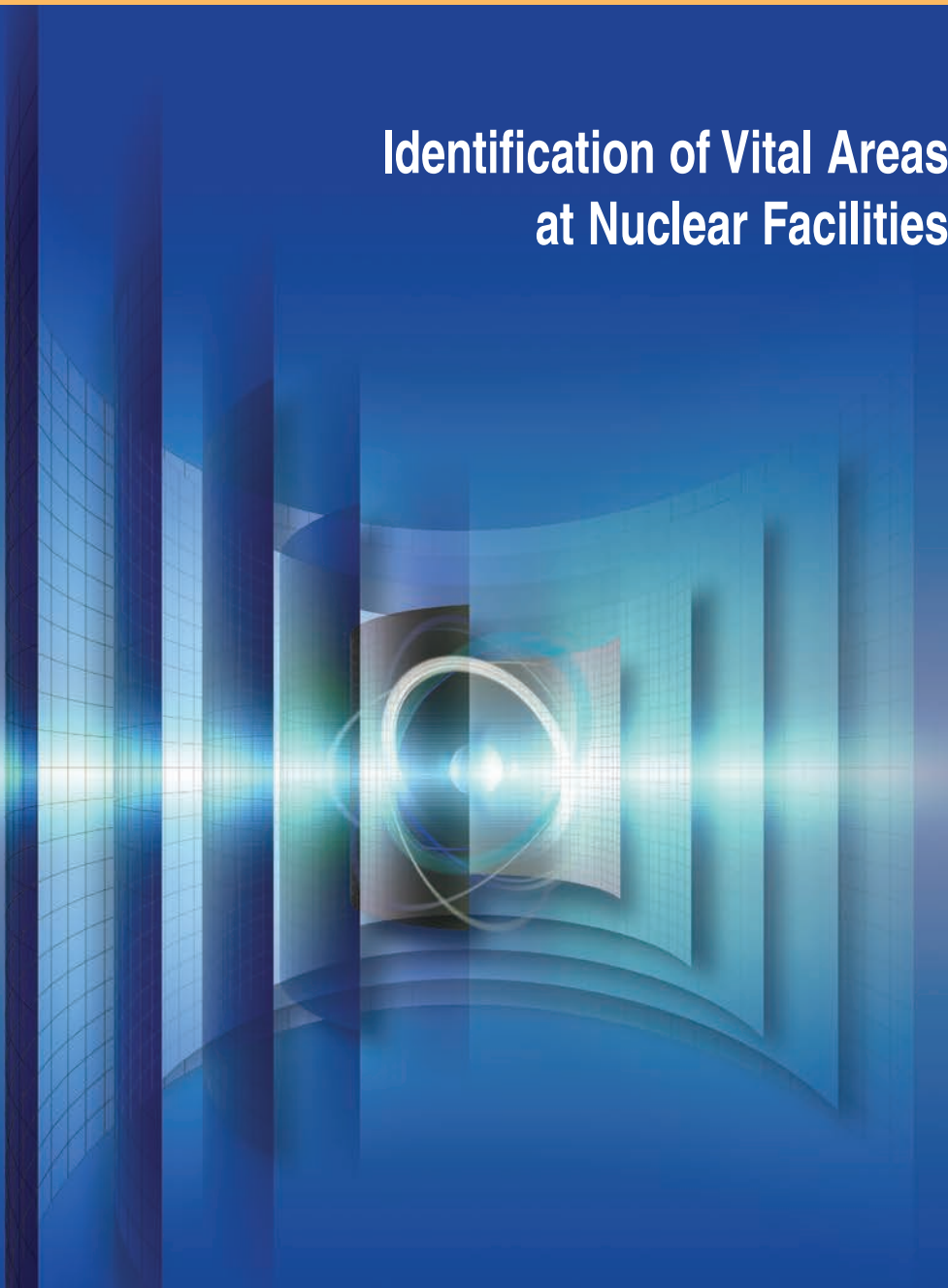
IAEA Nuclear Security Series No. 16

Technical Guidance
Reference Manual

Identification of Vital Areas at Nuclear Facilities



IAEA
International Atomic Energy Agency

THE IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the **IAEA Nuclear Security Series** of publications. These publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material, the Code of Conduct on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

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

DRAFTING AND REVIEW

International experts assist the IAEA Secretariat in drafting these publications. For Nuclear Security Fundamentals, Recommendations and Implementing Guides, open-ended technical meeting(s) are held by the IAEA to provide interested Member States and relevant international organizations with an appropriate opportunity to review the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review. This allows Member States an opportunity to fully express their views before the text is published.

Technical Guidance publications are developed in close consultation with international experts. Technical meetings are not required, but may be conducted, where it is considered necessary, to obtain a broad range of views.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns. An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications.

IDENTIFICATION OF VITAL AREAS AT NUCLEAR FACILITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 16

IDENTIFICATION OF VITAL AREAS AT NUCLEAR FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2012

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
November 2012
STI/PUB/1505

IAEA Library Cataloguing in Publication Data

Identification of vital areas at nuclear facilities : technical guidance. — Vienna : International Atomic Energy Agency, 2012.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 16)
STI/PUB/1505
ISBN 978–92–0–114410–2
Includes bibliographical references.

1. Nuclear facilities — Safety regulations. 2. Nuclear facilities — Safety measures. 3. Nuclear security series. I. International Atomic Energy Agency. II. Series.

IAEAL 12–00702

FOREWORD

The possibility that nuclear or other radioactive material could be used for malicious purposes cannot be ruled out in the current global situation. States have responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material and to effectively respond to nuclear security events. States have agreed to strengthen existing and established new international legal instruments to enhance nuclear security around the world. Nuclear security is fundamental in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported.

Through its nuclear security programme, the IAEA supports States to establish, maintain and sustain an effective nuclear security regime. The IAEA has adopted a comprehensive approach to nuclear security. This recognizes that an effective national nuclear security regime builds on: the implementation of relevant international legal instruments; information protection; physical protection; material accounting and control; detection of and response to trafficking in such material; national response plans; and contingency measures. With its nuclear security series, the IAEA aims to assist States to implement and sustain such a regime in a coherent and integrated manner.

The IAEA Nuclear Security Series comprises: Nuclear Security Fundamentals, which include objectives and essential elements of a State's nuclear security regime; Recommendations; Implementing Guides; and Technical Guidance publications.

Each State carries the full responsibility for nuclear security, i.e. to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; and to combat illicit trafficking and the inadvertent movement of such material. It should also be prepared to respond to a nuclear security event.

The IAEA recommendations for the protection of nuclear installations against sabotage are contained in IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). After the attacks of 11 September 2001, the perception of the potential terrorist threat to nuclear installations changed significantly, and the IAEA initiated an effort to develop a series of guidance publications on the security of nuclear and radioactive material and facilities.

This publication presents a structured approach to identifying the areas that contain equipment, systems, and components to be protected against sabotage. It specifically provides detailed guidance with regard to the identification of vital areas, that is, the areas to be protected in high consequence facilities. However, the process described is applicable to the identification of areas that should be protected at any nuclear facility. The method builds upon safety analyses to

develop sabotage logic models for sabotage scenarios that could cause unacceptable radiological consequences. The sabotage actions represented in the logic models are linked to the areas from which they can be accomplished. The logic models are then analysed to determine areas that should be protected to prevent these unacceptable radiological consequences.

The IAEA officers responsible for this publication were A. Stadalnikas and D. Ek of the Office of Nuclear Security, and A. Guerpinar and S.C. Kim of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The IAEA is preparing a set of guidance publications to be issued in the IAEA Nuclear Security Series to assist Member States in the design, implementation and evaluation of their physical protection systems of nuclear material and nuclear facilities. The present publication presents a systematic process for identifying the *vital areas* of a nuclear facility.

Identification of vital areas is an important step in the process of protecting against sabotage. *Vital area identification* (VAI) is the process of identifying the areas in a nuclear facility around which protection will be provided in order to prevent or reduce the likelihood of sabotage. INFCIRC/225/Rev. 5 (IAEA Nuclear Security Series No. 13) [1] — henceforth referred to as INFCIRC/225 — indicates that nuclear material in an amount which if dispersed could lead to high radiological consequences (HRCs) and a minimum set of equipment, systems, or devices needed to prevent HRCs, should be located within one or more vital areas, and be located inside a protected area[1]. All measures that have been designed into the facility for safety purposes should be taken into account when identifying vital areas.

1.2. OBJECTIVE

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

[1] 'High radiological consequences', as referred to in Ref. [1], indicate relatively severe radiological consequences resulting from large nuclear facilities such as nuclear power plants. The level of protection for vital areas specified in Ref. [1] is similar to that required to prevent the theft of Category 1 nuclear material. In the context of a graded approach, the areas that require protection for inventories in lower consequence categories (above unacceptable radiological consequences but below high radiological consequences) can be identified using the process described in this publication, although these areas may require lower levels of protection than required for vital areas.

1.3. SCOPE

This publication focuses solely on the process for VAI at nuclear facilities. The VAI process can be used for existing facilities to identify vital areas and to evaluate the effect that design changes have on vital area selection. This process may also be applied to new facilities in the design stage to analyse how design and layout features may be optimized for vital area selection. Also, the concepts and principles (i.e. identifying material or components that require protection in a vital area on the basis of unacceptable radiological consequence thresholds) of this publication may be applied at facilities other than nuclear ones.

1.4. STRUCTURE

Section 1 provides the background, objectives, and scope of this publication. Section 2 discusses the process used to identify vital areas, and the expected results of the process. Also, it outlines policy considerations that should be addressed by the competent authority (State regulatory body) and actions by the operator prior to the start of VAI, and describes the step by step process leading to the selection of a minimum set of areas in a nuclear facility that should be protected as vital areas. Section 3 provides guidance for documenting the results of VAI. The appendix provides an example of how logic models can be solved to identify candidate vital area sets.

2. VITAL AREA IDENTIFICATION PROCESS

This section describes the process used to identify vital areas in a nuclear facility. The vital area concept is used to define a boundary around the vital equipment, systems, or devices, or nuclear material to which physical protection can be applied. The objective of the VAI process is to identify a set of areas of a facility containing the equipment, systems, structures, components, devices, or of operator actions that, if adequately protected, will prevent HRCs.

The VAI process should be repeated when design changes are being considered or prior to their implementation, and when the threat has been modified. The best time to apply this process is in the design phase of a new facility, when physical protection can be optimized, and retrofitting avoided.

Typically, an operator is responsible for identifying the vital areas, and the State's regulatory body is responsible for validating the VAI process.

2.1. PROCESS OVERVIEW

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

— Gather information that is input to the VAI process.
  - Identify VAI process team
  - Policy considerations. Address the key policy considerations essential to the VAI process.
  - Site and facility characteristics. Identify the inventories of nuclear and other radioactive material. Evaluate the facility and site characteristics needed to determine whether sabotage could lead to HRCs.
  - Conservative analysis for each nuclear and other radioactive material inventory. Determine whether the complete release of any inventory could exceed the HRC criteria. Include direct dispersal of any such inventory as an event in the sabotage logic model and continue with the process described below.
— Identify any initiating events [2] of malicious origin (IEMOs) that can lead indirectly to HRCs.
— Identify any IEMOs that exceed the capability of mitigation systems. Include each such IEMO as an event leading to HRCs in the sabotage logic model.
— Identify systems, structures and components to mitigate each IEMO. For each IEMO that does not exceed mitigating system capability, identify the safety functions necessary to mitigate the IEMO, the systems, structures and components that perform the safety functions, and the success criteria for the systems.
— Develop a sabotage logic model that identifies the combinations of events (direct dispersal, IEMOs that exceed mitigating system capability, and IEMOs coupled with mitigating system disablement) that would lead to HRCs.
— Eliminate from the sabotage logic model any events that the assumed threat does not have the capability to perform.
— Identify the locations (areas) in which direct dispersal, IEMOs, and the other events in the sabotage logic model can be accomplished. Replace the events in the sabotage logic model with their corresponding areas.

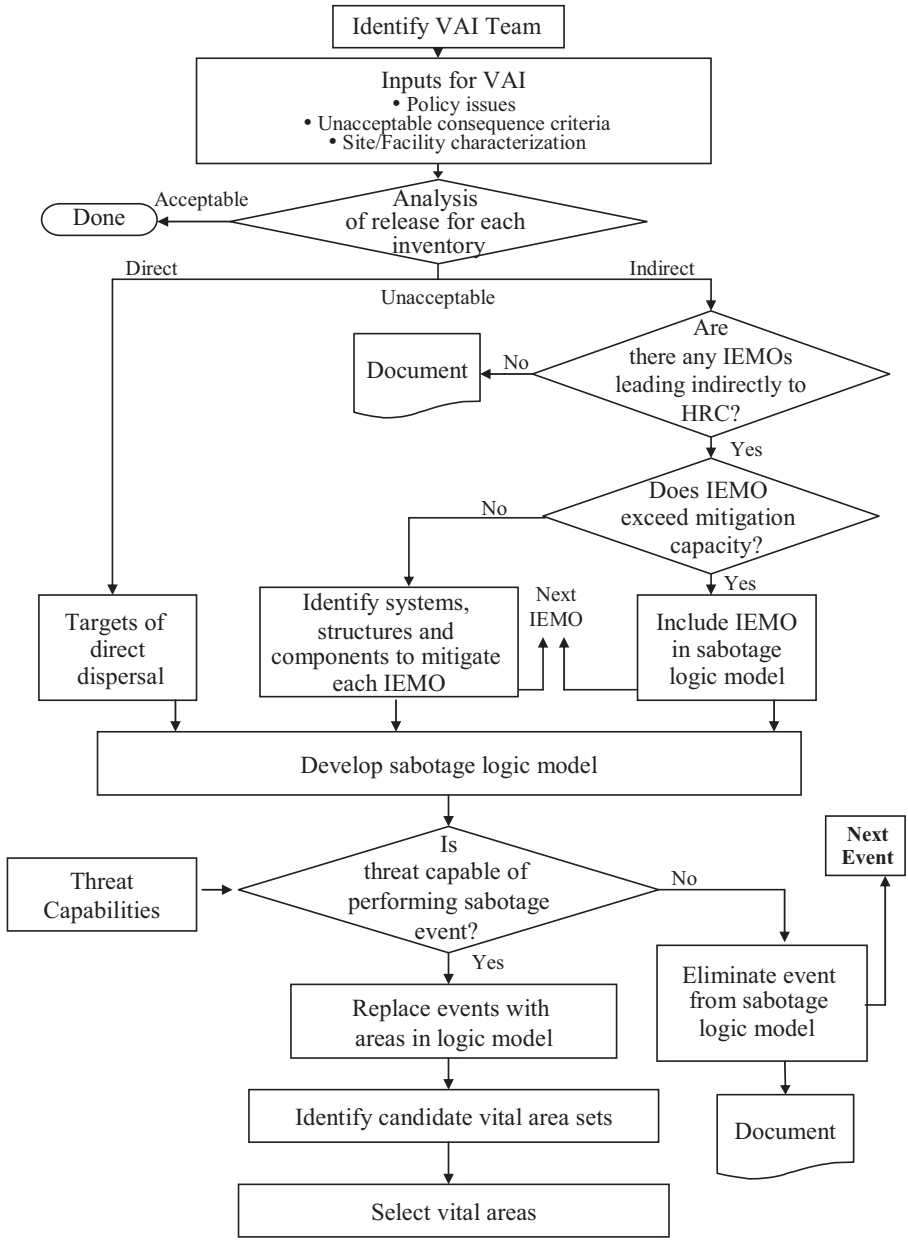


FIG. 1. Vital area identification process

— Solve the sabotage area logic model to identify the combinations of locations that should be protected.
— Select the vital area set that will be protected to prevent sabotage leading to HRCs.

Facility safety analyses can provide valuable information and models to support VAI. If a deterministic safety assessment (DSA) or a probabilistic safety assessment (PSA) has been completed for the facility, it will provide analyses of response of the facility to various initiating events (IEs) that may be caused by random failure, human error, etc. These events could also be caused by malicious acts. DSAs and PSAs [3, 4] provide extensive information on site and facility characterization that will be useful to the VAI team. Either type of analysis will contain information that can be used to construct the logic models needed for VAI [5–7].

2.2. INPUT TO THE VAI PROCESS

2.2.1. Policy considerations

Policy considerations to be addressed prior to initiation of the VAI process are:

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

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

2.2.1.1. Unacceptable radiological consequences

The first significant policy consideration is the explicit decision regarding *unacceptable radiological consequences* and high radiological consequences. Typically, these consequence levels would be defined in terms of an unacceptable dose level, unacceptable radioactive material release level or unacceptable plant state, such as core damage for an NPP. It should be noted that if HRCs are identical with those defined by the State in relation with nuclear safety considerations, the safety analyses performed for the facility could be used for VAI without significant modification. Further discussion on unacceptable radiological consequences and an example of a consequence categorization table for sabotage can be found in Ref. [8].

2.2.1.2. Determination of operational states to be assessed

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

2.2.1.3. Safe facility state

There may be a number of facility states that, if achieved subsequent to an accident or transient, are designed to maintain the facility in a safe state. In principle, all nuclear facilities should maintain the fundamental safety functions [9] of:

— Control of reactivity;
— Cooling of radioactive material;
— Confinement of radioactive material.

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

Any facility state accepted for this purpose should be one in which the necessary safety functions can be accomplished for a reasonable period, either by

the safety equipment designed to perform those functions, or by alternative arrangements such as accident management or on site emergency preparedness and response[2]. The defined facility safe state(s) may differ for analysis of different facility operational states. The competent authority should identify or approve the safe facility state for each facility operational state.

2.2.1.4. Equipment unavailability

Although VAI focuses on the consequences of malicious acts, equipment unavailability could conceivably occur by chance, or as a result of maintenance outages, concurrent with a malicious act. The results of the VAI need to be deterministic; that is, an area is either vital or it is not. Therefore, the assumptions that establish the requirements for the VAI should specify whether the analysis should include concurrent equipment unavailability due to random failure or maintenance[3].

2.2.1.5. Credit for recovery actions

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

[2] If alternative arrangements such as emergency preparedness and response are to be made, the time required and the situation in which these actions should be undertaken should be considered. In some cases, the deployment and availability of these measures might make them unsuitable to use in the time available to prevent HRCs.

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

2.2.1.6. Threat characteristics

Physical protection of nuclear facilities should be based on the State's current evaluation of the threat [10]. The competent authority should specify — in a design basis threat document or other statement of the threat — the threat characteristics against which the operator should provide protection. The threat characteristics are used in the VAI process to determine the malicious acts that the threat is capable of performing. Reference [11] provides guidance on the development, implementation and maintenance of a design basis threat.

2.2.2. Site and facility characteristics

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

— The site (area in which the facility is located), such as:
  • The population density in the vicinity of the facility and other site characteristics to determine the consequences of a potential radiological release when the criteria for HRCs involve off-site exposure rather than a surrogate, such as core damage or containment failure.
— The facility, such as:
  • The locations, inventory forms, characteristics, and quantities of nuclear and other radioactive material;
  • The nuclear facility's critical safety functions (e.g. shielding, criticality prevention, cooling, confinement, fire prevention, structural integrity); the detailed design information on process and safety systems needed to determine the equipment, systems, structures, components, devices, and operator actions that should be protected to prevent HRCs.

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

2.2.3. Analysis of radiological consequences

A conservative analysis should be performed to determine the potential radiological consequences of the complete release of each nuclear or other radioactive material inventory at the facility. The analysis should be performed without consideration of physical protection and mitigation measures present at the facility.

If the potential radiological consequences estimated for an inventory under these conservative analysis conditions are below the URCs, sabotage leading to URCs is not possible for this inventory[4]. Consequently, it is not necessary to designate any areas to be protected against sabotage for this inventory. For such inventories, the operator should protect safety related equipment and devices by controlling access and securing them. If the potential consequences are between the URC and HRC levels established by the State, the operator should identify the areas to be protected against sabotage and protect them as specified by State requirements. If the potential consequences are above the HRC level, the operator should identify vital areas as described in the following sections and protect them as recommended in Ref. [1].

If the conservative analysis indicates URCs, it may be appropriate to conduct a more sophisticated and resource intensive analysis to identify a more realistic estimate of the potential consequences from the same specified amount of radioactive material. The calculation of radiological consequences should be based on conservative, yet realistic, data and assumptions, considering such data as release fractions and plating. The parameters for the analysis should be defined or approved by the competent authority.

2.3. DIRECT SABOTAGE OF NUCLEAR OR OTHER RADIOACTIVE MATERIAL INVENTORY

Acts that lead directly to release of radioactive material are those that apply energy from an external source (for example, an explosive or incendiary device) to disperse the material. If the potential radiological consequences of the release of a complete inventory are equal to or greater than the HRC level, the direct dispersal of the inventory should be included in the sabotage logic model as a potential malicious act leading directly to HRCs, 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.

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

2.4. INDIRECT SABOTAGE OF NUCLEAR OR OTHER RADIOACTIVE MATERIAL INVENTORY

Malicious acts that lead indirectly to the release of nuclear and other radioactive material are the 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 equipment, systems, structures, components, devices or operator actions that normally maintain the facility in a safe state. If the potential radiological consequences of the release of a complete inventory are equal to or greater than a HRC limit, the possibility of sabotage that could lead indirectly to HRCs should be considered. To determine the areas that should be protected to prevent acts that lead indirectly to HRCs, two types of sabotage attacks should be considered, namely those:

— Causing an IE [2] that creates conditions more severe than the facility mitigating systems can accommodate (that is, events that are beyond the safety design basis);
— Causing an IE and disabling the systems needed to mitigate the effects of the IE.

An IE that is deliberately caused by an adversary in an attempt to cause a release from a facility is called an IEMO.

2.4.1. Initiating events of malicious origin

The main purpose of this step in the VAI process is to produce a list of malicious acts by which the potential adversary might initiate a chain of events leading to HRCs. Many IEs will have already been identified and analysed in facility safety documentation, such as a DSA or PSA report [3, 4], and these IEs should be considered as potential IEMOs. When identifying the IEMOs, the VAI team should consider three categories of events that may not be included in the safety case and that should be included in the VAI process:

(1) The first category of IEMOs not included in safety assessments involves situations in which there is no process energy or other energy sources present that could disperse radioactive material. For example, malicious acts involving explosives or other sources of energy for breaching or dispersal could cause barriers to fail or radioactive material to be dispersed in a manner

not possible without a malicious act. Because these IEs are not possible without a malicious act, they are not usually addressed in the safety analysis.

(2) The second, related, category of IEMOs that may not have been addressed in the safety analysis includes those IEs that are so unlikely to occur randomly that they are excluded from consideration. For example, multiple independent IEMOs or massive breaches or failures of passive components that, while extremely improbable as random events, can be accomplished by an adversary equipped with explosives or other resources, including in situ resources.

(3) The third category of IEMOs involves sources of radioactive material releases that may not have been within the scope of safety documents. Level 1 PSAs at nuclear power reactors address only events with the potential to lead to core damage and, thereby, the release of radioactive material from the reactor core. Other inventories of radioactive material that might be the source of release leading to HRCs (such as irradiated fuel and radioactive waste) also need to be considered in the VAI process.

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

(1) *Review of safety documentation.* This should be the starting point for this part of the VAI process. Lists of IEs in DSAs and PSAs, in fire analyses, seismic analyses, and other safety evaluations for the facility being analysed and for similar facilities should be reviewed. Because any of the IEs that can occur randomly may also be caused by malicious acts, this set of IEs should be included in the list of IEMOs. Note that the assumptions in safety analyses regarding the nature of these IEs and the plant response to them should be reexamined in the context of malicious acts and revised where appropriate.

(2) *Reference to other VAI analyses.* Where other VAI analyses have been performed for similar facilities, lists of the IEMOs used should be reviewed. It is particularly important to identify IEMOs that do not correspond to IEs in facility safety documentation.

(3) *Engineering evaluation.* The facility systems (operational and safety) and major components should be systematically reviewed to identify any additional IEMOs, for example where any consequences of malicious acts of which the potential adversary is deemed capable (e.g. disabling, causing to operate spuriously, breaching, disrupting, collapsing, or igniting) could

lead directly, or in combination with other malicious acts, to HRCs. Guidance for these analyses can be found in Ref. [12].

(4) *Deductive analysis*. In this approach, 'unacceptable radiological consequences' are systematically decomposed into all possible events that could cause it to occur. Successful operation of systems and other preventive actions are not included. The events at the most fundamental level are then candidates for the list of IEMOs for the facility.

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

2.4.2. IEMOs that exceed mitigating system capability

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

2.4.3. IEMOs that are within mitigating system capability

In order to address IEMOs that are within mitigating system capability, the combinations of IEMOs and mitigating system disablement events that could lead to HRCs should be determined. The mitigating system includes operator actions. These combinations of events that lead indirectly to HRCs are detailed in the sabotage logic model. The possibility that the threat could cause the IEMOs or disablement events is addressed when the threat characteristics are considered later in the process.

The specific systems that are used to mitigate IEs depend upon the facility and the amount or type of the radioactive material it contains; these systems may differ depending upon the facility's operational state. Systems that are used to mitigate IEs are ones that support safety functions such as reactivity control, decay heat removal, coolant boundary integrity, and containment integrity. The concept of safety functions is discussed in Refs [2, 4]. The systems that directly perform critical safety functions are defined to be front line systems, while those required for proper functioning of the front line systems are defined to be support systems [4]. The successful operation of a front line system may depend upon the availability of one or more support systems; it is essential that these dependencies be identified.

If a PSA has been prepared for the facility, the information on front line and support systems should be readily available from the PSA or supporting documentation [7]. If only a DSA is available, then the VAI team can usually derive most or all of this information from the accident analyses employing engineering judgment. If the DSA lists safety groups, these lists can be helpful in identifying front line systems and their dependencies. However, there may be other dependencies, beyond the safety analysis, that relate to specific malicious acts or sabotage scenarios. For example, explosive breaching of a cooling water pipe may cause flooding that disables equipment near or below the pipe breach. Such spatial interactions should be analysed in the VAI process (Section 2.7.3).

Successful operation of a front line system ('success criteria') means the minimum performance needed for the fulfillment of the system's safety function under the specific conditions created by an IEMO [8]. Relevant information for developing front line system and support system success criteria is given in facility safety analyses. The success criteria for front line systems are of particular importance for the VAI analysis because they define the starting points for the subsequent logic modeling of the system sabotage scenarios. Success criteria include performance measures (e.g. flow rate, response time), and also hardware requirements, such as the number of required flow paths, power trains, etc.

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

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

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

The steps discussed in Section 2.6 generate:

— A list of IEMOs that exceed the mitigation capability of facility systems;
— A list of IEMOs that can be mitigated and the front line systems and support systems needed to respond to each one;
— Front line and support system success criteria for each IEMO that can be mitigated;
— References to supporting documentation;
— Grouping of IEMOs (if needed).

2.5. SABOTAGE LOGIC MODEL

The next step in performing a VAI is constructing a sabotage logic model that identifies the events or combinations of events that could lead to HRCs necessitating protection in vital areas, including the direct dispersal of radioactive material, IEMOs that exceed mitigating system capacity, and the combinations of events that will lead to HRCs for IEMOs that are within mitigating system capacity. A logic model can be a statement; an algebraic expression; or a graphical representation, such as a fault tree or an event tree. The sabotage logic model includes all direct dispersal events and all IEMOs and associated mitigating system failures that will cause HRCs.

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

Information provided in the facility safety analyses and other safety documentation can be used to develop the sabotage logic model for IEMOs within mitigating system capability. Typically, this is done in two stages. The first stage is the development of the facility sabotage logic model that represents the combinations of IEMOs and disablement of front line systems leading to HRCs. This is accomplished using information discussed in Sections 2.4.1, 2.4.2 and 2.4.3 and information from the facility safety analysis. The second stage is developing sabotage logic models for individual front line systems and the support systems they are dependent upon. This activity is performed either by modifying existing logic models from the facility PSA, if one has been prepared, or by developing logic models using facility system configuration information

and the success criteria and dependency information. This process produces the portion of the facility sabotage logic model that links each IEMO with the disablement of the front line systems and corresponding support systems and operator actions that are required to mitigate the IEMO.

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

2.6. CAPABILITY OF THREAT TO PERFORM SABOTAGE EVENTS

The sabotage events addressed in the preceding sections do not consider the capability of the threat to perform the malicious acts. Indeed, all events that could lead directly or indirectly to HRCs are included to ensure that no potential vital areas are overlooked without regard to whether the assumed threat capabilities are sufficient to perform the sabotage acts. If the assumed threat characteristics change, the information and models developed in the preceding steps will be valid for use in identifying vital areas under the changed threat conditions[5].

In this step of the process, any events that are not credible given the assumed threat capabilities should be eliminated from consideration. The threat's capability to perform the direct dispersal of material (Section 2.3), to cause an IEMO (Section 2.4.1), and to disable mitigating systems (Section 2.4.3) should be assessed. Events that are beyond the capability of the threat may be removed from the sabotage logic model.

In addition, any events that are beyond the ability of the facility physical protection system to prevent should be identified. In the analysis of the sabotage logic model, any such events will be assumed to occur always. Generally, any events that the threat can accomplish without gaining access to the site should be assumed to occur. For example, it is practically impossible for the facility physical protection system to prevent the loss of off-site power; the threat can cause loss of off-site power in many ways without gaining access to the facility. Therefore, the VAI process should assume that off-site power is unavailable. Any other such events in the sabotage logic model should be identified and highlighted for proper treatment in the area identification process described in Section 2.7.

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

2.7. SABOTAGE AREA LOGIC MODEL

The next step in the VAI process is identifying and documenting the areas from which an adversary could accomplish each event in the sabotage logic model. The information about these areas is collected through a structured process and verified by conducting a walkdown of the facility. Spatial interactions among the adjacent areas should also be considered as discussed below.

2.7.1. Data collection and entry

The area data are entered into the sabotage logic model by replacing each event (each direct dispersal event, IEMO, and each mitigating system disablement event) in the model with the area or areas in the nuclear facility from which it can be caused. The result is a sabotage area logic model. The sabotage area logic model can then be solved as described in the following section to determine the combinations of areas from which malicious acts could cause HRCs and the minimum combinations of areas that should be protected to prevent HRCs.

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

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

2.7.2. Walkdown

Area information should be verified by conducting a VAI walkdown. In preparation for the VAI walkdown, the team should review the location information[6]. The VAI walkdown team should include representatives from the facility safety, security, design and operating organizations.

The main objectives of the VAI walkdown are to:

— Verify the areas from which the threat could accomplish direct dispersal;
— Verify the set of areas from which the threat could accomplish each IEMO identified in Section 2.4;
— Verify the set of areas from which the threat could accomplish each of the actions to disable equipment, systems, structures, components, devices or operator actions that are identified in the sabotage logic model;
— Assess the potential for spatial interactions between adjacent areas.

2.7.3. Spatial interactions

Additional consideration is required to address spatial interactions between adjacent areas. There may be cases in which a malicious act in one area can disable equipment, components, or devices in one or more adjacent areas. External event PSAs, such as seismic, fire and flooding PSAs, and Ref. [12] provide useful information on spatial interactions.

2.8. CANDIDATE VITAL AREA SETS

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

(1) *Identify target sets*: The sabotage area logic model is analysed to determine all combinations of areas to which an adversary would have to gain access in order to complete sabotage scenarios that could lead to HRCs. Each such combination of areas is a minimal cut set of the sabotage area logic model, and represents the full set of target areas an adversary needs to penetrate in order to accomplish a sabotage scenario. The combinations of areas from which malicious acts could cause HRCs can be useful in developing and

[6] For new designs, an analysis of the vital areas should be made prior to construction. The walkdown is conducted prior to turnover of the facility to the operator to confirm the analysis. Reference [12] includes a discussion of walkdowns.

evaluating the facility physical protection programme. These combinations of areas can be reviewed to identify potential adversary targets as a basis for development of sabotage scenarios for physical protection system design and evaluation.

(2) *Identify protection sets*: The sabotage area logic model is analysed to determine the minimum combinations of areas that should be protected in order to ensure that no sabotage scenarios could be completed. This step is accomplished by finding prevention sets [13] for the sabotage area logic model. Each prevention set presents an option of what could be protected to prevent all sabotage scenarios. A level 1 prevention set contains at least one area from each of the minimal cut sets of the sabotage area logic model (and is equivalent to one of the solutions for the Boolean complement of that logic model). If the adversary is prevented from gaining access to all the areas in one prevention set, he will not be able to complete any of the sabotage attacks represented in the sabotage area logic model. Each of the level 1 Prevention sets contain a minimum complement of equipment, systems, structures, components, devices and/or operator actions that, if protected against sabotage, ensures that no sabotage attacks can be completed. Protection of each area in any one of these sets will prevent all sabotage scenarios that could lead indirectly to HRCs[7].

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

2.9. VITAL AREA SET SELECTION

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

Each of the candidate vital area sets meets the recommendation in Section 7.1.5 of Ref. [1] for a set of facility vital areas. The facility operator may choose to protect any one of the candidate vital area sets. In making the selection of a set of areas to protect, the operator could take into account various factors important

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

to safe and efficient operation of the facility. For example, the operator might select the candidate vital area set that provides the optimum combination of:

— Low impacts on safety, plant operations, and emergency response;
— Low difficulty of providing protection;
— High effectiveness of protection measures; and
— Low cost of protecting the vital areas.

It is unlikely that one candidate vital area set will receive the highest rating for each the selection criteria. Thus, it will be necessary to affect 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 the analytical hierarchy process). References [14, 15] provide examples of structured trade-off analysis methods.

The results of vital area selection process are:

(1) A table that evaluates each of the candidate vital area sets in terms of each of the attributes considered in the selection of a vital area set and documents the aggregate score or ranking of each candidate vital area set, with associated rationale.
(2) A recommended vital area set based on the best overall score or ranking.

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

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

3. DOCUMENTATION OF RESULTS

3.1. OBJECTIVES AND PRINCIPLES OF DOCUMENTATION

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

3.2. ORGANIZING DOCUMENTATION

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

(1) *Traceability.* For review and updating of the analysis, it should be possible to trace any information with minimum effort.
(2) *Sequentiality.* The order of appearance of the analysis in the report should follow the order in which the analysis was performed, namely:
    — Input:
        • Basic assumptions used in the process;
        • Conservative analysis results.
    — Potential direct dispersal events;
    — Identification of IEMOs;
    — Identification of safety systems that mitigate IEMOs;
    — Logic model development;
    — Threat capability assessment;
    — Sabotage event area identification;
    — Identification of candidate vital area sets;
    — Selection of a set of vital areas.

3.3. PROTECTING INFORMATION

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

Appendix

EXAMPLE OF A SABOTAGE LOGIC MODEL

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

A logic model can be a statement, an algebraic expression or a graphical representation such as a fault tree or an event tree. The solution of different representations for the same logical problem will give the same results. A logic model is 'solved' by applying the rules of Boolean algebra to the model. Table 2 provides definitions of common logic symbols and Boolean algebra rules.

Consider a fictitious facility that has the following characteristics:

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

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

The statements above constitute one form of a logic model for sabotage of the facility. By carefully analysing these statements, we could determine the combinations of locations that a saboteur would have to enter to cause all the IEs and component failures that would lead to HRCs. For example, if a saboteur could gain access to L2 and L8 he could initiate IE1 and disable S1, resulting in a release that exceeds HRC limits. The saboteur can cause IE1 if he gains access to L8. If the saboteur disables both T1 and T2, S1 will not be able to mitigate IE1. Disabling C2 can disable T1 and disabling C3 can disable T2. Both C2 and C3 can be disabled from L2, so by gaining access to both L2 and L8 the saboteur can cause HRCs. By reviewing the statements and location table in detail, all the combinations of locations from which IEs can occur sufficient to cause HRCs could be identified.

As long as the facility is simple enough, it is possible to derive the location combinations from which sabotage can be accomplished by inspection as done in the previous paragraph. A more useful approach is to represent the relationships between IEs, disablement events and locations in a logic equation. The event to be represented in this logic equation is release in excess of HRCs. Using the definitions in Table 2, the following equations are developed corresponding to statements 1 through 5 above:

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

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

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

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

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

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

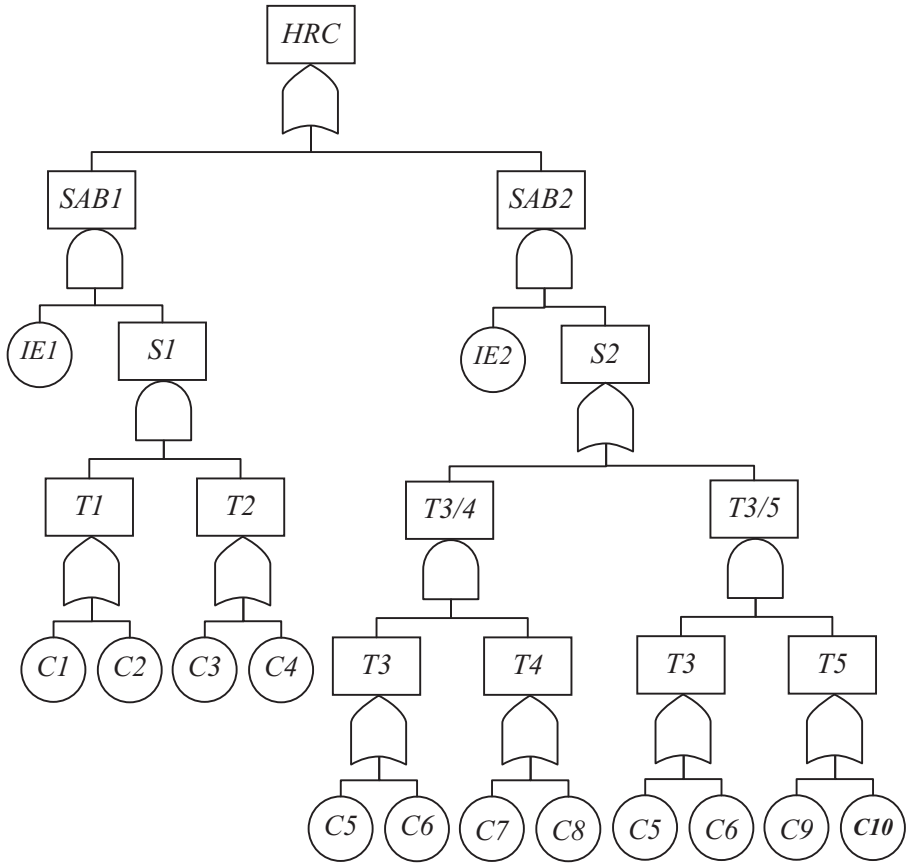
$$\begin{aligned}\text{HRC Prevented} = {} & \underline{L8}*\underline{L9} + \\ & \underline{L8}*\underline{L3} + \\ & \underline{L2}*\underline{L9} + \\ & \underline{L2}*\underline{L3} + \\ & \underline{L8}*\underline{L5}*\underline{L6} + \\ & \underline{L2}*\underline{L5}*\underline{L6}\end{aligned} \tag{18}$$

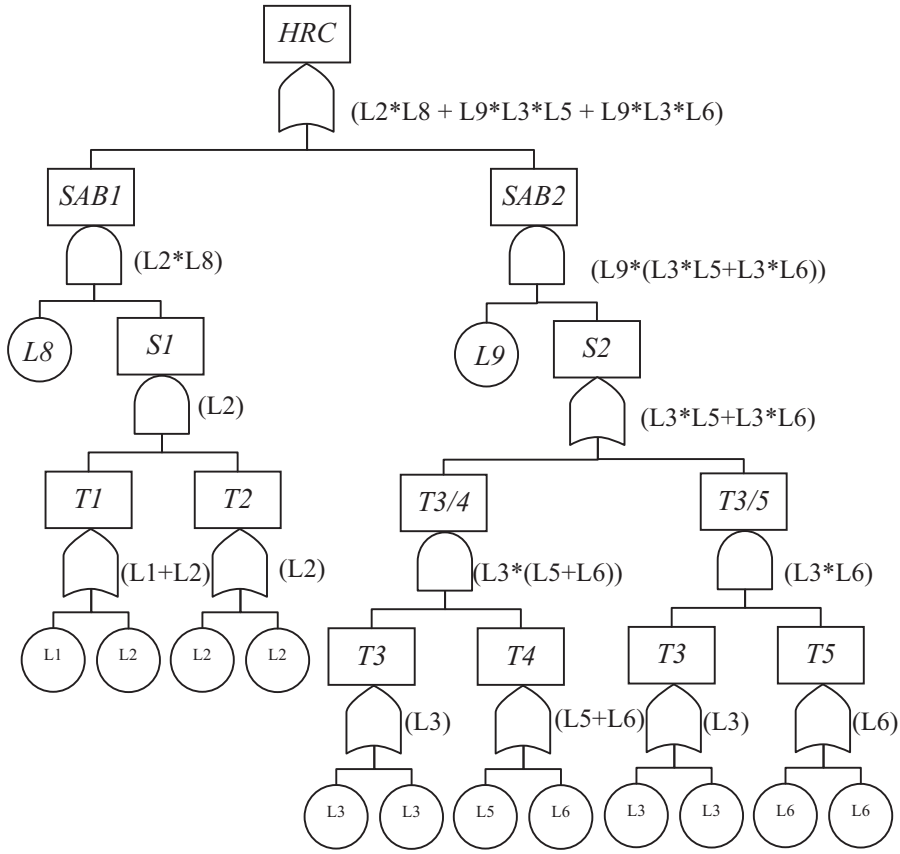
In Eq. (18), the underline indicates that access to the location is prevented; for example, L8 means access to L8 is prevented. In Boolean algebra terms, L8 is the complement (non-occurrence or NOT) of L8. For the example facility, there are six candidate vital area sets as shown in equation 18. This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

Fault trees can be used to efficiently represent the sabotage logic for more complicated facilities. Figure 2 provides a fault tree for the example facility that will be solved to further illustrate the process of identifying candidate vital area sets. The top event in this tree is release in excess of HRC limits (represented by the symbol HRC). The logic gates show the ways the events in the tree combine to cause the top event, and the tree is developed down to the level of component failures. Figure 3 shows the fault tree with all terminal events replaced with the locations from which the events can be caused. This sabotage location fault tree is solved using the Boolean algebra concepts applied in Eqs (1) through (17) to produce the same results. The expression in parenthesis beside each gate is the solution for the gate in terms of the terminal events in the tree. One way to generate the level 1 protection sets for a fault tree is to form and solve the dual for the tree. The dual of a fault tree is formed by changing each OR gate in the tree to an AND gate, each AND gate to an OR gate, and each event to the complement (NOT) of the event. There are a variety of software packages available for solving fault trees and generating the prevention sets (candidate vital area sets) needed in the VAI process.

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

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


HRC
SAB1
SAB2
IE1
S1
IE2
S2
T1
T2
T3/4
T3/5
C1
C2
C3
C4
T3
T4
T3
T5
C5
C6
C7
C8
C5
C6
C9
C10


HRC
(L2*L8 + L9*L3*L5 + L9*L3*L6)
SAB1
SAB2
(L2*L8)
(L9*(L3*L5+L3*L6))
L8
S1
L9
S2
(L2)
(L3*L5+L3*L6)
T1
T2
T3/4
T3/5
(L1+L2)
(L2)
(L3*(L5+L6))
(L3*L6)
L1
L2
L2
L2
T3
T4
T3
T5
(L3)
(L5+L6)
(L3)
(L6)
L3
L3
L5
L6
L3
L3
L6
L6

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/ Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

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

[6] VARNADO, G.B., ORTIZ, N.R., Fault Tree Analysis for Vital Area Identification, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, Nuclear Regulatory Commission, Washington, DC (1979)

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

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Facilities and Nuclear Material against Sabotage, IAEA, Vienna (in preparation)

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary 2007 Edition, IAEA, Vienna (2007).

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[13] WORRELL, R.B., BLANCHARD, D.P., "Top event prevention analysis: A deterministic use of PRA", Probabilistic Safety Assessment Methodology and Application (Proc. Int. Conf. Seoul, 1995).

[14] KEENY, R. L., RAIFFA, H., Decisions with Multiple Objectives: Preferences and Value Tradeoffs, Wiley, New York (1976).

[15] SAATY, T. L., Decision Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World, Analytic Hierarchy Process Series, Vol. 2, RWS Publications, Pittsburgh (2002).

DEFINITIONS AND ABBREVIATIONS

The following definitions are used for the purpose of this publication.

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

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

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

direct dispersal or release. Dispersal or release of material by application of energy from an external source (for example, an explosive or incendiary device) on the material.

front line system. A system that directly performs a facility safety function. See also the definition of support system.

indirect dispersal or release. Dispersal or release of material by utilizing the potential energy (i.e. heat or pressure) contained in the nuclear or radioactive material or in a process system to disperse the material.

initiating event (IE). An event identified during design as capable of leading to antcipated operational occurrences or accident conditions. Referred to in Ref. [9] as a postulated IE.

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

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

minimal cut set. A minimal cut set is a smallest set of events sufficient to cause the outcome of a logic model. For a fault tree, a minimal cut set is a smallest set of basic events that will cause the top event to occur.

physical protection. Measures (including structural, technical and administrative protective measures) taken to prevent an adversary from achieving an undesirable consequence (such as radiological sabotage, or the unauthorized removal of nuclear or other radioactive material in use, storage or transport) and to mitigate or minimize the consequences if the adversary initiates such a malicious act.

prevention set. A prevention set is a smallest set of events that will prevent the outcome of a logic model. For a fault tree, a prevention set is a smallest set of basic events that should be prevented in order to prevent the top event.

probabilistic safety assessment (PSA). A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk [9].

protected area. Area inside a limited access area, containing category I or II nuclear material, and/or sabotage targets surrounded by a physical barrier with additional physical protection measures.

sabotage. Any deliberate act directed against a nuclear facility or nuclear and other radioactive 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.

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

success criteria. The minimum system performance that will allow for performance of a system safety function under the specific conditions created by an initiating event.

support system. A system required for the proper functioning of one or more front line system(s)

threat. A person or group of persons with motivation, intention and capability to commit a malicious act**.**

unacceptable radiological consequences (URCs). A level of radiological consequences, established by the State, above which the implementation of physical protection measures is warranted

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 high radiological consequence.

MEETINGS TO PREPARE THIS PUBLICATION

Consultants Meetings

Vienna, Austria7–11 June 2004;
Vienna, Austria, 6–10 June 2005;
Seoul, Republic of Korea, 6–10 December 2005

Technical Meeting

Vienna, Austria, 18–22 September 2006

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

CHINA
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CZECH REPUBLIC
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Email: romuald.verrier@lavoisier.fr • Web site: http://www.lavoisier.fr

GERMANY
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Telephone: + 49 228 94 90 20 • Fax: +49 228 94 90 20 or +49 228 94 90 222
Email: bestellung@uno-verlag.de • Web site: http://www.uno-verlag.de

HUNGARY
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net

ITALY
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Website: www.libreriaaeiou.eu

JAPAN
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

REPUBLIC OF KOREA
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746 • Web site: http://www.kins.re.kr

NETHERLANDS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Telephone: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Email: books@delindeboom.com • Web site: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888
Email: infoho@swets.nl • Web site: http://www.swets.nl

NEW ZEALAND
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

SLOVENIA
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

SPAIN
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63
Email: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

UNITED NATIONS
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

UNITED STATES OF AMERICA
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com · Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

11-34851

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 15
STI/PUB/1488 (33 pp.; 2011)
ISBN 978–92–0–112210–0 Price: €23.00

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 14
STI/PUB/1487 (35 pp.; 2011)
ISBN 978–92–0–112110–3 Price: €22.00

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (62 pp.; 2011)
ISBN 978–92–0–111110–4 Price: €28.00

INTERNATIONAL LEGAL FRAMEWORK FOR NUCLEAR SECURITY
IAEA International Law Series No. 4
STI/PUB/1486 (30 pp.; 2011)
ISBN 978–92–0–111810–3 Price: €26.00

DEVELOPMENT AND APPLICATION OF LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. SSG-3
STI/PUB/1430 (195 pp.; 2010)
ISBN 978–92–0–114509–3 Price: €35.00

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT
IAEA Nuclear Security Series No. 10
STI/PUB/1133 (72 pp.; 2009)
ISBN 92–0–116702–4 Price: €20.50

ENGINEERING SAFETY ASPECTS OF THE PROTECTION OF NUCLEAR POWER PLANTS AGAINST SABOTAGE
IAEA Nuclear Security Series No. 4
STI/PUB/1271 (58 pp.; 2007)
ISBN 92–0–109906–1 Price: €30.00

AMENDMENT TO THE CONVENTION ON THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL
IAEA International Law Series No. 2
STI/PUB/1275 (158 pp.; 2006)
ISBN 92–0–110806–0 Price: €48.00

This publication provides detailed guidance on the identification of vital areas. It presents a structured approach to identifying the areas that contain equipment, systems and components to be protected against sabotage. The method builds upon safety analyses to develop sabotage logic models for sabotage scenarios that could cause unacceptable radiological consequences. The sabotage actions represented in the logic models are linked to the areas from which they can be accomplished. The logic models are then analysed to determine areas that should be protected to prevent these unacceptable radiological consequences.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–114410–2
ISSN 1816–9317