sabotage fault tree is "Nuclear Power Plant Radiological Sabotage." The second level of the plant sabotage fault tree identifies the radioactive material inventories of concern for the plant, the reactor core, the spent fuel pool, and any other inventories of concern. These events are linked by an OR gate, because an adversary could cause radiological sabotage by attacking any of these inventories.

The third level of the plant sabotage fault tree identifies the types of attacks (direct or indirect) appropriate for each inventory. Once again, the events are linked by an OR gate, because an adversary could cause radiological sabotage by any of the means deemed plausible. Figure 3-1 shows an example of the top three levels of the sabotage fault tree for a nuclear power plant. The symbols with concave bottoms are OR gates, and the triangles are transfer symbols, indicating that there is additional development of the event in other branches of the tree. The remainder of this section discusses the development of the sabotage fault tree for significant core damage. The development of fault tree branches for the other inventories of concern should follow the same approach.

For each IEMO that can be mitigated, the fault tree should connect the bounding IEMO with disablement of the associated front line systems identified in Section 3.3.4. An example would be "Small Loss of Coolant Accident (LOCA) with Mitigating Systems Disabled." The events at this level are linked by an OR gate because an adversary could cause radiological sabotage employing any of these sabotage scenarios. These events are further developed based upon the success criteria developed in Section 3.3.3. The technique for the further development of these events uses event tree models from the plant-specific PRA as discussed below. The general techniques for constructing and manipulating fault trees are described in Reference 16.

The PRA event trees illustrate the combinations of safety IEs and front line system failures that cause specific plant damage states.[7] This information is used in developing portions of the plant sabotage fault tree in the following three steps:

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

2. Simplify the event tree by removing branching events where both branches lead to core damage. See Figure 3-2 and Figure 3-3 for an example. The IE is shown at the left side of the event tree (Large LOCA in this case), and the mitigating systems for the IE are listed along the top. The branches indicate whether the system functions properly (the Yes branch) or fails (the No branch). Figure 3-3 shows the event tree in Figure 3-2 with the branching event "Containment Integrity" removed since both branches for this event lead to core damage. Containment integrity is irrelevant to the identification of vital areas, because radiological sabotage is achieved once core damage occurs.

[7] For a discussion of event trees and their use in PRA, see Reference 13 and 14.

3. Once the event trees have been simplified, convert them into fault tree branches by linking together the various event tree branches leading to radiological sabotage with an OR gate and then linking the events along each of the branches with an AND gate. Figure 3-4 illustrates the fault tree branch constructed from the simplified event tree in Figure 3-3. The symbols with flat bottoms are AND gates, indicating that all the inputs must be present in order for the event to occur. The circles indicate basic events for which no further development is needed.

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.[8] For example, if the event tree includes recovery of offsite power within a specific time period, the VAI analyst should determine, based upon the DBT characteristics and plant contingency measures, whether credit can be taken for the recovery of off-site power. If so, then the event tree branch where off-site power is not recovered should be ignored when developing the sabotage fault tree branch. Similar considerations apply to operator recovery actions. The determination of whether credit can be taken for operator recovery actions should be based upon conditions specified in Section 2.

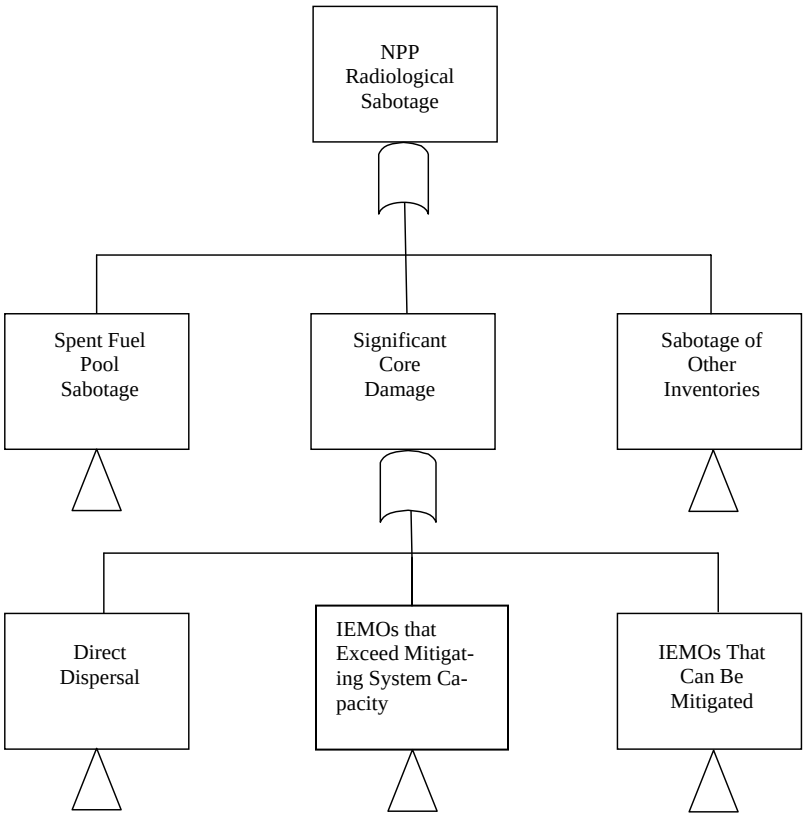

Figure 3-1. Example of Top Three Levels of a Nuclear Power Plant Sabotage Fault Tree.

[8] These probabilistic events must be resolved into a deterministic sabotage scenario. Therefore, the VAI analyst should determine whether they will be credited as occurring during the sabotage scenario.

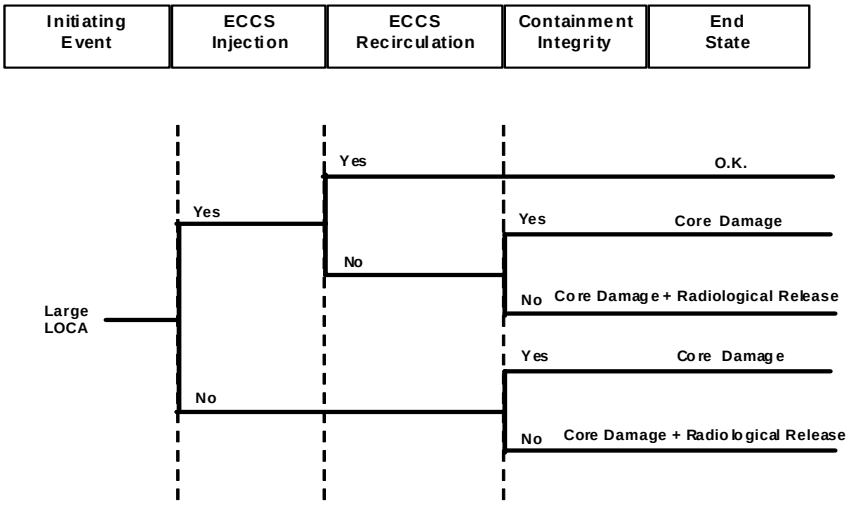

Figure 3-2. Example Event Tree

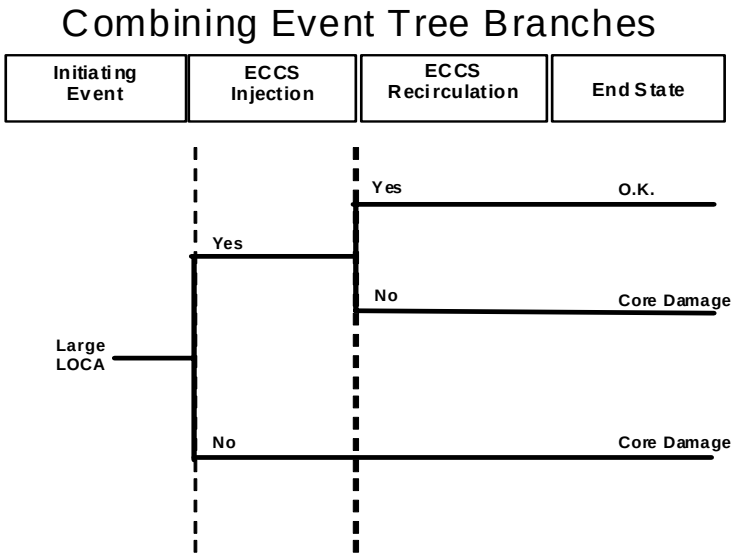

Figure 3-3. Event Tree with Branching Event "Containment Integrity" Removed

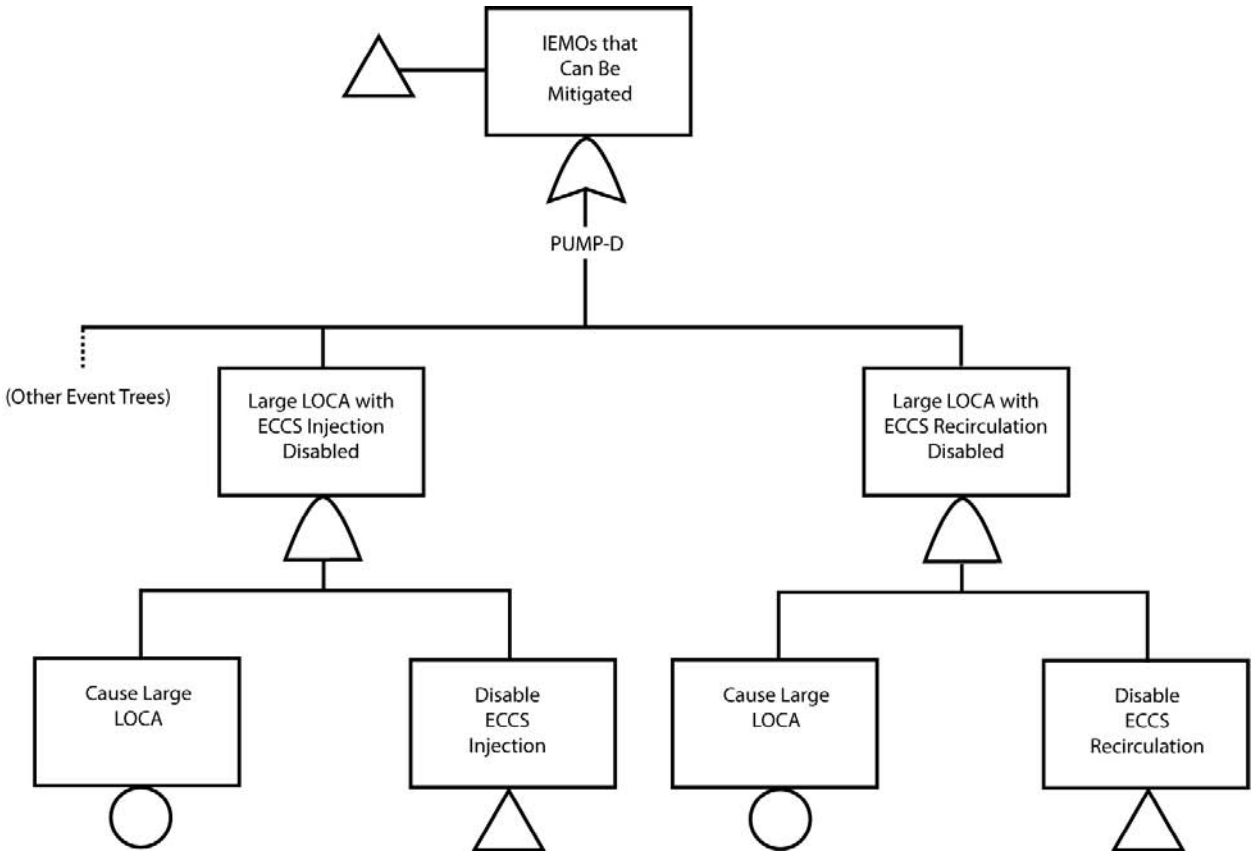

Figure 3-4. Equivalent Sabotage Fault Tree Branch

The plant sabotage fault tree has "Nuclear Power Plant Radiological Sabotage" as its top event and the bounding IEMOs and front line systems that must be disabled to cause significant core damage as its lowest level events. Section 3.4.2 discusses the development of the sabotage fault tree branches for each front line system and the support systems upon which the front line systems depend.

3.4.2 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 plant sabotage fault tree and for each of the support systems with which they have dependencies. These sabotage fault tree branches are similar to the corresponding fault trees used in PRAs. However, there are some differences because sabotage fault tree branches are designed to model sabotage scenarios while PRA 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 should comprehensively identify 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 should include any sabotage events that are so unlikely to occur randomly that they were not considered in the PRA, such as destruction of robust passive components.

3. Operator recovery actions and other events in PRA system fault trees that affect system availability but do not correspond to malicious acts in a sabotage scenario must be treated in a special manner. This type of event is treated as either occurring or as never occurring during or in response to a malicious act. Thus, operator actions that meet the conditions specified in Section 2 are treated as always occurring; those that don't meet the conditions are treated as never occurring in the sabotage fault tree.

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

3.4.2.1 Location Focus

The VAI sabotage fault tree branches are designed to identify the locations (areas) from which an 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 3.6 reflect all locations and combinations of locations where an 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, disabling a pump motor by cutting its control or power cables, or disabling or improperly positioning a component by a remote cyber attack. These methods of disabling components should be shown in the system sabotage fault tree branches.

Therefore, PRA 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." This single event should then be developed to show the areas from which the component can be disabled. Figure 3-5 gives an example of the way that the sabotage fault tree branch for disabling a motor-driven pump is developed. (Note that this branch includes only 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 "Pump Disabled Locally."

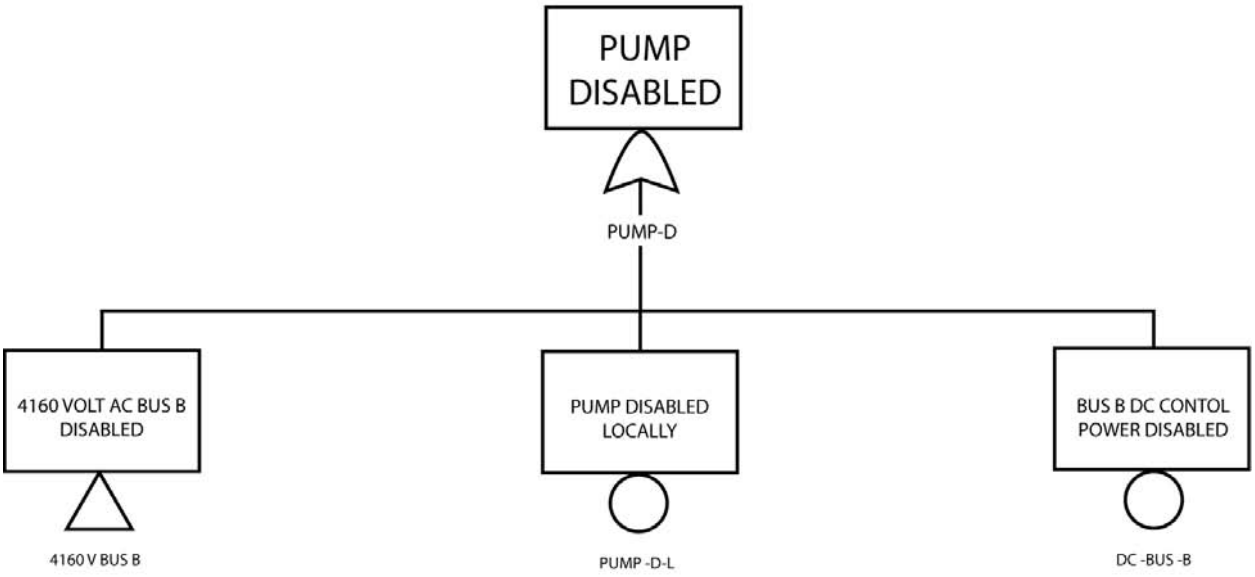

Figure 3-5. Fault Tree Branch for Disabling a Motor-Driven Pump

3.4.2.2 Low Probability Events

The fault trees in PRAs are simplified by not including component failures of such low probability that they do not contribute to risk. However, an 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 malicious acts as disabling a system by breaching piping, breaching tanks or reservoirs, and cutting cables. For events in fluid systems where piping is breached, it is also necessary to consider situations in which the breach creates an alternate flow path that seriously degrades or disables the system. In addition, fluid from pipe breaches or tank ruptures may cause local flooding that disables or degrades the performance of nearby equipment.

Two additional events involving valve position are frequently not considered in PRAs because of their very low probability of occurrence: (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, an adversary could 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 causing the IEMO and disable cabling to ensure that the valve never receives the automatic signal to return to its operable state when required to do so. Possible malicious acts of this type should be addressed in the system sabotage fault tree branches.[9]

[9] These types of failures (faults) may be included in the plant fire PRA.

3.4.2.3 Non Equipment Fault Events Affecting System Availability

The system fault trees developed for PRAs 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. However, non-fault events do not translate directly into sabotage scenario events. Test and maintenance outage and human error events should be deleted from PRA fault trees when they are translated into system sabotage fault tree branches. As discussed in Section 2, it is not necessary to assume that maintenance outages or random failure events occur simultaneously with an attack when developing the sabotage fault tree.[10] Operator actions can be included in the sabotage logic model if they satisfy the conditions listed in Section 2 under which credit can be taken for operator actions. An operator action event included in the sabotage fault tree might be named "Adversary Prevents Completion of Operator Action X."

3.4.3 Sabotage Fault Tree Development Results

The process described above produces a sabotage fault tree that describes the combinations of malicious acts that can lead to radiological sabotage. This sabotage fault tree will have the IEMOs and disablement of systems, personnel, and equipment as basic events. The fault tree and related supporting information should be documented and retained as part of the VAI document of record.

3.5 Assess DBT Capability to Perform Sabotage Acts

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

In this step of the process, any events that are not credible given the DBT capabilities should be eliminated from consideration. The DBT capability to perform the direct dispersal of material, to cause IEMOs, and to disable mitigating systems should be assessed. Events that are beyond the capability of the threat may be removed from the sabotage logic model. The rationale for removal of events and any associated analyses should be documented and retained as part of the VAI document of record.

In addition, any events that are beyond the ability of the facility physical protection system to prevent should be identified. In the analysis of the sabotage logic model, any such events will be assumed to occur always. Generally, any events that the threat can accomplish without gaining access to the site should be assumed to occur. The VAI process should assume that offsite power is unavailable at the time that optimizes the possibility of adversary attack success. Any other

[10] As noted in Section 2, vital equipment maintenance outages during operations should be addressed as specified in Reference 10, Volume 3 and may require the implementation of compensatory measures.

such events in the sabotage logic model should be identified and highlighted for proper treatment in the area identification process described in Section 3.6.

3.6 Identify Areas for Malicious Acts

The next step in the VAI analysis process is identifying and documenting the locations from which an adversary could accomplish each of the events in the sabotage fault tree. This step answers the question, "To what plant areas must the adversary gain access to in order to cause radiological sabotage?" Once the location information has been collected, it is entered into the plant sabotage fault tree as discussed in Section 3.6.4. The resulting sabotage area fault tree can then be solved to determine the combinations of locations from which malicious acts could cause radiological sabotage.

3.6.1 Area Designations

The first step in collecting location data is to subdivide the plant 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 10 CFR 73.55. Therefore, it must be feasible to use existing structures or implement new construction to establish a physical barrier around each defined area. It must also be feasible to control access to each area and to alarm and secure appropriately all points of access to the area.

The VAI analyst should consult with the organization responsible for physical protection system design when defining areas for VAI. Generally, it is more efficient to subdivide the plant into areas that are as small as could be feasibly designated as vital areas. 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 additional review to split a larger area into two or more smaller areas.

Once area divisions are established, they should be documented by marking them on plant elevation drawings or other plant 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 plant as practicable.

3.6.2 Data Collection

The VAI analyst should consult with plant design and operations staff to determine the plant areas to which the adversary would have to gain access in order to cause each IEMO and each disablement event in the sabotage fault tree. This data collection may require support from several technical disciplines, such as plant mechanical, electrical, and instrumentation and control engineering organizations. Studies such as safe shutdown analyses and fire and seismic PRAs may provide good sources of data on equipment locations to support the data collection.

The VAI analyst should look for ways that malicious acts in other nearby areas could accomplish the disablement events. Examples of events that could couple multiple areas 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. Fire paths and combustible loading that might permit a fire to spread into the area if fire protection/suppression systems were disabled should also be considered. Another way that malicious 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, thereby disabling them.

In addition to identifying the plant areas in which malicious acts can be performed the VAI analyst should identify and document any IEMOs or disablement actions that can be accomplished by an adversary from outside the plant boundary.

3.6.3 Data Preparation

The data collected in the previous section should be organized into a table or spreadsheet that lists the area(s) from which for each basic event in the sabotage fault tree can be accomplished. 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 IEMO*, not because the *bounding IEMO* can be accomplished from there but rather because a *bounded IEMO* can be accomplished from there.

3.6.4 Incorporating Location Data in the Sabotage Fault Tree

Incorporating location information into the plant sabotage fault tree links the IEMOs and the disablement acts represented in the sabotage fault tree, with the locations from which they can be accomplished. This is accomplished in three slightly different ways depending upon the specific sabotage scenario being modeled. The three approaches are discussed separately below.

3.6.4.1 On-site IEMOs or Disablement Events

For IEMOs or the disablement events that can be accomplished from one or more on-site locations the area data is included in the sabotage fault tree as follows:

1. Change the basic event that represents the IEMO or disablement event into an OR gate.

2. Add new basic event(s) under the OR gate that represent the area(s) from which the IEMO or disablement event can be accomplished. The new location basic event(s) should be named in accordance with the abbreviation(s) established when the areas were defined.[11]

Figure 3.6 illustrates this process for the malicious act of disabling control power to an emergency diesel generator.

[11] Some fault tree analysis or PRA 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.

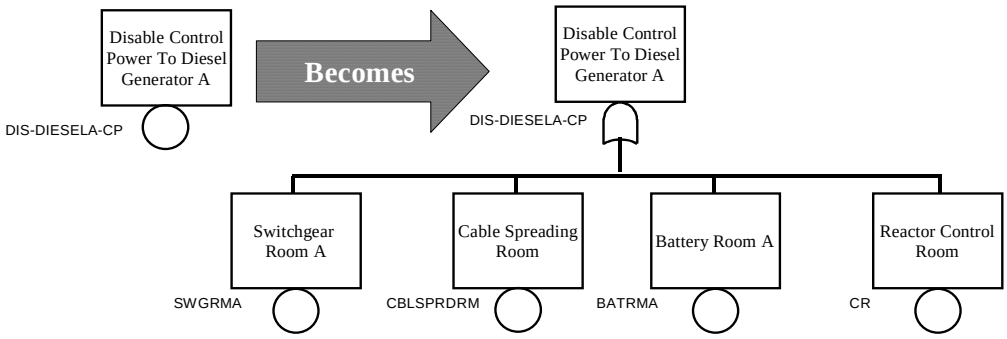

Figure 3-6. Location Modeling Example for On-site Malicious Acts

3.6.4.2 Off-site IEMO or Disablement Event

IEMOs (e.g., isolating the facility from the electrical grid) or disablement events (e.g., breaching a water or fuel storage tank) that can be accomplished from offsite are modeled in the sabotage fault tree in the following manner:

1. Convert the basic event corresponding to each of the IEMOs and disablement events to a House Event (also referred to as an External Event in Reference16).[12]

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 malicious acts that can be accomplished from offsite cannot be protected against by designating onsite areas as vital areas and providing protection for them.

3.6.5 Results from Incorporating Location Data into the Sabotage Fault Tree

The result of this task is a sabotage area fault tree that reflects the locations from which IEMOs can be accomplished and items can be disabled. In this sabotage area fault tree:

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

2. All basic events are area locations.

The area designations, table of areas in which malicious acts can be performed, and sabotage area fault tree should be documented and retained as part of the VAI document of record.

[12] This first step is specified only to enhance the clarity of the fault tree model and to permit quality assurance checks. The basic event probabilities may also be modified without changing the event type.

3.7 Identify Target Sets

The combinations of areas to which the adversary must gain access in order to cause radiological sabotage are the target sets for the plant. The target set identification is done by solving the area sabotage fault tree to obtain its 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. Each minimal cut set is a minimal set of areas from which an adversary could perform actions that would cause radiological sabotage. The target sets identified in this way can be used in planning evaluations of the physical protection system at the plant (such as tabletop exercises, force-on-force exercises, or nuclear power plant security assessments [Ref. 10, 17]). In order to prevent malicious acts leading to radiological sabotage, the plant must protect at least one area in each of these area combinations. The target sets and related fault tree analysis results should be documented and retained as part of the VAI document of record.

3.8 Identify Candidate Vital Area Sets

The candidate vital area sets are the combinations of areas that must be protected to prevent radiological sabotage. Each candidate vital area set contains at least one area from each target set. If the adversary is denied access to all the areas in any one of the candidate vital area sets, then the adversary will not be able to complete any of the sabotage scenarios represented in the sabotage fault tree. Each of the candidate vital area sets contains a minimum complement of systems, personnel, and equipment that, if protected against malicious acts, will prevent radiological sabotage.

The candidate vital area sets are identified by constructing and solving the dual (or the Boolean complement) of the sabotage fault tree. [Ref. 16] Most fault tree analysis computer programs have features that make it possible to take the Boolean complement of a fault tree. If this feature is not available, the sabotage prevention tree can be derived directly from the sabotage area fault tree by complementing all events and interchanging OR and AND gates. When solving the plant sabotage fault tree, the areas in the minimal cut sets mean that an adversary enters the area to commit a malicious act. When solving the prevention fault tree, the complemented areas in the tree mean that an adversary is prevented from entering the areas. Thus, the cut sets for the sabotage prevention fault tree (or the prevention sets [Ref, 18] for the sabotage fault tree) are the sets of areas that contain the minimum complement of systems, personnel, and equipment to be protected against sabotage. Thus any one of these prevention sets is a candidate to be selected as the set of vital areas for the plant. As noted in Section 2, any areas containing inventories of unirradiated MOX fuel should also be included in the set of areas to be protected as vital areas. Consequently, any areas containing unirradiated MOX fuel should be added to every candidate vital area set. The list of candidate vital area sets and the analysis used to identify them should be documented and retained as part of the VAI document of record.

3.9 Select a Vital Area Set to Protect

The final stage of the VAI analysis answers the question, “Which of the candidate vital area sets (i.e., the prevention sets) is it best to designate as the set of plant vital areas to protect?” Typi-

cally, this stage of the VAI includes close coordination with the plant organization responsible for physical protection system design.

Each of the candidate vital area sets identified in the previous step of the VAI process contains a minimum complement of systems, personnel, and equipment that must be protected against sabotage. Licensees might consider factors such as those listed below in the selection of one of the candidate vital area sets as the set of areas to be protected:

1. Impacts on safety and emergency response;

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

3. Reliability of protected SSC and operation actions.

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 such as multi-attribute utility theory [Ref. 19] or the analytic hierarchy process [Ref. 20]. The following sections provide more detailed discussions of the three considerations listed above in selecting one prevention set as the set of vital areas for the plant.

3.9.1 Safety and Emergency Response Impacts

Selecting a candidate vital area set can affect plant 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 plant equipment in vital areas. Although mitigating actions can be taken (e.g., dropping vital area access controls during an emergency), this may actually aid an adversary by granting him access to the remainder of the plant once he has initiated a sabotage scenario. Therefore, in selecting vital areas, preference might be given to candidate vital area sets for which access controls would not unduly impede operator emergency response actions.

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 might 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 analyst 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 an adversary from entering or carrying out malicious acts in a vital area. Discharging firearms in a nuclear plant can pose a number of hazards to plant and personnel safety. The hazards to plant safety include inadvertent disabling of equipment or instrumentation. The hazards to personnel safety include

rupturing of lines containing hazardous materials (e.g., steam, pressurized water, or chemicals) and inadvertent friendly fire. 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. While the discussion of protection measures is beyond the scope of VAI in the selection of vital areas to protect, preference might 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 plant operations or safety.

3.9.2 Ease, Effectiveness, and Cost of Protection

Requirements for measures to protect vital areas are discussed in 10 CFR 73.55. It may be easier or less expensive to apply these protection measures to the areas in one candidate vital area set than to those in another. For example, by virtue of their construction and location, some candidate vital area sets may be able to meet the requirement for bullet-resisting walls, doors, ceiling, and floor, while other sets might require modification to meet those requirements. The licensee may consider the ease, effectiveness, and cost of protection in rating candidate vital area sets.

3.9.3 SSC and Operator Action Reliability

Where facilities have diverse means of accomplishing safety, the systems in different candidate vital area sets or operator actions performed in them may have different reliability. In such cases, preference in the selection of vital area sets to be protected might be given to candidate vital area sets that contain higher reliability systems or actions. This reduces the likelihood that the system protected in vital areas would experience random failure concurrent with a malicious act, reduces the need for entry into the areas for maintenance activities therefore reducing the impact on operations, and increases the likelihood that operator actions will be completed successfully.

3.9.4 Results

The results of this analysis should include:

- 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 to be protected, and documents the rating of each of the candidate vital area sets.

- A recommended vital area set to be protected with the best rating.

These results should be documented and retained as part of the VAI document of record.

4. DOCUMENTATION OF VITAL AREA IDENTIFICATION RESULTS

Thorough documentation should be developed for each step in the VAI process. The analysis, by its nature, generates information that could be quite valuable to an 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 the VAI. The specific nature of these protection requirements and procedures are discussed in 10 CFR 73.21. All team members should receive training in these measures.

The analysis documentation should be well structured, clear, and easy to follow, to review, and to update. Updates or extensions may be needed to address changes in the capabilities of the DBT; the types of IEMOs or disablement events the DBT can accomplish and the locations from which it can accomplish them; plant layout; plant operations; safety systems and measures; and the locations of SSC and operator actions. The documentation should explicitly present how the assumptions in Section 2 are addressed.

In the report (or by reference to available material), the documentation should provide all the necessary information to reconstruct the results of the analysis. The plant management should have a clear understanding of the elements of the report that are viewed as licensee or applicant commitments by the NRC and that will require NRC approval for changes.

The sequence of each analysis documented in the report should follow the order in which the analysis was performed. That is:

- Identification of inventories of radioactive material for which vital areas are required;
- Identification of IEMOs;
- Top-level sabotage fault tree development;
- System sabotage fault tree branch development;
- Sabotage location determination;
- Identification of area target sets;
- Identification of candidate vital area sets; and
- Recommendation of a set of vital areas to be protected.

5. CONCLUSION

The process presented in this document provides a structured, logical approach to identifying the vital areas of a nuclear power plant. The vital areas contain a minimum complement of SSC and operator actions sufficient to ensure safe operation or safe shutdown of the plant. The method incorporates information from plant safety documentation, including PRAs. It employs fault tree analysis to deal with the complexity of a nuclear power plant and to document the logic employed in the identification of vital areas. The process allows the licensee or applicant to select the set of vital areas that meets the requirement for protection against radiological sabotage while minimizing impacts of physical protection measures on plant safety, costs, and operations. Proper documentation of the process will provide the necessary information to reconstruct the results of the analysis to support review, approval, and updating of the vital area selection.

6. REFERENCES

1. 10 Code of Federal Regulations, Part 73.2.
2. 10 Code of Federal Regulations, Part 73.55.
3. Drayton D. Boozer, et. al., "Safeguards System Effectiveness Modeling," SAND76-0428, Albuquerque, NM, 1976.
4. G. Bruce Varnado and N. R. Ortiz, Fault Tree Analysis for Vital Area Identification, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, U. S. Nuclear Regulatory Commission, Washington, DC, June 1979.
5. G. Bruce Varnado and Roy A. Haarman, "Vital Area Analysis for Nuclear Power Plants," SAND80-0553C, Albuquerque, NM, 1980.
6. U. S. Nuclear Regulatory Commission, Vital Equipment/Area Guidelines Study: Vital Area Committee Report, NUREG-1178, February 1988.
7. Staff Requirements Memorandum on SECY-99-024, "Recommendations of the Safeguards Performance Assessment Task Force," U.S. Nuclear Regulatory Commission, June 29, 1999.
8. International Atomic Energy Agency, *Identification of Vital Areas at Nuclear Facilities*, IAEA-NUCLEAR SECURITY SERIES-XXXX, IAEA, Vienna, June 2005 (Draft).
9. John Hockert and David F. Beck, *A systematic Method for Identifying Vital Areas at Complex Nuclear Facilities*, SAND2004-2866, Sandia National Laboratories, Albuquerque, NM, May 2005.
10. USNRC, *Nuclear Power Plant Security Assessment Format and Content Guide*, Washington, DC, September 2007.
11. 10 Code of Federal Regulations, Part 100.
12. NS-R-1, *Safety of Nuclear Power Plants: Design*, International Atomic Energy Agency, Vienna, Austria, 2000.
13. USNRC, PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Final Report, Vols. 1 and 2, NUREG/CR-2300, January 1983.
14. American Society of Mechanical Engineers, *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME-RAS-2002, April 5, 2002.
15. Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, International Atomic Energy Agency, Vienna, Austria, 1992.
16. U.S. Nuclear Regulatory Commission, "Fault Tree Analysis Handbook," NUREG-0492, Washington, DC, USA, 1981.
17. USNRC, *Nuclear Power Plant Security Assessment Technical Manual*, SAND2007-5591, Washington, DC, September 2007.
18. R.B. Worrell and D.P. Blanchard, "Top Event Prevention Analysis: A Deterministic Use of PRA," International Conference on Probabilistic Safety Assessment Methodology and Application, Seoul, Korea, Nov. 26–30, 1995.
19. R. L. Keeny and H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, Wiley, New York (1976).
20. Thomas L. Saaty, *Decision Making for Leaders*, Vol. II, AHP Series, RWS Publications, Pittsburg, PA (2002).

DISTRIBUTION

# of copies	Mailstop	Name, Org	
5		Albert Tardiff U.S. Nuclear Regulatory Commission MS T4F25M 11545 Rockville Pike Rockville, MD 20852	
1	MS0759	Biringer, Betty	6461
1	MS0759	Green, Mary	6411
1	MS1361	Matter, John	6754
5	MS1361	Varnado, Bruce	6754
1	MS9018	Central Technical Files	8944 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories