

IAEA NUCLEAR SECURITY SERIES

**Step 8: Soliciting comments by
Member States**

Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities

NST063

DRAFT TECHNICAL GUIDANCE

\

CONTENTS

1. INTRODUCTION	1
BACKGROUND.....	1
OBJECTIVE.....	2
SCOPE	2
STRUCTURE.....	3
2. GENERAL OVERVIEW OF PROTECTION OF NUCLEAR FACILITIES AGAINST SABOTAGE	3
THREAT ASSESSMENT FOR SABOTAGE	4
BASIS FOR A GRADED APPROACH FOR PROTECTION AGAINST SABOTAGE	5
OVERVIEW OF THE PROCESS FOR SABOTAGE TARGET AND VITAL AREA IDENTIFICATION	7
3. INPUT DATA FOR THE SABOTAGE TARGET IDENTIFICATION PROCESS	8
DETERMINATION BY THE STATE OF UNACCEPTABLE AND HIGH RADIOLOGICAL CONSEQUENCES	9
IDENTIFICATION OF POTENTIAL TARGETS	9
DETERMINATION OF FACILITY STATES TO BE ASSESSED	10
THREAT CHARACTERISTICS	14
SITE AND FACILITY CHARACTERISTICS.....	14
4. DEVELOPING SABOTAGE ATTACK SCENARIOS	15
ADDRESSING DIRECT AND SEMI-DIRECT ACTS OF SABOTAGE.....	15
ADDRESSING INDIRECT ACTS OF SABOTAGE: IDENTIFYING INITIATING EVENTS OF MALICIOUS ORIGIN.....	16
CREDIBILITY OF SABOTAGE ACTS.....	19
5. IDENTIFYING POTENTIAL SABOTAGE TARGETS	20
SABOTAGE LOGIC MODEL	20
IDENTIFICATION OF AREAS AND FACILITY WALKDOWN	21
SABOTAGE AREA LOGIC MODEL.....	22
6. VITAL AREA IDENTIFICATION	22
VITAL AREA SET SELECTION.....	23
VULNERABILITY EVALUATION OF SABOTAGE TARGETS	24
7. OFF-SITE SABOTAGE ATTACKS	25
CONSIDERATIONS FOR TYPE 2 SABOTAGE ATTACK SCENARIOS.....	25
DEVELOPMENT AND SELECTION OF FACILITY SPECIFIC ATTACK SCENARIOS	27
SABOTAGE MARGIN ASSESSMENT FOR TYPE 2 SABOTAGE ATTACK SCENARIOS.....	29
IDENTIFICATION OF ONE OR MORE FACILITY SUCCESS PATHS.....	32

CONSIDERATIONS FOR THE METHODOLOGY OF COPING WITH IDENTIFIED
VULNERABILITIES OF CRITICAL SSCs.....33

8. DOCUMENTATION AND INFORMATION PROTECTION.....35

 SECURITY OF SENSITIVE INFORMATION.....35

REFERENCES37

ANNEX I: EXAMPLE OF SABOTAGE LOGIC MODEL40

ANNEX II: FACILITY WALKDOWN47

ANNEX III: EXAMPLE OF EXTREME ENVIRONMENT LOAD EVALUATION55

DRAFT

1. INTRODUCTION

BACKGROUND

1.1. The Convention on the Physical Protection of Nuclear Material as amended (A/CPPNM) [1] defines sabotage as, "...any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances." The A/CPPNM obligates State Parties to establish an appropriate physical protection regime applicable to nuclear material and nuclear facilities under its jurisdiction, with the aim of protecting against sabotage and/or preventing, mitigating or minimizing radiological consequences of sabotage. IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2], contains recommended requirements for the protection against sabotage while applying the principle of a graded approach, based on an analysis of the potential consequences.

1.2. This publication provides guidance on identifying the set of structures, systems and components (SSCs) of nuclear facilities as well as material and associated operator actions that need to be protected against sabotage.

1.3. In particular, this publication provides guidance on how to implement recommended requirements set out in Ref. [2] related to sabotage target identification and identification of vital areas. This publication also supports the guidance provided in IAEA Nuclear Security Series No.27-G Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [3].

1.4. This publication refers to cyber-attacks only as a capability of an adversary to degrade nuclear security measures in support of a physical attack. IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities [4] provides detailed guidance on the computer security aspects of protection against all forms of cyber-attack.

1.5. This publication also builds on the threat assessment presented in IAEA Nuclear Security Series No. 10-G (Rev. 1), National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements [5], and can be used to provide input to the design of nuclear security systems and measures.

1.6. This publication supersedes IAEA Nuclear Security Series No. 4¹, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, and IAEA Nuclear Security Series No.16, Identification of Vital Areas at Nuclear Facilities².

OBJECTIVE

1.7. The objective of this Technical Guidance is to provide guidance for States and/or operators for analyzing the potential effects of sabotage events on a nuclear facility and on actions that can be taken to mitigate these effects.

1.8. Detailed guidance is provided for the identification of potential sabotage targets in a nuclear facility. Guidance is also provided for identifying SSCs and associated operator actions presenting potential vulnerabilities that could, if an initiating event of malicious origin (IEMO) were to take place, lead to unacceptable or high radiological consequences. Identification of vital areas is also addressed. Further, this publication includes guidance to assist States in accounting for the potential risks to a facility associated with stand-off sabotage events.

1.9. This publication is intended for use by States, competent authorities (including the regulatory body), relevant technical and scientific support organizations, and the operators of facilities and activities associated with nuclear and other radioactive material. Specifically, this publication is meant to support any of the above users who are involved in the protection of nuclear material and other radioactive material against sabotage.

SCOPE

1.10. This Technical Guidance applies to all nuclear facilities. It is particularly relevant for nuclear facilities where a successful act of sabotage could result in unacceptable radiological consequences (URC) or high radiological consequences (HRC), as defined by the State.

1.11. This publication does not address in detail the design of specific nuclear security systems and measures. IAEA Nuclear Security Series No. 40-T, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities [6], paragraph 1.6, states that its contents, "...focuses primarily on the design, equipment selection and operational steps of designing, implementing and sustaining a [physical protection system]."

1.12. This publication also does not address the identification of targets for unauthorized removal of nuclear material or response planning to mitigate the consequences resulting from sabotage. These topics are covered in IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [7], and Refs. [2 and 3].

¹ 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).

² INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, Technical Guidance, IAEA, Vienna (2012).

1.13. This publication also does not address the identification of cyber-attack targets to affect sabotage through the maloperation of functions performed by computer-based systems important to or related to nuclear safety and nuclear security. The identification and characterization of computer-based systems that may be targeted for exploitation with a cyber-attack to compromise safety, security or nuclear material accounting and control functions is covered in IAEA Nuclear Security Series No. 17-T Rev. 1, Computer Security Techniques for Nuclear Facilities [4]. Ref [4] also provides detailed guidance on the design and implementation of computer security policy, programmes and measures to provide for the protection of computer-based systems against compromise.

1.14. The process and methodology for sabotage target identification presented in this publication may also be applicable to other radioactive material associated facilities, other high-valued assets and SSCs and associated operator actions³ associated with facility operation and nuclear material processing.

STRUCTURE

1.15. After this introductory section, Section 2 provides a general overview of the methodology of protection against sabotage. Section 3 sets out the input that is necessary for the completion of the sabotage target identification process. Section 4 describes the process of developing sabotage attack scenarios. Section 5 presents the process of identifying potential sabotage targets, Section 6 describes identifying sabotage targets to be protected in vital areas, and Section 7 provides information on extreme sabotage situations. Finally, Section 8 discusses the protection of documentation and information related to the identification of vital areas and sabotage targets. Three annexes are provided to give practical examples on the sabotage logic model, facility walkdowns and extreme environment load evaluation.

2. GENERAL OVERVIEW OF PROTECTION OF NUCLEAR FACILITIES AGAINST SABOTAGE

2.1. The general objective of nuclear safety is, as defined in the Fundamental Safety Principles as “to protect people and the environment from harmful effects of ionizing radiation” [8]. The Nuclear Security Fundamentals in IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State’s Nuclear Security Regime, define “The objective of a State’s nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event” [9].

2.2. Sabotage is a severe nuclear security event that could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances. The success of an act of sabotage could result in conditions that challenge the above quoted safety objective and security objective. The success of an act of sabotage necessitates the successful defeat of not only the nuclear security system, but also the facility safety systems and accident management provisions. Therefore, measures to protect against sabotage should be designed and evaluated with cooperation between nuclear safety experts and nuclear security experts.

³ Associated operator actions are actions associated with structures, systems and components performed by the operating personnel.

2.3. The following sub-sections will provide a general overview of nuclear security for sabotage, including threat assessment, applying a graded approach and a short overview of the process for sabotage target and vital area identification described in the remainder of the publication.

THREAT ASSESSMENT FOR SABOTAGE

2.4. To protect a nuclear facility against sabotage, the first step is to perform a national nuclear security threat assessment. A national nuclear security threat assessment is an evaluation of the existing nuclear security related threats to determine the attributes and characteristics of potential adversaries. This national nuclear security threat assessment process makes use of global, regional and national sources of information. Detailed information on performing a nuclear security threat assessment is provided in Ref. [5].

2.5. Both this threat assessment and the consequences of a successful sabotage attempt should be taken into account in the development of a design basis threat (DBT) or representative threat statement (RTS), as set out in Ref. [5]. This DBT should be disseminated to the operators.

2.6. If a performance-based regulatory approach is used, facility-specific sabotage attack scenarios should then be developed by the operators, based on the facility specific DBTs. These scenarios should be used to design the nuclear security systems. If a prescriptive regulatory approach is used, the RTS should be used by the regulatory body to develop sabotage attack scenarios and then to establish the corresponding physical protection requirements. The goal of the sabotage attack scenarios should be to counter an act of sabotage and to meet the nuclear security objectives established in the State's nuclear security regime.

2.7. Sabotage attack scenarios can be of either of two types: type 1 sabotage attack scenarios or type 2 sabotage attack scenarios. Sabotage attack scenario type 1 represents scenarios involving insiders or external adversaries intending to intrude into the facility to commit their act (with or without insider assistance), including cyber threats blended with physical attacks.

2.8. Type 2 sabotage attack scenarios include attacks launched from outside the plant boundary that do not require the presence of adversaries on the site. Examples may include standoff attacks such as airborne attacks using drones, missiles, airplanes or attacks using directed energy weapons; blasts from chemical explosions; or destruction of a heat sink. Some type 2 sabotage attack scenarios may be addressed by the strengthening of the facility nuclear security system; however, others can present a significant challenge.

2.9. Type 1 sabotage attack scenarios provide a basis for the design of the facility nuclear security system against sabotage. The nuclear security system should be designed to detect, delay and respond to a malicious act as defined in credible sabotage attack scenarios based on the DBT or RTS. Examples of detection, delay and response measures can be found in Refs. [3] and [6]. To design an appropriate response to a sabotage, the immediate operator actions related to restoration of disabled systems need to be taken into consideration. When considering sabotage, "State requirements for physical protection should be based on the concept of defence in depth," as stated in Ref. [2].

2.10. The distinction between sabotage attack scenarios requiring the physical presence of an adversary on the site and the scenarios that not requiring physical presence on the site is made to reflect the differences in the ways engineering measures are considered in countering each

type of sabotage attack scenarios. For type 1 sabotage attack scenarios, when adversaries initiate acts of sabotage after intrusion to the site, the engineering measures become an additional layer of defence in depth. For type 2 sabotage attack scenarios, when adversaries are acting from outside the facility boundary, engineering measures provide the main elements of protection against sabotage.

2.11. The risks associated with threats that are capable of resulting in URC can be reduced, but will never be zero. It is also unlikely that a single organization will be capable of implementing a system to adequately reduce the risk of sabotage alone. Therefore, success criteria for protection against sabotage could be a combination of the following:

- (a) Defeat of sabotage attack scenarios developed based on DBT/RTS by the nuclear security system;
- (b) Prevention of URC by safety systems and accident management; and
- (c) Effective mitigation of radiological consequences by taking on-site and off-site emergency response actions as required in IAEA Safety Standards Series No. GSR Part 7⁴ [15].

BASIS FOR A GRADED APPROACH FOR PROTECTION AGAINST SABOTAGE

2.12. A graded approach to nuclear security involves the development of physical protection requirements by the regulator based on “the current evaluation of the threat, the relative attractiveness, the nature of the nuclear material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear facilities” [2]. Specific recommendations regarding considerations for protection against sabotage following a graded approach can be found in Section 5 of Ref. [2].

2.13. For a nuclear facility, an analysis, validated by the competent authority, should be performed to determine whether the radioactive material inventory has the potential to result in unacceptable radiological consequences, as determined by the State. This analysis should only consider the inventory of the facility, and should assume that the sabotage acts will be successfully completed, and not account for any physical protection or mitigation measures.

2.14. On the basis of this analysis, the State should consider the range of radiological consequences that can be associated with all of its nuclear facilities and should appropriately categorize these radiological consequences, as described below. In particular, potential radiological consequences that exceed the limits established by the State for URC should be identified.

2.15. The categorization of potential radiological consequences resulting from a sabotage attack should associate the potential consequences with corresponding requirements and measures. For example, a three-tier association of radiological consequences with physical protection requirements could be applied as follows:

⁴ To enable on-site and off-site emergency arrangements be designed to enable mitigating effectively the consequences of an emergency triggered by such nuclear security events, results of the threat assessment for sabotage should inform the hazard assessment for emergency preparedness and response purposes in line with Req. 4 of IAEA Safety Standards Series No. GSR Part 7. Further guidance in this regard can be found in IAEA Safety Standards Series no. GS-G-2.1 and EPR Protection Strategy 2020.

- a) For radiological consequences below unacceptable radiological consequences, prudent management practices should be applied.
- b) For radiological consequences greater than the State's definition of URC, but lower than the State's definition of HRC, "...the operator should identify equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to this condition as potential sabotage targets and protect them in accordance with the following design process and protection requirements" [2].
- c) For consequences greater than HRC, in addition to those measures applied for URC, "a minimum set of equipment, systems or devices needed to prevent high radiological consequences, should be located within one or more vital areas, located inside a protected area" [2]. HRC can be attributed to facilities such as a nuclear power plant, or other facilities with comparable material inventories.

It is the responsibility of the State to assign facilities to a level of consequence, based on the material inventory.

2.16. For States with a number of nuclear facilities, it may be appropriate to divide the range between URC and HRC by defining more tiers than the three described above. This would enable the operator to implement nuclear security measures that more adequately balance the risk for each level of potential radiological consequences, potentially resulting in a more effective allocation of resources. Additional tiers beyond the three described above could, for example, account for the differences in the material inventories or material attractiveness at various facilities. These categorizations ultimately attempt to allow for the most effective application of the graded approach.

2.17. A graded approach should then be taken to appropriately reduce any identified security risks, as needed. Facility operators should identify SSCs, associated operator actions or nuclear or other radioactive material, which, if sabotaged, could directly or indirectly lead to unacceptable radiological consequences. These SSCs, associated operator actions and nuclear material should then be identified as potential sabotage targets and protected accordingly.

2.18. Following a graded approach, the stringency of the nuclear security measures put into place for individual SSCs or associated operator actions may depend on the potential radiological consequences that could result from the compromise or cessation of their operability. In general, the level of physical protection should be driven by the radioactive material inventory and the potential radiological consequences. In addition, the operator may choose to protect more stringently SSCs and associated operator actions that, if sabotaged, would immediately lead to URC or HRC than those the sabotage of which would constitute one step in a series of sabotage acts needed to initiate an URC or HRC. In addition, to address concerns regarding insider threats, more stringent access control could be put into place for some SSCs, based on operational needs.

2.19. Security systems as a whole are designed using the principle of defence in depth, "... a concept of several layers and methods of protection that have to be overcome or circumvented by an adversary in order to achieve his objectives" [2]. Even the best security measures are only effective against a finite number of sabotage attack scenarios, typically limited by the design basis threat as defined by the State, as discussed in the preceding sub-section. Therefore, security measures may ultimately fail during the course of an attack exceeding the capabilities

defined in the design basis threat or representative threat statement. Even in this case, the nuclear safety systems of a facility may prevent URC or HRC.

2.20. Specific criteria should be established to assess the risks associated with threats that are capable of resulting in URC or HRC. The following is a sample set of questions that should be assessed by the competent authority and/or the operator:

- (a) Is the nuclear facility sufficiently robust to prevent immediate, uncontrolled release of significant amounts of fission products (i.e., robust against catastrophic failure) in the event of a sabotage attack?
- (b) Do the essential safety systems continue to perform their functions in the event of a sabotage attack or can they be started and operated as needed for essential cooling of the nuclear fuel, control of reactivity and containment of radioactive substances?
- (c) Following a sabotage attack, can essential safety systems be operated until repairs can be carried out, even when subjected to related effects of the attack such as fire, smoke and structural damage?
- (d) Does the facility and system design and operation, in addition to the response procedures and capabilities, adequately mitigate and minimize any exposure of the public and facility personnel to radiation in the event of nuclear accident caused by any sabotage attack?

OVERVIEW OF THE PROCESS FOR SABOTAGE TARGET AND VITAL AREA IDENTIFICATION

2.21. The process described in this publication for sabotage target identification can be used for the evaluation of all types of nuclear facilities, from design through operation and, ultimately, decommissioning. It also can be used for evaluations in situations when the DBT, RTS or sabotage attack scenario assumptions have been changed.

2.22. For the consideration of type 1 sabotage attack scenarios leading to situations with URC or above, as defined above in the sub-section on threat assessment, a sabotage target and vital area identification process should be used to identify sabotage targets and appropriately assign vital areas within the nuclear security system to protect these targets. This process, outlined in Sections 3 to 6 of this publication, involves the following steps:

- (a) Gathering input data needed for the analysis, including the determination by the State of URC and HRC, the facility states to be included in the target identification process, the characteristics of the threat, and the site and facility characteristics;
- (b) Developing sabotage attack scenarios based on a range of possible initiating events deliberately caused by an adversary in an attempted sabotage to a facility;
- (c) Identifying potential sabotage targets and areas in which these targets are located, and performing an analysis using a logic model to determine candidate set of areas as vital areas to prevent all possible sabotage attack scenarios leading to URC or greater;
- (d) Performing an analysis to determine which of the candidate area sets should be selected as the final vital area set, including by assessing the feasibility of protecting the areas contained in each candidate area set;
- (e) Performing a vulnerability evaluation to assess whether the selected vital area set is sufficient.

2.23. For the consideration of type 2 sabotage attack scenarios leading to situations with URC or above, the assignment of vital areas may not be sufficient to mitigate the risk associated with this type of sabotage attack. Thus, an alternative process and set of considerations is provided in Section 7, which involves the following steps:

- (a) Gathering input data needed for the analysis;
- (b) Developing sabotage attack scenarios based on a range of possible initiating events deliberately caused by an adversary in an attempted sabotage to a facility;
- (c) Undertaking a sabotage margin assessment to evaluate the capacity of engineering safety features to resist the identified sabotage attack scenarios, including identifying one or more sabotage attack scenarios under which the facility is able to be safely shut down and maintained in a safe shutdown condition in response to the relevant sabotage attack scenarios;
- (d) Considering methods for successfully mitigating of adverse consequences resulting from vulnerabilities of critical SSCs or SSCs with unacceptably low capacities.

Policies and criteria to enable the detailed engineering evaluation and the decision process are also provided in Section 7.

2.24. The results of sabotage target identification provide a basis for decisions on design modifications, technical measures, procedures, assignment of responsibilities and risk acceptance criteria. The results of the safety analysis as well as guidance provided in the IAEA Safety Standards can provide useful information for sabotage target identification and evaluation of potential radiological consequences for several types of nuclear facilities during their entire lifecycle [10 – 20].

2.25. The application of the processes presented in this publication should involve operating staff and safety specialists working together with security specialists, agencies responsible for emergency preparedness and response, and other competent authorities in close cooperation to provide defence in depth against sabotage-initiated events.

2.26. Identification of sabotage targets and vital areas during the design stage of a nuclear facility provides the opportunity to reduce the number of sabotage targets and the size of vital areas, and allows the implementation of a more cost-effective nuclear security system. For example, locating non-critical SSCs out of vital areas can dramatically reduce the number of personnel that need access to vital areas. Additionally, safety measures can be designed to provide better capabilities to mitigate IEMOs by placing redundant critical SSCs in different vital areas and thus making more difficult for an adversary to defeat safety mitigation capabilities.

3. INPUT DATA FOR THE SABOTAGE TARGET IDENTIFICATION PROCESS

3.1. The first step in the process of sabotage target and vital area identification, regardless of the sabotage attack scenario type, is the gathering of input data. This data collection may require cooperation between the competent authority and the operator. The operator should determine the need for performing each type of analysis depending on the State's DBT or RTS and the particular situation of the facility for which the sabotage assessment is being performed.

3.2. Input to the process for identification and evaluation of potential sabotage attack scenarios and targets includes: the determination by the State of unacceptable and high radiological consequences; the facility states to be included in the target identification process; the characteristics of the threat; and the site and facility characteristics. Guidance regarding the preparation each of these inputs is provided in the sub-sections to follow.

DETERMINATION BY THE STATE OF UNACCEPTABLE AND HIGH RADIOLOGICAL CONSEQUENCES

3.3. For nuclear facilities, radiological consequences of concern are typically the release of radioactive substances, radioactive contamination and radiation exposure.

3.4. URC is defined in Ref [2] as “[a] level of radiological consequences, established by the State, above which the implementation of physical protection measures is warranted.” This level is typically defined in terms of dose and radioactive material release.

3.5. Safety documentation may serve as a basis for defining the threshold for URC and HRC, and if appropriate, categories in between URC and HRC thresholds.

3.6. If the determination of URC and HRC for nuclear security purposes is identical to thresholds that are defined by the State in relation to nuclear and/or radiation safety considerations, the safety analyses performed for the facility could be used for vital area identification, but may require modification.

IDENTIFICATION OF POTENTIAL TARGETS

3.7. Further, according to paragraphs 5.4 and 5.5 of Ref. [2]:

“For each nuclear facility, an analysis, validated by the competent authority, should be performed to determine whether the radioactive inventory has the potential to result in URC as determined by the State, assuming that the sabotage acts will be successfully completed while ignoring the impact of the physical protection or mitigation measures.

On the basis of these analyses, the State should consider the range of radiological consequences that can be associated with all its nuclear facilities and should appropriately grade the radiological consequences that exceed its limits for URC in order to assign appropriate levels of protection.”

3.8. According to Ref. [3], “the factors that should be taken into account when determining whether or not URC are possible at a facility include the characteristics described below (as applicable):

- (a) The amount, type, physical form and status of radioactive material at the nuclear facility (e.g. solid or liquid form, in process or storage).
- (b) The intrinsic risk (e.g. of criticality) associated with the physical processes and chemical processes that normally take place at the nuclear facility.
- (c) The characteristics of processes or engineering features that may become unstable during an attack.

- (d) The thermal power capacity of the facility and the irradiation history of the nuclear fuel (for a nuclear reactor).
- (e) The configuration of the nuclear facility for different types of activity.
- (f) The spatial distribution of radioactive material at the nuclear facility. For example, in research reactor facilities, most of the radioactive inventory is typically in the reactor core and the fuel storage pool; in processing and storage facilities, the radioactive inventory may be distributed across the site.
- (g) The characteristics of the nuclear facility relevant to the consequences of dispersal of radionuclides to the atmosphere and the hydrosphere (e.g. the size, design and construction of the facility, weather conditions, or the demographics and land and water features of the region).
- (h) The potential for off-site versus on-site radiological contamination (which will depend in part on the location of the radioactive material relative to the site boundaries)."

3.9. Ref. [2] recommends that "Nuclear material in an amount which if dispersed could lead to HRC and a minimum set of equipment, systems or devices needed to prevent high radiological consequences, should be located within one or more vital areas, located inside a protected area." Further, Ref. [3] elaborates that "States should also define the threshold for high radiological consequences, above which it is recommended that vital areas are identified and protected at a higher level."

3.10. Safety assessment of an operating facility supports potential target identification. In addition, the potential radiological impacts of accidents involving spent fuel should also be assessed by the operating organization and reviewed by the competent authority. Such safety assessments can provide important input for the design and evaluation of protection against sabotage. The spent fuel related safety assessment should include an assessment of hazards in operational states and accident conditions. It should also provide an assessment of doses at the site boundary and of the potential for exposure in areas within the site to which there is unrestricted access, as described in Ref. [12].

DETERMINATION OF FACILITY STATES TO BE ASSESSED

3.11. Typical nuclear facility states include normal operation, facility shutdown, reactor refueling, overhaul and maintenance and accident conditions. These different facility states may rely on different SSCs to perform necessary safety functions and different nuclear security measures may be needed to protect the SSCs and material under different facility states. Each facility state should be analyzed to identify related sabotage targets and vital areas, or, alternatively, a bounding facility state could be identified, that if protected adequately, will ensure protection during all operational states.

3.12. In the following sub-sections, a number of considerations will be addressed related to the determination of facility states to be considered as part of the analysis to identify sabotage targets and associated vital areas: safety defence in depth; fundamental safety functions; SSC unavailability; and associated operator actions.

Facility safe state(s) and safety defence in depth

3.13. Any facility state considered as part of the analysis to identify sabotage targets and associated vital areas should be a safe state, defined in the IAEA nuclear safety glossary [21],

as a [p]lant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

3.14. The defined facility safe state(s) may be different for different lifecycle stages (e.g., operation, decommissioning).

3.15. As noted in IAEA Safety Reports Series No. SRS- 46, Assessment of Defence in Depth for Nuclear Power Plants [22], “Defence in depth is generally divided into five levels. Should one level fail, the subsequent level comes into play. Table 1”, reproduced below from Ref. [22], “summarizes the objectives of each level and the corresponding means that are essential for achieving them. The levels are intended to be independent to the extent practicable. The general objective of defence in depth is to ensure that a single failure, whether an equipment failure or a human failure, at one level of defence, and even a combination of failures at more than one level of defence, does not propagate to jeopardize defence in depth at subsequent levels. The independence of different levels of defence is crucial to meeting this objective.”

DRAFT

TABLE 1. SAFETY DEFENCE IN DEPTH LEVELS

Level of Defence in Depth	Objective	Essential means for achieving the objective
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
3	Control of accidents within the design basis	Engineered safety features and accident procedures
4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

3.16. The objectives for each level of safety defence in depth summarized in Table 1, extracted from Ref [23]. These objectives can be used to develop facility-specific objectives for protection against sabotage when designing the facility nuclear security system. A process for designing a nuclear security system, including to protect against sabotage, is set out in Section 4 of Ref [3].⁵

3.17. For example, the Level 3 safety objective above, control of accidents within the (safety) design basis, could be used as an objective for protection against sabotage. Protecting against in line with level 3 would also meet the safety objectives of levels 4 and 5.

3.18. In addition, the levels of safety defence in depth could be used as part of a graded approach to categorizing sabotage attack scenarios developed during the process of identifying sabotage targets (discussed further in Section 5).

Fundamental safety functions

3.19. According to IAEA Safety Standards No SSR 2/1 (Rev 1), Safety of Nuclear Power Plants: Design, [16] “Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.”

⁵ Phase 1 of the development of a physical protection system involves “identifying the objectives and requirements of the physical protection system.” (Ref [3], page 51)

3.20. Safety analysis reports should be considered as an important input for the sabotage target identification process. According to IAEA Safety Standards SSG-61, Format and Content of the Safety Analysis Report, [24] “the plant specific safety functions that are necessary to fulfil the main safety functions and how their fulfilment is ensured by the plant’s inherent features” should be identified in the safety analysis report.

3.21. Other information to be provided in the safety analysis report is provided in Ref. [24], including “information on emergency arrangements, demonstrating in a reasonable manner that, in a nuclear or radiological emergency, all actions necessary for the protection of workers (including emergency workers), the public and the environment could be taken, and that the decision-making process for the implementation of these actions would be timely, disciplined, coordinated and effective.”

3.22. This information provided in the safety analysis report, particularly on the fulfilment of the safety functions and on emergency arrangements, should be considered to determine the facility states that are assessed as part of the analysis to identify sabotage targets and associated vital areas.

Structures, systems and components unavailability

3.23. SSC unavailability could conceivably occur concurrently with a malicious act either by chance or as a result of repair or maintenance outages. Thus, the identification of potential sabotage targets and associated vital areas should consider such situations..

3.24. Alternative on-site arrangements to compensate SSC unavailability can be arranged. For example, a mobile supply power system could supply cooling pump operation and provide electric power to control the reactor vessel pressure in a case of station black out. If alternative arrangements such as the deployment of mobile equipment or emergency response measures are proposed, the time required, the possibility to implement such provisions despite the presence of malicious actors, and the situation in which these actions should be undertaken should be considered. In some cases, a deployment delay or unavailability of these measures might make them unsuitable to use in the time available to prevent HRC.

Operator actions

3.25. Safety and other analyses used as input for sabotage target and associated vital area identification frequently contain explicit or implicit assumptions about operator actions associated with SSCs. These operator actions may involve routine, emergency or accident management actions needed to maintain the facility in a safe state. They may also be implicit in the way that the facility response to events is modelled. During the sabotage target and vital area identification process all implicit and explicit assumptions about operator actions included in the safety and other analyses used as input should be carefully identified.

3.26. After these operator actions have been identified, it should be determined whether they should be considered in the analysis as part of the facility response to sabotage. In this context, the availability of SSCs and operator personnel needs to be evaluated, and possible recovery actions to compensate for disabled SSCs may also be identified (see paragraphs 3.22 – 3.23). It should be determined if the recovery actions are also considered to be as part of the facility response to sabotage. It should be considered whether the sabotage attack scenario allows the

performance of these operator actions. The rationale for considering operator actions, including recovery actions, should be documented.

THREAT CHARACTERISTICS

3.27. Fundamental Principle G of the CPPNM as Amended states that “The State’s physical protection should be based on the State’s current evaluation of the threat.” Further, Fundamental Principle H states that “[p]hysical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat” [1].

3.28. Ref. [2] recommends that “[t]he State should define requirements — based on the threat assessment or design basis threat — for the physical protection of nuclear material in use, in storage, and during transport, and for nuclear facilities depending on the associated consequences of either unauthorized removal or sabotage.”

3.29. National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements (NSS No 10-G, Rev. 1) states that “[a]n assessment of the current threat related to nuclear security, provided in threat statements such as design basis threats and representative threat statements, can be used to facilitate a risk informed approach to nuclear security and risk management at individual facilities and activities.” [4]

3.30. Further, according to Ref. [4], “[i]n a performance based regulatory approach, design basis threats and the State’s nuclear security objectives provide the basis for designing, implementing and evaluating nuclear security systems and measures.” Further information applicable to sabotage threats on this topic can be found in paragraphs 7.2-7.4 of Ref. [4], including on the development of credible sabotage attack scenarios using the threat characteristics defined in the design basis threat. These credible sabotage attack scenarios should be used in the target identification and vital area identification process, discussed further in Sections 4 and 5.

SITE AND FACILITY CHARACTERISTICS

3.31. Site characteristics, including those such as the population density, high grounds or other relevant places for standoff attacks, and land use in the vicinity of the facility, are important factors when evaluating the consequences of a potential radiological release.

3.32. Facility characteristics provide essential input to the process of identifying sabotage targets and vital areas. The characteristics that should be identified and provided as input to the analysis include:

- (a) locations, characteristics and quantities of nuclear and other radioactive material;
- (b) inventory forms;
- (c) information about the nuclear facility’s safety provisions, such as those related to shielding, criticality control, cooling, confinement, fire prevention and structural integrity;
- (d) detailed design information on processes and safety systems.

In particular, the design information on processes and safety systems should be used to identify the SSCs and associated operator actions to be protected against sabotage.

4. DEVELOPING SABOTAGE ATTACK SCENARIOS

4.1. To determine the areas that should be protected to prevent acts that lead to high radiological consequences, potential sabotage attack scenarios leading to consequences equal to or greater than the State's definition of URC should be identified. All credible sabotage attack scenarios, consistent with the DBT or RTS, should be considered. Criteria considered for the selection of these scenarios should be documented and justified. This analysis will use as input the data discussed in Section 3: the determination by the State of URC and high radiological consequences; the facility states to be included in the target identification process; the characteristics of the threat; and the site and facility characteristics. The resulting sabotage attack scenarios will be used as input to the sabotage logic model discussed in Section 5, which will be used to identify sabotage targets that are candidates for protection in vital areas.

4.2. Sabotage resulting from direct, semi-direct or indirect acts should be considered in developing these sabotage attack scenarios.

4.3. Acts of direct sabotage lead to the dispersion of radioactive material via the application of energy from an external source (for example, an explosive or incendiary device). Semi-direct sabotage includes malicious acts involving explosives or other sources of energy that are used for breaching safety barriers or that could cause safety barriers to fail, resulting in radioactive material to be dispersed in a manner that is usually not addressed in the safety analysis.

4.4. Acts of indirect sabotage lead to the dispersal of radioactive material or an exposure to radiation using the energy contained within the nuclear or radioactive material, or the energy that is generated during the processing of material within the processing systems. Indirect sabotage attacks may not involve an adversary gaining access to the area in which the material is located, but may involve an attack on the SSCs or associated operator actions that maintain the facility in a safe state. For example, a sabotage attack directed at the SSCs responsible for maintaining core temperature within operational limits at a nuclear power plant could result in a dispersion of radioactive material.

ADDRESSING DIRECT AND SEMI-DIRECT ACTS OF SABOTAGE

4.5. According to paragraph 3.72 of Ref. [2], "[t]he State should consider how to protect nuclear facilities while taking into account the potential for sabotage to cause unacceptable radiological consequences. The State should also ensure that protection measures are required for the targets within the facilities which if subject to sabotage would produce such consequences." Thus, if the release would lead to consequences greater than URC, the direct dispersal of the inventory should be included in the sabotage logic model discussed in Section 5, and the remaining steps of the vital area identification process should be performed for the inventory.

4.6. Inventories of radioactive material, including nuclear fuel in-process, that might be the source of a direct release leading to URC or HRC should also be considered. These inventories

could include, for example, irradiated fuel, radioactive sources or radioactive waste. If the potential radiological consequences of the release of radioactive material caused by indirect sabotage of these materials are equal to or greater than the URC, these SSCs and associated operator actions should be considered as sabotage targets.

ADDRESSING INDIRECT ACTS OF SABOTAGE: IDENTIFYING INITIATING EVENTS OF MALICIOUS ORIGIN

4.7. An initiating event that is deliberately caused by an adversary in an attempted sabotage to a facility is called an initiating event of malicious origin (IEMO). IEMOs should be identified with the aim of producing a list of sabotage attack scenarios triggered by such events that have the potential to lead to URC or high radiological consequences. The list of IEMOs identified, either alone or in combination with mitigating system failures, should be included in the sabotage logic model discussed in Section 5, which sets out a methodology for the identification of sabotage targets.

4.8. Two types of indirect acts of sabotage should be considered, namely:

- (a) Attacks causing an initiating event [15] that creates conditions more severe than the facility mitigating systems can accommodate (that is, events that are beyond the safety design basis); and
- (a) Attacks causing an initiating event and disabling the systems needed to mitigate the effects of the initiating event.

4.9. Many initiating events will have already been identified and analyzed in facility safety documentation, such as safety case studies, deterministic safety analysis or the probabilistic safety analysis report. These initiating events should be considered as potential IEMOs.

4.10. In particular, facility safety assessments, reports and analyses contain valuable information and models. A deterministic safety analysis or a probabilistic safety analysis (PSA) for the facility will, for example, provide analyses of response of the facility to various initiating events. The IAEA Safety Standards, such as IAEA GSR Part 4 [24], contain information about the safety documents the operator should have prepared. Guidance on systematic identification of hazards and accident scenarios associated with facility states and accident conditions are discussed in Ref. [26].

4.11. Three categories of potential initiating events should be considered when identifying potential IEMOs that may not have been included in the safety case:

- (a) Situations in which there is no process energy or other energy sources present that could disperse radioactive material, such as those involving malicious acts using explosives or other sources of energy for breaching barriers, or those involving radioactive material being dispersed in a manner not possible without a malicious act.
- (b) Initiating events that are so unlikely to occur randomly that they are excluded from safety consideration, such as multiple independent initiating events 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. Initiating events that are considered independent from a safety point of view may sometimes be triggered by a same malicious attack and thus,

cannot be considered as independent from security point of view. For example, the simultaneous loss of all trains of service that might be the result of an explosion or several coordinated sabotage actions would challenge the performance of safety functions beyond design.

- (c) Sources of radioactive material releases that may not have been within the scope of safety analysis. For example, level 1 probabilistic safety analyses at nuclear power plants 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 HRC (such as irradiated fuel and radioactive waste) also should be considered.

4.12. There are four approaches that can be used to identify the IEMOs:

- (a) *Review of safety documentation.* This should be the starting point for understanding the facility's potential hazards. Safety reports, assessments, deterministic safety analyses and probabilistic safety analyses, fire analyses, seismic analyses, and other safety evaluations for the facility and for similar facilities help to identify initiating events. Any of the initiating events that can occur randomly may also be caused by malicious acts, so this set of initiating events should be included in the list of IEMOs. Notably, the assumptions in made safety analyses regarding the nature of initiating events and the facility response to them should be re-examined in the context of malicious acts and revised where appropriate.
- (b) *Reference to other vital area identification analyses.* Where other vital area identification analyses have been performed for similar facilities, lists of the IEMOs used for these analyses should be reviewed. It is particularly important to identify IEMOs that do not correspond to initiating events identified in facility safety documentation.
- (c) *Engineering evaluation.* The facility systems (operational and safety) and major structures and components should be systematically reviewed to identify any additional IEMOs. For example, any initiating events should be identified that could result from malicious acts in which the potential adversary is deemed capable of initiating an event that leads directly, or in combination with other malicious acts, to unacceptable (or high) radiological consequences.
- (d) *Deductive analysis.* In this approach, URC are systematically decomposed into postulated events that could cause them to occur. Successful operation of systems and other preventive actions are not included. The events at the most fundamental level that may trigger successive events leading to URC or HRC are then candidates for the list of IEMOs for the facility.

4.13. Because the objective is to produce a list of IEMOs that is as complete as possible, all of these approaches should be used.

4.14. Each IEMO should also be assessed to determine whether there are systems capable of mitigating it. These events will either exceed mitigating system capability or be within mitigating system capability, as discussed in the two sub-sections to follow.

IEMOs that exceed mitigating system capability

4.15. Every IEMO that exceeds mitigating system capability should be included in the sabotage logic model discussed in Section 5. An example is a pipe break that creates a loss of coolant that cannot be compensated by an injection system.

4.16. The likelihood that a given threat could cause an IEMO that exceeds the mitigating system capability is addressed when the threat characteristics are considered later in the process (see paragraphs 4.27-4.29).

IEMOs that are within mitigating system capability

4.17. Even if an event is within the capability of the mitigating systems, if these systems are disabled, including through associated operator actions, this may allow IEMOs to proceed unhindered. Thus, for IEMOs that are within mitigating system capability, combinations should be determined of IEMOs and events disabling the mitigating systems (mitigating system disablement events) that could lead to unacceptable or high radiological consequences. Such combinations of mitigating system disabling events and associated IEMOs should be included in the sabotage logic model discussed in Section 5. For example, the loss of offsite power in combination with a loss of emergency power supply could disable decay heat removal and lead to unacceptable radiological consequences, and thus should be included.

4.18. The credibility of the threat causing these mitigating system disablement events and IEMOs is addressed when the threat characteristics are considered later in the process (see paragraphs 4.27-4.29).

4.19. The specific systems that are used to mitigate initiating events may differ depending upon the facility state. Systems that are used to mitigate initiating events also support safety functions such as reactivity control, decay heat removal, coolant boundary integrity, and containment integrity. The systems that directly perform fundamental safety functions (see paragraph 3.18) are safety systems, while equipment needed for proper functioning of the safety systems are referred to as support features. The successful operation of a safety system may depend upon the availability of one or more support features. Dependencies of safety systems on support features should be identified during the assessment of the IEMOs and mitigating system disablement events, as they could represent vulnerabilities.

4.20. If a probabilistic safety analysis (PSA) has been prepared for the facility, the information on safety systems and support features should be readily available from the PSA or supporting documentation. If only a deterministic safety analysis is available, then most or all of this information can be derived from the accident analyses by employing engineering judgment.

4.21. If the deterministic safety analysis lists safety SSCs, this list can be helpful in identifying safety systems and their dependencies. However, there may be other dependencies, beyond the safety analysis, that relate to specific sabotage attack scenarios. For example, explosive breaching of a cooling water pipe may cause flooding of equipment near or below the pipe breach, if, for example, an installed drainage system was sabotaged, even though the drainage system may have satisfied safety concerns on flooding as a non-malicious initiating event.

4.22. In the context of this analysis, successful operation of a safety system means that the system's safety function is performed to at least the minimum level needed to address the conditions created by an IEMO. Relevant information for developing success criteria for safety systems and support features is given in facility safety analyses. The success criteria for safety

systems are of particular importance when analysing IEMOs, because they define the starting points for the subsequent logic modelling of the system sabotage attack scenarios. Success criteria could include performance measures (e.g. flow rate or response time) as well as hardware requirements (e.g., the number of required flow paths or power trains).

4.23. Defining success criteria for support features can be more complicated than for safety systems. In most cases, support features serve more than one safety 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 safety systems that perform a certain safety function. Thus, the success criteria for a support feature vary with different safety functions and associated safety systems.

4.24. For some facilities, there may be a large number of potential IEMOs that, coupled with mitigating system disablement events, could lead to URC or greater. For such facilities, it may be desirable to group together IEMOs for which the same safety system and support feature performance is needed to mitigate them. Grouping IEMOs in this way will reduce the complexity of the sabotage logic model. In a given group of such IEMOs, the safety systems and support features should then meet essentially the same success criteria. This permits sabotage attack scenarios to begin with any of the IEMOs in a group and apply to all of the events in the group.

4.25. It may not be desirable to group IEMOs for facilities where only a small number of potential IEMOs are identified.

4.26. If a PSA has been performed for the facility, the PSA documentation should contain the grouping of initiating events considered in the PSA. The same groupings can be employed for corresponding IEMOs. If a PSA has not been performed for the facility, it may be possible to begin with groupings of initiating events from other safety documentation or another source. However, IEMOs 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.

CREDIBILITY OF SABOTAGE ACTS

4.27. The discussion of acts of sabotage addressed in the preceding sub-sections do not consider the capability of the threat to perform the acts. All events that could lead directly or indirectly to levels of URC or above are initially included in the analysis, to ensure that no potential sabotage targets are overlooked, without regard to whether the defined threat capabilities and sabotage attack scenarios are sufficient to perform the sabotage acts. If the assumed threat characteristics change, the information developed in the preceding steps will remain valid under the changed threat conditions.

4.28. However, after all potential acts of sabotage have been identified, these sabotage targets "...should then be considered in conjunction with the attributes and characteristics of the potential adversaries described in the national nuclear security threat assessment documentation...", as noted in Paragraph 6.10 of Ref. [5]. Further explained in Paragraph 6.11 of Ref. [5], " If the capabilities of a given adversary are not sufficient to commit such an act, then that adversary may be excluded from further consideration".

4.29. The credibility of direct dispersal of material, of causing an IEMO, and of disabling mitigating systems should be assessed. Events that are not credible may be removed from the sabotage logic model.

4.30. Preventing, for example, loss of off-site power is practically impossible for a facility's nuclear security system. The loss of off-site power can be achieved in many ways without gaining access to the facility. Therefore, it should be assumed that off-site power is unavailable as a boundary condition for determining the credibility of sabotage attack scenarios.

5. IDENTIFYING POTENTIAL SABOTAGE TARGETS

5.1. Once the needed inputs for the process for identification and evaluation of potential sabotage attack scenarios and targets have been identified and, based on these inputs, a list of IEMOs and associated sabotage attack scenarios has been compiled, the next step is to identify sabotage targets that would be candidates for protection in vital areas (see Section 6 for more discussion of vital area identification).

5.2. The minimum set of SSCs and associated operator actions to be protected may include all safety systems if necessitated by the overall safety philosophy at the facility, or alternatively, the minimum set may be defined as a subset of all SSCs and associated operator actions. The number and extent of the SSCs and associated operator actions to be protected and the designated vital areas are specific to each facility.

5.3. To identify sabotage targets that are candidates for protection in vital areas, a sabotage logic model should be developed that uses as inputs the sabotage attack scenarios for direct and semi-direct sabotage and IEMOs identified in Section 4, along with the SSCs and associated operator actions that mitigate these initiating events (if any). The areas in the facility from which an adversary could accomplish each event in the sabotage logic model should then be identified and documented, and candidate area sets should then be identified. Each of these steps is discussed in the following sub-sections.

SABOTAGE LOGIC MODEL

5.4. A sabotage logic model can be a statement, an algebraic expression or a graphical representation, such as a logic fault tree or a logic event tree, which is used to identify the events or combinations of events that could lead to URC or greater.

5.5. The sabotage logic model should include all direct and semi-direct sabotage events and all IEMOs that exceed mitigating system capacity as single events leading to URC or greater. IEMOs within mitigating system capacity should be included alongside associated mitigating system disablement events. The part of the logic model relevant to mitigating system disablement should be developed to the component level using a top-down approach, and in sufficient detail to allow linking of disablement events to the facility locations (areas) in which the system disablement can be accomplished.

5.6. 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.

5.7. Typically, the development of the overall sabotage logic model is done in two steps:

- (a) Development of the facility sabotage logic model that represents the combinations of IEMOs and disablement of safety systems leading to URC or greater. This is accomplished using the information in paragraph 5.5 alongside information from the facility safety analysis.
- (b) Development of sabotage logic models for individual safety systems and the support features they are dependent upon, either by modifying existing logic models from the facility PSA or by developing logic models using facility system configuration information and the success criteria and dependency information.

The second step of the above process produces the portion of the sabotage logic model that links each IEMO with the disablement of the mitigating safety systems as well as corresponding support features and associated operator actions.

5.8. An example of a simple sabotage logic model is provided in Annex I.

IDENTIFICATION OF AREAS AND FACILITY WALKDOWN

5.9. It is not reasonable to design and implement SSC and operator action specific nuclear security measures to protect individual SSCs and associated operator actions. Thus, areas surrounding these systems should be identified as candidates for implementing nuclear security measures.

5.10. After developing the sabotage logic model, the areas in the facility from which an adversary could accomplish each event in the sabotage logic model should be identified and documented. These areas may later be identified as vital area candidates (see paragraph 5.15-17 and Section 6). Information about these areas should be collected through a structured process and verified by conducting a walkdown of the facility. Annex II provides more detail on conducting a facility walkdown.

5.11. 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 probabilistic safety analyses are other sources of information on equipment locations.

5.12. In preparation for the walkdown, the location information for the overall facility (e.g., buildings, elevations, rooms or compartments) should be reviewed. The walkdown should be performed by representatives from the facility safety, security, design and operating organizations. The main objectives of the walkdown are to:

- (a) Verify the areas from which the threat capabilities defined in the DBT/RTS could accomplish direct dispersal;
- (b) Verify the set of areas from which the threat capabilities defined in the DBT/RTS could accomplish each identified IEMO;
- (c) Verify the set of areas from which the threat capabilities defined in the DBT/RTS could accomplish each of the actions to disable sabotage targets or associated operator actions that are identified in the sabotage logic model; and

- (d) Assess the potential for spatial interactions between adjacent areas. External event PSAs, such as those for seismic, fire and flooding may provide useful information on spatial interactions.

5.13. Any area that could be selected as a vital area needs to be capable of supporting appropriate detection and delay at its boundaries as well as timely response. Therefore, for each area identified, it should be feasible to employ existing structures or new construction to establish a physical barrier to the area, to control access, to minimize the number of entrances to and exits, and detect unauthorized access. This approach can be provide a more effective and cost effective solution if taken into account at an early stage of the design of the nuclear facility.

5.14. Areas should be documented by marking them on facility arrangement drawings or other facility design and layout documents to clearly define the area boundaries.

SABOTAGE AREA LOGIC MODEL

5.15. After the areas in the facility from which an adversary could accomplish each event in the sabotage logic model have been identified, the sabotage area logic model is then created by replacing each event in the sabotage logic model (i.e., each direct dispersal event, IEMO, and each mitigating system disablement event) with the area or areas in the nuclear facility from which it an adversary could cause the event.

5.16. 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 considered initiating events are replaced by areas in which they can be performed.

5.17. The sabotage area logic model should be solved to find a minimum set of areas accommodating targets requiring protection against sabotage to prevent all possible sabotage attack scenarios leading to URC or greater, as follows:

- (a) Identification of all combinations of areas to which an adversary would gain access in order to complete sabotage attack scenarios that could lead to URC or greater;
- (b) Determination of the minimum combinations of areas that should be protected to ensure that no sabotage events resulting in URC or greater can be completed (at least one of the areas in each combination of areas from which sabotage can be accomplished should be protected).

5.18. Each combination of locations whose protection will prevent all sabotage attack scenarios constitutes a candidate set of vital areas, as discussed in Section 6. Each of the candidate vital area sets should be capable of providing for detection and delay of and response to sabotage acts, as noted in paragraph 5.13.

6. VITAL AREA IDENTIFICATION

6.1. The identification of sabotage targets, as set out in the previous Section, focuses on identifying the SSCs and associated operator actions that perform safety functions. The design of a nuclear security system then addresses how to protect these SSCs and associated operator actions identified as potential targets, focusing on the area around the targets.

6.2. Target identification does not consider whether the nuclear security measures can be overcome or whether it is difficult to provide physical protection for the target under consideration. This is accounted for in the next step of the analysis, where the vital areas are selected from the candidate sets of vital areas identified in paragraphs 5.15 – 5.18. Once the vital areas are selected, a vulnerability assessment should be performed to assess whether the vital area selection is sufficient.

6.3. The SSCs and associated operator actions identified as targets to be protected in vital areas in the selected vital area set should be listed in the safe shutdown equipment list (SSEL) and corresponding operator actions. The SSCs listed in the SSEL are those SSCs that must function in order to safely shut down the nuclear facility and maintain it in a safe shutdown condition. The SSEL for a nuclear power plant will contain a few hundred SSCs, however, other facility types may have significantly fewer SSCs in their SSELs. The operator actions to be listed alongside the SSEL are those that must be completed in order to safely shut down the nuclear facility and maintain it in a safe shutdown condition.

6.4. If the evaluation is being performed at a facility with implemented nuclear security measures, it is expected that the majority of the SSCs in the SSEL as well as corresponding operator actions will be located in or take place in previously identified vital areas. However, vital area designations should be revisited as part of this assessment. For sabotage attack scenarios that have not been previously considered in the assessment, some areas may need to be designated as vital; similarly, some areas previously designated as vital may no longer need to be defined as such. A re-evaluation after design changes of the facility could show similar results.

VITAL AREA SET SELECTION

6.5. Once the candidate sets of vital areas have been identified as described in paragraphs 5.15 – 5.18, a vital area set should be selected. When selecting a vital area set, it should be ensured that all sabotage targets identified from the safe shutdown equipment list (SSEL) are located within a vital area.

6.6. The operator should also account for the various factors important for the safe and efficient operation of the facility when selecting the vital area set. An overly conservative approach to selecting the vital area set has the potential to result in unacceptable impacts to safe operations and high costs, due to the increased measures necessary to ensure the protection of the identified sabotage targets. Specific needs for access to some areas and SSCs may influence the selection of candidate vital areas. For example, the operator may propose the candidate vital area set that provides the optimum combination of:

- (a) Lowest impacts on safety, facility operations and emergency response;
- (b) Lowest difficulty of implementing protection measures;
- (c) Highest effectiveness of protection measures; and
- (d) Lowest cost of protecting the vital areas.

6.7. Further, the selected vital area set should include:

- (a) All areas from which the threat has the capability to cause direct or semi-direct dispersal of radioactive material;

- (b) All areas from which the threat could cause initiating events that exceed the mitigation capability of facility systems; and
- (c) All areas from which the threat could cause an initiating event and either mitigating SSCs and associated operator actions are located or a minimum set of mitigating SSCs and associated operator actions are located.

6.8. As part of the vital area selection process, a table should be produced 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. The table should record the aggregate score or ranking of each candidate vital area set, with associated rationale (e.g., an adversary path was considered but not determined to be credible because it was too complicated). A recommended vital area set should be selected based on the best overall score or ranking.

6.9. It is unlikely that one candidate vital area set will receive the highest rating for each of the selection criteria. Thus, trade-offs should be assessed in selecting the final vital area set. This can be done using engineering judgment or a more structured analytical approach.

VULNERABILITY EVALUATION OF SABOTAGE TARGETS

6.10. Once the vital area set is selected, a vulnerability assessment should be undertaken to assess whether the nuclear security of the selected vital area set is sufficient.

6.11. The vital area set should first be assessed to determine if the target set contained in it is adequate to prevent URC or greater.

6.12. If so, it should be reviewed to determine whether the vital areas identified in the vital area set can support adequate detection and delay for timely response, using the facility layout and information on the operational access, response capabilities and any safety constraints. If the capability of the vital area set to support detection and delay is considered adequate, then it should be assessed whether the targets inside the vital areas, as protected with the detection and delay measures, are vulnerable to attacks by the threats described in the DBT or RTS (see Ref. [5] for more information on DBT and RTS).

6.13. If targets to be protected in vital areas are assessed to be vulnerable, it should be considered whether the vital area can be fortified, using the facility layout as well as information on the response capabilities and their timeliness, operational access, safety concerns and engineering safety. If a vital area cannot be fortified:

- (a) The target robustness should be strengthened;
- (b) Contingency measures should be considered;
- (c) Required functions should be modified;
- (d) The safety margin should be assessed; or
- (e) The target set needs to be reset.

6.14. Depending on the adversary capabilities defined in the DBT or RTS, insider threat may need to be taken in consideration for vulnerability evaluation. It can lead to identify the necessity of additional security measures.

7. OFF-SITE SABOTAGE ATTACKS

7.1. As briefly mentioned in Section 2, sabotage attack scenarios developed by the operator can be divided into two types:

- Type 1 sabotage attack scenarios, those involving physical presence of adversaries on the site, which provide a basis for the design of the facility nuclear security system against sabotage (the focus of the evaluation in the previous Sections); and
- Type 2 sabotage attack scenarios, which are launched from outside the facility boundary.

Both type 1 and type 2 sabotage attack scenarios are possible and can be generated, however, the nuclear security system should be designed and evaluated separately for the two types of scenario. For this reason, they are treated separately in this publication.

7.2. Type 1 sabotage attack scenarios represents scenarios involving the physical presence of the adversaries on the site. Type 2 sabotage attack scenarios do not involve intrusion into the facility. As a result, the options to adjust the design of nuclear security system functions of detection, delay and response against type 2 sabotage attack scenarios are limited and therefore may require support by State organizations. Thus, type 2 sabotage attack scenarios may not be considered in the design of the nuclear security system. Examples may include standoff attacks such as airborne attacks using drones, missiles, airplanes or attacks using directed energy weapons or blasts from chemical explosions.

7.3. Due to these distinctions between type 1 and type 2 sabotage attack scenarios, where type 2 sabotage attack scenarios are to be considered, they often require a separate analysis, involving the consideration of engineering safety aspects of the protection of nuclear facilities against sabotage. Sections 3-6 addressed the identification of sabotage targets and vital areas, with a focus on type 1 sabotage attack scenarios; this Section will focus on special considerations and additional analysis needed to consider sabotage attack scenarios launched from outside the facility boundary.

7.4. In the following sub-sections, some considerations related to type 2 sabotage attack scenarios are provided, then guidance is set out for the development of relevant facility-specific type 2 sabotage attack scenarios; the identification of success paths for the facility against these scenarios; sabotage margin assessment; particular considerations for the facility walkdown and, finally, a methodology for decisions on how to cope with identified vulnerabilities of critical SSCs.

CONSIDERATIONS FOR TYPE 2 SABOTAGE ATTACK SCENARIOS

7.5. According to Ref. [2], “The State should give attention to providing protection measures against any airborne threat and against possible stand-off attacks specified in the State’s threat assessment or design basis threat.”

7.6. Some type 2 sabotage attack scenarios may involve threats greater than the facility’s design basis threat. It may be decided by the State that such threats should remain outside the capacity of the facility nuclear security system.

7.7. The various systems meant to protect the facility will experience a loading as a result of a sabotage attack. Extreme loads correlate to the extensive pressure placed on these SSCs, which could result in the failure of the SSCs to adequately mitigate the sabotage. This situation is referred to as “extreme loading.”

7.8. In some cases, type 2 sabotage attack scenarios may result in extreme loads on the facility, and the SSC capacity to manage these loads will need to be evaluated. Following this analysis, the SSCs and associated operator actions that will need to be protected more stringently, due to the consequences resulting from the compromise or cessation of their operability and/or their lack of capacity to manage extreme loads, should be determined. The acceptance criteria to be used by the operator in this evaluation should be agreed to by the competent authority.

7.9. To support this evaluation, an extreme environmental load matrix should be developed, compiling environment loads and load combinations for engineering evaluations, and should include: the SSC name; component type; manufacturer; design conditions; function; physical location; and physical loading conditions, such as direct or indirect impact effects, direct or indirect blast effects, heat and fire loading, vibration and effects of smothering on operability (including smoke effects from fire; and flooding from an internal or external source). In addition, extreme environment loads (such as those provided in Table III-1 in Annex III) and the supporting data should be identified for each of the SSCs in the matrix. A suggested format for the matrix is provided in Annex III, Table III-6.

7.10. As stated in Paragraph 8.1 of Ref. [5], “The national nuclear security threat assessment documentation should be periodically reviewed to assess whether the assessment still represents a comprehensive and balanced view of the credible threats to nuclear security in the State, and the assessment should be revised if necessary”. This review may show that a credible type 2 sabotage attack scenario has become an actual subject of concern, and an evaluation should be undertaken.

7.11. In this case, a re-evaluation of the facility needs to be carried out using realistic margins. This may lead to upgrades and perhaps inclusion of some type 2 sabotage attack scenarios into the process described in Sections 4-6 for vital area identification and nuclear security system design and evaluation. Alternatively, the evaluation may result in a decision concerning the feasibility of continuing operations. The State may also decide to take on part of the responsibility for protection against type 2 sabotage attack scenarios.

7.12. In a nuclear emergency, the operator will need to be capable of overseeing and managing severe facility conditions, in order to take actions to mitigate the potential consequences of a sabotage event. The operator security plan should consider the possibility of continued adversary presence at the site aimed at hindering or disrupting the mitigation activities.

7.13. Off-site emergency response should be available to mitigate off-site radiological consequences of a malicious act that has led, or has the potential to lead, to the loss of safety functions through the compromise or inoperability of the safety systems. The national level emergency and contingency response plans should include all actions performed by State organizations in cooperation and coordination with the operating organization to cope with the situation, including specific measures to counter malicious acts aimed at disrupting and disabling emergency response.

7.14. The response by competent authorities may involve the active support of the operator's response to an attack on the facility, including emergency response actions of emergency organizations in the State.

7.15. As noted in Paragraph 3.41 of Ref. [2], "The State should ensure that the State's physical protection regime is capable of establishing and maintaining the risk of unauthorized removal and sabotage at acceptable levels through risk management." The State should decide whether, with the implementation of all available layers of nuclear security defence in depth, the remaining risk from any particular sabotage attack scenario is within the established limits of acceptability. In this decision, the responsibilities and the roles of the operator and the competent authorities — including security and emergency response organizations — should be taken into consideration.

7.16. The consideration of type 2 sabotage attack scenarios in the design of SSCs (security by design) may improve robustness concerning external hazards in general and could help to avoid the need for potential upgrades at a later time.

DEVELOPMENT AND SELECTION OF FACILITY SPECIFIC ATTACK SCENARIOS

7.17. Similarly to the development of type 1 sabotage attack scenarios described in Section 4, type 2 sabotage attack scenarios should be developed based on the threat detailed in the DBT or RTS. These scenarios should be refined to account for the characteristics of the specific facility being evaluated.

7.18. This process may lead to the exclusion of some scenarios on the basis of site and facility characteristics, type and number of inventories and facilities at the site, design of the facility and any facility-independent off-site security measures, as described in the following paragraphs.

7.19. The surrounding topography and vegetation may be sufficient to exclude certain attack scenarios initiated outside the facility boundary. Notably, the location and layout of the facility site may limit the likelihood that particular on-site areas will be affected by certain attack scenarios. Consideration of nuclear security solutions in the design stage may provide the opportunity to adapt the general layout of a facility and improve protection against stand-off attacks. For example office buildings may be placed astutely to prevent a potential straight path and clear sight, a facility's location in hills, mountains or a valley may limit the feasible approach angles and speed of a large aircraft attack on the site. Other factors, such as the location of transmission lines, may limit approach paths for attacks by large aircraft. For blast loading conditions, the shielding of structures provided by topographic effects and adjoining structures may limit the area of influence and thus should be considered. Alternatively, containment structures that can withstand a stand-off attacks can locate vital areas and sabotage targets.

7.20. However, potential site conditions that may benefit adversaries also need to be taken into careful consideration, for example, the proximity of nuclear facilities to public transport infrastructure (roads, railways, airports) or to industry and populated areas. For example, research reactors tend to be located within research centres or on university campuses, which may make the identification of potential intruders or attackers difficult.

7.21. The type and number of facilities and the radioactive material inventories at the site should also be considered, as some type 2 sabotage attack scenarios may have a simultaneous impact on all facilities at a site. A nuclear site, for example, may contain several reactor units, potentially with interdependent safety systems. Multi-unit sites often assume the availability of companion unit systems when addressing non-common-cause events. In addition, other facilities having high potential radiological consequences may be present within the facility boundary, such as those for spent fuel storage in fuel pools or dry cask storage. Further, research reactor sites may have associated laboratories, isotope production facilities and hot cells.

7.22. Thus, the evaluation should take into consideration all on-site facilities and any interdependence of their safety systems. Such consideration includes consequence assessment of possible environmental discharges that are cumulative for all facilities on a site and limited number of emergency response forces.

7.23. High radiological consequence nuclear facilities, like nuclear power plants or reprocessing facilities, are designed for a wide range of extreme environment loading conditions. The design basis incorporates measures to defend against internal and external events — such as fire, pipe whip, loss of coolant accidents, earthquakes, extreme winds, explosions or aircraft impacts — which provide an ‘envelope’ of protection. This protection should be taken into account when evaluating type 2 sabotage attack scenarios. In fact, some scenarios may be excluded from further consideration because they are effectively bounded by design basis conditions. Bounding can be demonstrated on the basis of the event (for the whole facility), the extreme load (for each SSC) or the sizing requirement derived from the loads.

7.24. Finally, facility-independent off-site security measures should be considered. These measures can range from increased security in the aviation industry to surveillance performed by off-site entities in the vicinity of the site. If they are in place and effective, the measures may serve to exclude certain sabotage attack scenarios from consideration or may be used to better define the bounding conditions of such scenarios.

Screening process for type 2 sabotage attack scenarios

7.25. Two methods are generally used to determine whether a type 2 sabotage attack scenario should be further considered: (1) the minimum distance needed for the attack and the magnitude of its potential consequences, and (2) the approximate probability of the scenario’s occurrence.

7.26. In the first method, the minimum distance from the facility that the attackers would need to undertake the scenario is postulated, as is the maximum magnitude of its potential consequences (i.e. the most conservative approximation). The potential damaging effects on the facility’s safety are then assessed. If the consequences are found to be insignificant, the event is removed from consideration in the overall sabotage assessment. For example, an attack scenario involving a vehicle containing explosives may be removed from consideration on the basis of the effective barrier’s distance from the safety systems of interest.

7.27. Determining the probability of a scenario’s occurrence and applying probabilistic screening (parallel to probabilistic screening for safety undertaken for scenarios resulting from events of an accidental origin) is generally more complex and uncertain. However, it may be applied to events not eliminated by the above process.

7.28. Sabotage acts do not lend themselves to probabilistic screening on an absolute probability basis, and further, a significant difference exists between probabilistic screening of events of an accidental origin and events due to sabotage. For screening criteria for accidental external events, it is generally assumed that scenarios with a larger damage potential will occur with less frequency — that is, the larger the event, the lower the frequency of occurrence. For sabotage, depending on the adversary's objectives and capabilities, this assumption does not hold. For example, a State can decide that intentional plane crashes must be considered from a security point of view, even if the probability of accidental plane crashes is considered extremely low from safety point of view.

7.29. However, probabilistic safety assessments (PSA or dynamic PSA) tools adapted to address scenarios, where conditional end metrics are calculated, may be able to be used provide the basis for screening an individual scenario. This approach assumes that the most upstream event is deterministic (i.e. $p = 1$), but sequences evolving from this event may be represented probabilistically on the basis of the facility layout, systems design and structural robustness.

7.30. A good practice is to use a probability level for screening of sabotage attack scenarios that is generally one or two orders of magnitude smaller than that used for accidents and extreme events; the smaller order of magnitude is used so that conservatism is maintained and no event is excluded as a result of the approximate nature of the probabilistic screening procedure.

7.31. In addition, to reduce the effort needed to evaluate the facility for the sabotage attack scenarios, type 2 sabotage attack scenarios can be grouped according to similarities in effects on the nuclear facility, and one scenario or a composite of the grouped attack scenarios can be selected for detailed evaluation. Grouping the scenarios in this way can reduce the overall number of scenarios to be considered to a more manageable number. A panel of experts in attack scenario development and nuclear safety could be appointed for this activity.

7.32. SSCs that have low capacity and low safety importance can be screened out; for example, some structures may be identified as having low capacities and thus be excluded from consideration.

SABOTAGE MARGIN ASSESSMENT FOR TYPE 2 SABOTAGE ATTACK SCENARIOS

7.33. A sabotage margin assessment involves evaluating the capacity of safety systems to resist the identified type 2 sabotage attack scenarios. This procedure involves starting with the definitions of extreme environment loads and load combinations for engineering evaluations, and should result in an evaluation of the SSC capacity when subjected to the extreme environment loads specified.

7.34. First, an extreme environment load evaluation should be undertaken to evaluate the capacity of the safety systems of nuclear facilities to withstand malicious attacks. An example methodology is provided in Annex III.

7.35. As part of this evaluation, extreme environment load definition matrices should be developed, including a short description of each relevant type 2 sabotage attack scenario and the extreme environment loads and load combinations for engineering evaluations. The extreme environment loads in the matrix may include, for example, impact, explosion and blast,

heat and fire, vibration, hazardous material release, flooding and other site-specific conditions. An example of such a matrix is provided as Table III-1 in Annex III.

7.36. The overall performance criteria should then be defined for the nuclear facility subjected to the extreme environment loads. For example, for a nuclear power plant subjected to a type 2 sabotage attack scenario, the overall performance criteria may be defined as hot or cold shutdown for 24 hours after the attack scenario is initiated, with the assumption that additional aid from outside the facility boundary can be effectively mobilized within 24 hours. In all cases, the performance criteria, including the duration of shutdown before additional aid from outside the facility boundaries can be mobilized, should be identified and approved by the competent authorities.

7.37. Following this, the assumptions that will be used in the engineering evaluation should be defined. Examples of assumptions for nuclear facilities are:

- (a) Loss of off-site power;
- (a) Plant state (e.g. material transport, material movement, full operation, shutdown/refueling/ maintenance); and
- (b) System criteria (e.g. redundancy of the success path(s)).

7.38. Next, the SSC capacity criteria should be defined, then one or more success paths should be identified, as discussed in detail in the next sub-section. Once the success paths have been determined, the required SSCs should be added to the safe shutdown equipment list. For each SSC in the SSEL, the functional requirements for achieving system performance success should be specified, and the extreme environment loads for these components should be included in the extreme environment definition matrix described above. The failure modes to be identified, evaluated and verified relate directly to these extreme environment loads. Evaluation of the capacity or fragility of SSCs relies to a large extent on the combined expertise and experience of the engineering safety personnel carrying out the evaluation.

7.39. It should then be confirmed that each candidate vital area set identified in the vital area identification process set out in Sections 4-6 contains the equipment for at least one success path. An alternative approach would be to determine the candidate vital area sets and then perform the capacity evaluation on some or all of them.

7.40. The SSCs that make up the success path(s) should be identified, given the aforementioned assumptions. The specific functions that these SSCs need to perform during and after the sabotage attack should be set out, noting that some attack scenarios may have such large affected areas that a simple screening of the overall facility site for likelihood of significant damage within these affected areas may limit the number of SSCs to be evaluated. SSCs within the affected areas of the attack scenario may be reasonably assumed to fail, and their further detailed consideration is unwarranted.

7.41. Finally, the SSC capacity when subjected to the extreme environment loads specified should be evaluated. The SSC capacity evaluation should include:

- (a) Facility familiarization, many aspects of which are accomplished during the determination of success path(s), the generation of the SSEL and the determination of the loading environment of SSEL components. Additional familiarization with specific documents for the SSCs of interest is performed during this step.

- (b) In-office and in-facility evaluations of SSCs in the SSEL, notably including a facility walkdown. In-office evaluations should involve assembling of design and qualification data for the specific SSCs in the safe shutdown equipment list. The facility walkdown should review the screening that has been performed, identify new and review proposed easy-fix concepts, review identified success paths and the SSCs in the safe shutdown equipment list, verify as-built or as-is conditions with design information, group similar SSCs and their demand environments and review vital area definitions and boundaries. Calculations should be made as necessary to determine the loading environment and the failure or capacity of the SSCs.
- (c) Confirmation of assumptions made in all phases of the evaluation during the facility walkdown, and documentation of the facility walkdown.
- (d) Documentation of the evaluation.

7.42. In evaluating capacity, considerable flexibility may be necessary to combine engineering judgement based on experience with experimental data and analysis to obtain the capacities of SSCs along a given success path. For SSCs in the ‘disposition 1’ category (see Annex III), available data may need to be supplemented with experimental data. Careful documentation is essential to ensure that all SSCs and associated operator actions on the success path have been thoroughly evaluated and meet the environmental conditions of the attack scenario under consideration.

7.43. A facility walkdown should be performed to review the screening that has been performed, to identify new and review proposed easy-fix concepts, to review identified success paths and the SSCs in the safe shutdown equipment list, to verify as-built or as-is conditions with design information, to group similar SSCs and their demand environments, to review vital area definitions and boundaries. Considerations for facility walkdowns are discussed in paragraphs 5.9 – 5.14, and in more detail in Annex II.

7.44. The impact of some type 2 sabotage attack scenarios on the safety of a nuclear facility can have commonalities with external events like earthquakes and fire. Thus, useful information can be provided by existing safety documentation as well as guidance and information contained in the IAEA Safety Standards and Safety Reports Series (see in particular Refs. [27-29]).

7.45. Sabotage margin assessment for type 2 sabotage attacks should be performed by experts in the following areas:

- (a) Nuclear safety experts knowledgeable about facility systems, security, operations, emergency response and engineering, who will be responsible for converting the stand-off scenarios into specific extreme loading conditions in different areas of the facility.
- (b) Nuclear security experts;
- (c) Experts in facility operations and on-site emergency management;
- (d) Experts in engineering safety assessment, system design and engineering (civil, structural, fire, electrical, mechanical, instrumentation and control).

In addition, experts in areas such as missiles, aircraft or demolition may be helpful in the evaluations.

7.46. The evaluation of structures should be performed using the structural acceptance criteria provided in Ref. [27]. For the evaluation purpose, less stringent acceptance criteria than safety design criteria could be used.

IDENTIFICATION OF ONE OR MORE FACILITY SUCCESS PATHS

7.47. After the relevant type 2 sabotage attack scenarios to be analysed have been identified, the next step is to identify one or more ‘success paths’ for the facility, or scenarios under which the facility is able to be safely shut down and maintained in a safe shutdown condition in response to the relevant type 2 attack scenarios.

7.48. As noted in the previous sub-section, criteria are used to define both what is meant by success (safe shutdown alone or with additional requirements) and the number of success paths needed, and is further addressed in the next sub-section. Depending on the criteria, ‘success’ in response to a type 2 sabotage attack scenario may refer only to fundamental safety functions as reactivity control, confinement and residual heat removal (“safe shutdown”) on a defined safety level.

7.49. A success path is a minimum set of systems and associated operator actions, and typically does not comprise all safety systems. In general, several possible success paths may exist. Each success path comprises a set of SSCs and associated operator actions, whose operability and survivability are sufficient to safely shut down the facility and maintain it in a safe shutdown condition for the period specified.

7.50. Success paths should be compatible with facility operations. In addition, the success paths should take into consideration facility operator training and established procedures, while recognizing that, for some type 2 sabotage attack scenarios, the damage to the facility may be so extensive that existing training and procedures may not be applicable or adequate.

7.51. SSCs subjected to extreme environmental loads on the success paths should have the capacity to withstand these loads as designed or specific measures are needed against adversaries.

7.52. If, in the course of the assessment, the successful performance of one or more of these fundamental safety functions cannot be demonstrated, means for restoring and maintaining containment integrity and reducing radiological release should be considered.

7.53. A tiered approach can be used for defining the success paths and the acceptance criteria for SSC performance:

- (e) A first tier could apply to type 2 sabotage attack scenarios that are not catastrophic, where evaluation criteria may be similar to safety design basis considerations — that is, full system redundancy (adherence to single failure criteria and redundant paths) and SSC performance limits at design levels. Two examples of such a threat are the impact of a light aircraft on-site or a vehicle bomb explosion at some distance from the facility. In these cases, it is feasible to restart the facility after inspections have been performed.
- (f) A second tier could apply to type 2 sabotage attack scenarios where only a single success path would need to be demonstrated for all attack scenarios in the tier (i.e. a means to control reactor, cool the fuel and contain the release of radioactive substances). In such cases, structure and system acceptance criteria may be significantly

relaxed compared to the safety design basis, taking into account permanent deformation of structures and components.

- (g) A third tier could apply to type 2 sabotage attack scenarios involving very extreme loads that could be catastrophic — for example, the impact of a large commercial aircraft with high speed or of multiple missiles on-site. In these cases, response should include on- and off-site emergency measures.

Each of these cases leads to a different success path or paths. For a less severe scenario, the success path may encompass all or a portion of the success path for a catastrophic event.

7.54. Documentation of the success path(s) generally includes a list of systems (front-line and support systems) and an itemization of their functions, designs and dependencies. Often, two dependency tables are created documenting the direct dependency of front-line systems on support systems and dependencies between support systems.

CONSIDERATIONS FOR THE METHODOLOGY OF COPING WITH IDENTIFIED VULNERABILITIES OF CRITICAL SSCs

7.55. At the completion of the sabotage margin assessment described above, some vulnerabilities of critical SSCs or SSCs with unacceptably low capacities may be identified. Methods for successfully mitigating adverse consequences resulting from these identified vulnerabilities should be considered, taking into account defence in depth and any additional on-site safety and security measures not considered to this point that may mitigate adverse consequences.

7.56. Available off-site resources should also be identified, such as those for emergency response (e.g., fire suppression material, pumps, cables, power supplies, heavy lifting equipment and other equipment that could be used to mitigate the results of damage from a wide range of attack scenarios). Emergency management is a task in the evaluation process, including accident management, containment performance and other mitigation measures.

7.57. For identified vulnerabilities of critical SSCs, facility management has a number of options, including

- (a) strengthening the nuclear security system for vital areas;
- (b) introducing engineered changes to SSCs;
- (c) adjusting the facility to provide a layout that is easier to protect; and
- (d) upgrading the facility's accident and emergency management capabilities.

7.58. Factors that should be taken into consideration in the decision-making process include the severity of the assessed vulnerabilities, the options available for facility upgrades, optimization of the allocation of resources required for upgrades and changes, based on estimated improvements regarding prevention or mitigation of consequences of a successful sabotage attack scenario; use of available severe accident management capabilities; and strengthening of off-site capabilities.

7.59. Options available for facility upgrades may include physical protection upgrades; safety system upgrades, including redundancy, diversity and separation measures; structural strengthening, including efforts targeting the survival of a given SSC. Additionally, if there is no warning time prior to the sabotage event, operator action during or after the attack may be essential in diagnosing the event and responding, if this is not done automatically.

7.60. Decisions to allocate the resources required for upgrades and changes should be based on estimated improvements regarding prevention or mitigation of sabotage consequences. Specifically, decisions should be based on the following:

- (a) Estimated 'performance' improvements (e.g. margin improvements)
- (b) Ease of implementation;
- (c) Time for completion of upgrade (e.g. outage);
- (d) Time at risk.

7.61. Mitigating features, such as existing accident management procedures, may need to be enhanced to better address any command and control issues and emergency plan implementation under conditions that may include partial or complete loss of the main control room, alternative shutdown panel, technical support centre and/or operating staff. This should be complemented by other intervention and response measures.

7.62. It may also be possible to strengthen off-site capabilities, for example, by the installation of physical barriers, creation of exclusion zones or surveillance of access roads to the nuclear installation by law enforcement. These measures have the potential to reduce the potential for and the severity of attacks.

7.63. It may be necessary to discuss with competent authorities how to respond to certain attack scenarios for which protection based on facility resources (e.g. engineering upgrades and enhancements of physical protection) is problematic. As an alternative, the competent authorities may decide to implement additional off-site prevention or response measures.

8. DOCUMENTATION AND INFORMATION PROTECTION

8.1. Thorough documentation should be maintained of the process undertaken to identify and categorize sabotage targets and to identify vital areas at the facility.

8.2. The documentation maintained related to this process should contain the following data:

- (a) Identification and evaluation of inventories;
- (b) Determination of potential radiological consequences;
- (c) Sabotage attack scenarios considered;
- (d) Considered facility states;
- (e) Identification of sabotage targets that could lead to URC/ HRC;
- (f) Identification of IEMOs;
- (g) Identification of safety systems that mitigate IEMOs;
- (h) Identification of sabotage targets that are needed to prevent HRC;
- (i) Definition of safe facility state;
- (j) Identification of sabotage targets needed to maintain safe facility state;
- (k) Logic model development;
- (l) Sabotage event area identification;
- (m) Identification of critical SSCs locations contained in safe shutdown equipment list (SSEL);
- (n) Identification of candidate vital area sets;
- (o) Selection of a set of vital areas;
- (p) Measures for detection, access control and delay for the protection of critical SSCs.

8.3. The organization of the documentation should be governed by four general principles:

- (a) **Traceability:** For reviewing and updating the analysis, it should be possible to trace any information with minimum effort.
- (b) **Sequentially:** The order of appearance of the analysis in the report should follow the order in which the analysis was performed.
- (c) **Transparency:** The applied thresholds and acceptance criteria, dates and names of participants need to be documented.
- (d) **Confidentiality:** The information and the developed documentation should be appropriately secured and administrated.

SECURITY OF SENSITIVE INFORMATION

8.4. The process for sabotage target identification and categorization and vital area identification generates sensitive information that should be protected properly according to information security requirements as set out by 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 this process should understand and follow relevant information security requirements. Guidance on security of nuclear information is set out in IAEA Nuclear Security Series No. 23, Security of Nuclear Information [30].

8.5. All documentation generated by this process containing physical protection information - whether on an individual basis or assembled for the purpose of assessing engineering safety aspects – should be considered security sensitive information and secured appropriately.

8.6. Notably, procedures should be in place to minimize the risk of disclosure of confidential information. Keeping security information separate from facility condition information supports the application of the need-to-know principle.

8.7. The walkdown team and support personnel (e.g. administrative support) should consist of staff for whom the trustworthiness has been assessed. Further guidance on trustworthiness assessment is contained in paragraphs 4.13 – 4.18 of Preventive and Protective Measures against Insider Threats [31].

REFERENCES

- [1] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6, IAEA, Vienna (2005).
- [2] 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).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021)
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).
- [8] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State’s Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Conversion Facilities and Uranium Enrichment Facilities, IAEA Safety Standards Series No. SSG-5, IAEA, Vienna (2010).
- [11] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Uranium Fuel Fabrication Facilities, IAEA Safety Standards Series No. SSG-6, IAEA, Vienna (2010).
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Storage of Spent Nuclear Fuel, IAEA Safety Standards Series No. SSG-15 (Rev.1), IAEA, Vienna (2020).

- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Fuel Reprocessing Facilities, IAEA Safety Standards Series No. SSG-42, IAEA, Vienna (2017).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA General Safety Requirements No. GSR Part 7, IAEA, Vienna (2015).
- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Specific Safety Requirements No. SSR-2/1, IAEA, Vienna (2016).
- [17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Specific Safety Requirements No. SSR-3, IAEA, Vienna (2016).
- [18] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Fuel Cycle Facilities, IAEA Specific Safety Requirements No. SSR-4, IAEA, Vienna (2017).
- [19] INTERNATIONAL ATOMIC ENERGY AGENCY, Storage of Spent Nuclear Fuel, IAEA Specific Safety Requirements No. SSR-3, IAEA, Vienna (2016).
- [20] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Specific Safety Requirements No. SSR-15 (Rev.1), IAEA, Vienna (2020).
- [21] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: 2018 Edition, Non-serial Publications, 2019
- [22] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, IAEA Safety Reports Series No. SRS-46, IAEA, Vienna (2005).
- [23] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).
- [24] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61, IAEA, Vienna (2021).
- [25] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Reports Series No. GSR Part 4, IAEA, Vienna (2016).
- [26] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Nuclear Installations Against External Events Excluding Earthquakes, IAEA Safety Standards Series No. SSG-68, IAEA, Vienna (2021).
- [27] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of Nuclear Power Plants in Human Induced External Events: Assessment of Structures, IAEA Safety Reports Series No. SRS- 87, IAEA, Vienna (2018).

- [28] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Reports Series No. SSG-9, IAEA, Vienna (2010).
- [29] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards in the Design of Nuclear Power Plants, IAEA Safety Reports Series No. SSG-64, IAEA, Vienna (2021).
- [30] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
- [31] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8 (Rev. 1), IAEA, Vienna (2008).

DRAFT

ANNEX I: EXAMPLE OF SABOTAGE LOGIC MODEL

I-1. This annex 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.

I-2. A logic model is ‘solved’ by applying the rules of Boolean algebra to the model. TABLE I-1 provides definitions of common logic symbols and Boolean algebra rules.

I-3. Consider a fictitious facility that has the following characteristics:

- (a) 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.
- (b) Safety system S1 is designed to mitigate IE1 and system S2 is designed to mitigate IE2.
- (c) System S1 has two trains of equipment, T1 and T2. If either of these trains function properly, S1 can successfully mitigate IE1 (that is, both trains must fail for S1 to fail).
- (d) 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).
- (e) The trains in the systems have components (designated by C below) that must operate for the trains to function.
 - (i) T1 fails if either of the two components (C1 or C2) fails.
 - (ii) T2 fails if either C3 or C4 fails.
 - (iii) T3 fails if either C5 or C6 fails.
 - (iv) T4 fails if either C7 or C8 fails.
 - (v) T5 fails if either C9 or C10 fails.
- (f) In order to cause the IEs and disable the various components, a saboteur would have to gain access to different facility 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

I-4. The statements above constitute one form of a logic model for sabotage of the facility. By carefully analysing these statements, the combinations of locations that a saboteur would have to enter to cause all the IEs and component failures that would lead to HRCs can be determined. For example, if a saboteur could gain access to L2 and L8, they could initiate IE1 and disable S1, resulting in a release that exceeds HRC limits. The saboteur can cause IE1 if they gain 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, can 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 I-1, the following equations are developed corresponding to statements 1 through 5 above:

$$\text{HRC} = \text{IE1} * \text{S1} + \text{IE2} * \text{S2} \quad (1)$$

$$\text{S1} = \text{T1} * \text{T2} \quad (2)$$

$$\text{S2} = \text{T3} * \text{T4} + \text{T3} * \text{T5} \quad (3)$$

$$\text{T1} = \text{C1} + \text{C2} \quad (4)$$

$$\text{T2} = \text{C3} + \text{C4} \quad (5)$$

$$\text{T3} = \text{C5} + \text{C6} \quad (6)$$

$$\text{T4} = \text{C7} + \text{C8} \quad (7)$$

$$\text{T5} = \text{C9} + \text{C10} \quad (8)$$

I-5. 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:

$$T1 = L1 + L2 \quad (9)$$

$$T2 = L2 + L2 = L2 \quad (10)$$

$$T3 = L3 + L3 = L3 \quad (11)$$

$$T4 = L5 + L6 \quad (12)$$

$$T5 = L6 + L6 = L6 \quad (13)$$

$$S1 = (L1 + L2)*L2 = L2 \quad (14)$$

$$S2 = L3*(L5 + L6) + L3*L6 = L3*L5 + L3*L6 \quad (15)$$

$$\begin{aligned} \text{HRC} &= L8*L2 + L9*(L3*L5 + L3*L6) \\ &= (L8*L2) + (L9*L3*L5) + (L9*L3*L6) \end{aligned} \quad (16)$$

I-6. For this simple example, there are three combinations of locations from which a saboteur could cause HRCs:

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

I-7. 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 where targets are to be protected against sabotage to prevent all possible sabotage attack scenarios leading to HRCs. This means that at least one of the areas in each combination of areas from which sabotage can be accomplished is determined as vital area. Each combination of locations whose protection will prevent all sabotage attack 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.

$$\text{HRC Prevented} = L8*L9 +$$

$$L8*L3 +$$

$$\begin{aligned}
 & \underline{L2} * \underline{L9} + & (18) \\
 & \underline{L2} * \underline{L3} + \\
 & \underline{L8} * \underline{L5} * \underline{L6} + \\
 & \underline{L2} * \underline{L5} * \underline{L6}
 \end{aligned}$$

I–8. In Eq. (18), the underline indicates that access to the location is prevented; for example, $\underline{L8}$ means access to L8 is prevented. In Boolean algebra terms, $\underline{L8}$ 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 facility that would be protected as vital areas. Protecting these two areas will ensure that none of the possible sabotage attack scenarios can be completed. Fault trees can be used to efficiently represent the sabotage logic for more complicated facilities. FIG. 7 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. FIG. 8 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 attack scenarios can be completed.

TABLE I-1. ATTACK PATHWAY KEY

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		
$A+A=A$	$A+A*B=A$	$\overline{(A+B)} = \overline{A} * \overline{B}$
$A*A=A$	$A*(B+C)=A*B+A*C$	$\overline{(A*B)} = \overline{A} + \overline{B}$

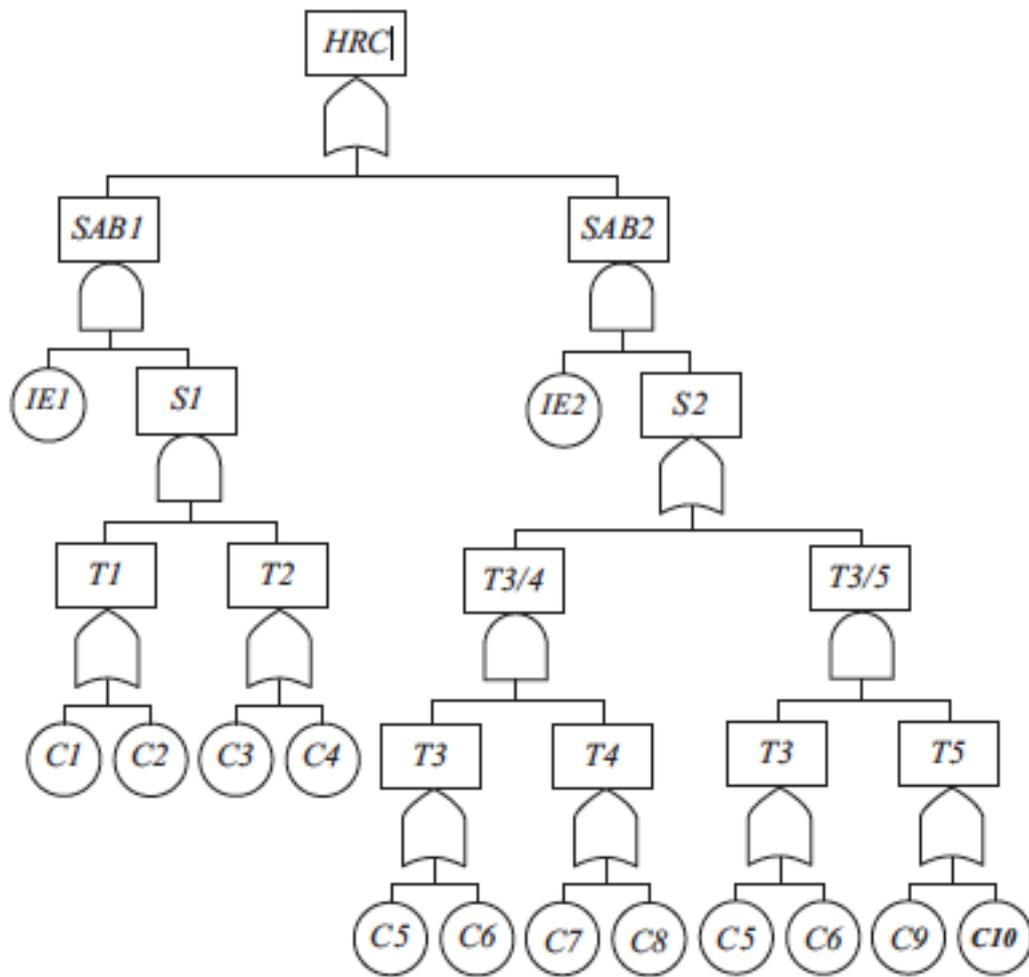


FIG. 1. Attack Pathway (HRC) Example 1

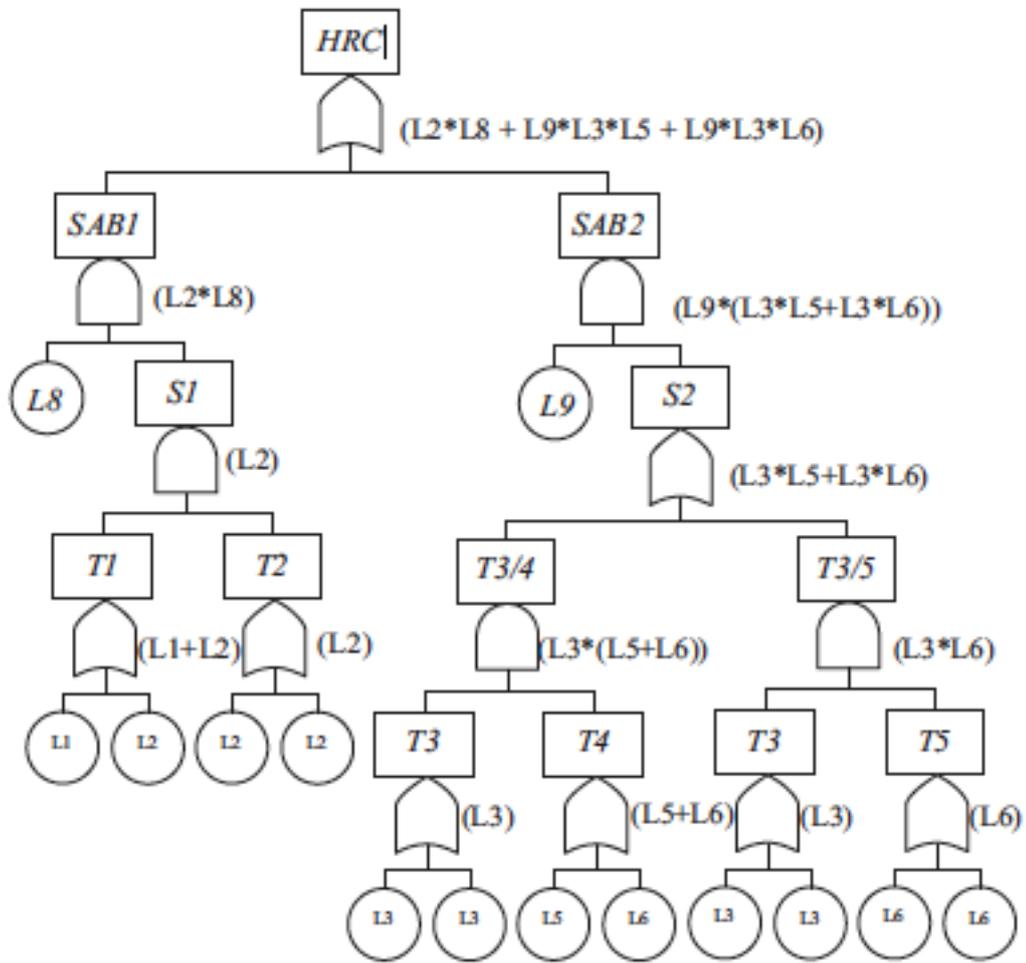


FIG. 2. Attack Pathway (HRC) Example 2

ANNEX II: FACILITY WALKDOWN

FACILITY WALKDOWN TEAMS

II-1. Facility walkdown teams consist of members of the operator's staff and consultants with specific expertise. The tasks and responsibilities are as follows:

(a) *Team leader*: The team leader supervises the field activities, engineering evaluations and security requirements. Because of the sensitive nature of this effort, the activities need to be performed in a focused and secure manner to ensure control of all related information. The team leader must be trustworthy (preferably an employee of the operator), with the authority, supervisory skills, appropriate engineering background and thorough understanding of security information control necessary to supervise these activities and ensure the security and integrity of the process. The team leader may interact with competent authorities, as necessary, to define or clarify the elements of the sabotage attack scenarios to be evaluated.

(b) *Engineering safety experts*: Engineering safety experts (experts from the operator's staff and, if necessary, consultants with specific expertise) make up the walkdown team focused on engineering safety aspects. The engineering disciplines to be represented are systems, civil, structural, mechanical, electrical, and instrumentation and control. All engineering disciplines are considered in each evaluation to ensure completeness. All engineering safety experts must be judged trustworthy by the operator, or other relevant organization (e.g. the regulator), and must have the proper clearance and training to maintain the security and integrity of the process.

(c) *Personnel from facility operations*: Facility operations personnel are an essential component of the team, and their expertise is available throughout the facility walkdown activities.

II-2. This publication focuses on engineering safety. When the nuclear security system is evaluated in conjunction with the engineering safety aspects, an integrated team may be formed, including physical protection experts. Forming such a team is particularly desirable if the sabotage attack scenarios include multimode attacks that encompass combined sabotage attack scenarios.

II-3. The team members, including the team leader, are to be assigned to the walkdown effort for as long as their involvement is needed, with minimal collateral duties.

FACILITY WALKDOWN PROCEDURE

II-4. The facility walkdown procedure comprises the walkdown preparation, the preliminary screening walkdown and the detailed screening walkdown. Facility walkdown activities and controls benefit from a separate secure workplace that ensures the security and integrity of the effort and related documentation.

Walkdown preparation

II-5. Walkdown preparation includes:

(a) Facility familiarization:

(i) General facility documentation is assembled, including safety analysis reports, system descriptions, piping and instrumentation diagrams, electrical one-line drawings, operating procedures, facility general arrangement drawings, facility mechanical and electrical equipment location drawings, probabilistic safety analyses for internal and external events, and any other beyond safety design basis assessments;

(ii) Limited nuclear security system information is assembled, in particular, designated vital area set to prevent IEMOs;

(iii) Facility access requirements are met, including radiation protection, safety practices and security practices (adherence to the ‘as low as reasonably achievable’ (ALARA) principle is required).

II-6. Facility documents on success paths and the SSCs in the safe shutdown equipment list (SSEL) are consulted or created, and the environmental demand on each SSC in the SSEL, including physical and security demands, is defined.

II-7. A database of the safe shutdown equipment list (SSEL) is to be prepared summarizing the evaluation of each SSC in the SSEL for the demand environments. It is expected that the SSEL of a nuclear power plant will comprise a few hundred SSCs. Other facility types may have significantly fewer SSCs in their SSELs.

II-8. Individual SSC data sheets are to be prepared containing some of the above mentioned information. If necessary, the data can be supplemented with field and office generated SSC specific evaluations, including field notes; safety, security and engineering analyses performed; and field modifications.

II-9. An in-facility walkdown plan is to be developed indicating the number of teams and the composition of each team. It is expected that more than one team will be used, with the total number depending on the issues to be considered, the experts required and confidentiality requirements.

II-10. TABLE II-1 illustrates a format that can be used for the SSEL database.

- (i) Explosion/blast effects to be considered can be direct or indirect. Direct impact effects are blast pressures; indirect blast effects are conditions such as vibration induced loadings.
- (j) Heat/fire refers to heat from a fire or direct flame effects on the SSC.
- (k) Smothering and related conditions may arise as a result of smoke, toxic chemicals or firefighting techniques. This failure mode may affect personnel or systems; for example, smothering of the diesel generator system could occur if the air intake system is inundated. Control room habitability and on-site security personnel safety is to be evaluated.
- (l) Flooding from internal or external sources may need to be evaluated.

II-12. TABLE II-2 provides a sample format for individual data sheets in the evaluation of SSCs with regard to physical loading conditions. In the pre-walkdown stage, the basic information identifying the SSC under consideration is entered into the forms; the remainder of the table is filled out upon completion of the walkdown and evaluations. Documentation of the evaluation then comprises these summaries and the detailed evaluations. TABLE II-2 is based on the data sheets used for SSC evaluations for seismic and other external events. For the seismic evaluation case, unique data sheets exist for each of the 22 equipment categories. Each category has unique equipment characteristics and conditions that need to be evaluated to verify the seismic performance. These data sheets, called 'screening evaluation work sheets', or SEWS, were the basis for developing similar worksheets for the current evaluation. The data to be collected and evaluated may need to be modified to take into account non-vibrational modes of failure, that is, environmental conditions such as heat, humidity and direct impact.

TABLE II-2. EXAMPLE OF A SCREENING EVALUATION WORK SHEET (SEWS) FOR PHYSICAL LOADING CONDITIONS

SSC name: _____ SSC ID No.: _____

SSC description: _____

Location: Bldg. _____ Elev. _____ Room/compartment/row/col. _____

Threat scenario No./description: _____

Vital area identification: _____

Performance requirements: _____

SUMMARY (capacity versus demand)

Impact loads:

Direct: _____

Indirect: _____

Blast loads:

Direct: _____

Indirect: _____

Heat/fire loads:

Heat: _____

Fire: _____

Preliminary screening walkdown

II-13. The preliminary screening walkdown achieves the following objectives:

- (a) Determine the location and accessibility of each SSEL SSC in the facility;

- (b) Identify any other SSCs needed for safe shutdown, which are then be added to the SSEL;
- (c) Review and validate screening of SSCs with respect to capacity considerations;
- (d) Identify potential easy-fixes;
- (e) Group all the components belonging to the same system;
- (f) Group components within the same location, particularly in the same vital area, for evaluation of spatially common environments;
- (g) Evaluate whether SSC capacity is adequate for the specified threat(s);
- (h) Document conclusions.

II-14. The preliminary screening walkdown visually examines those SSCs that are accessible. There are three alternative dispositions for each SSC on the SSEL:

- (a) Disposition 1: For SCCs in this category, capacity is clearly less than the demand and a modification is required.
- (b) Disposition 2: The capacity of SSCs in this category is uncertain, and further evaluation is needed to determine whether a modification is required.
- (c) Disposition 3: For SSCs in this category, the capacity is clearly greater than the demand and the SSC is adequate for the specified threat.

II-15. The preliminary screening walkdown is to be properly documented. The main result of the preliminary walkdown is the identification of SSEL SSCs that are obviously robust. These SSCs are categorized as disposition category 3 and are therefore excluded from further evaluation. SSCs in disposition categories 1 and 2 require a more detailed in-office and in-facility evaluation.

Detailed screening walkdown

II-16. The detailed screening walkdown is to be performed for all SSCs whose capacity for the defined environment loadings has not been verified. This includes in-facility evaluations and, in many cases, further analytical calculations and evaluations. Two categories of SSCs result:

- (a) SSCs in the first category are those that were not excluded from further consideration during the preliminary walkdown. At this stage, walkdown engineers evaluate these systems and components in more detail and make a judgment as to whether or not the component requires further analysis or modification.
- (b) For SSCs in the second category, facility modifications are clearly warranted. In these cases, the walkdown engineers suggest that the modifications be implemented.

II-17. The detailed screening walkdown is to be properly documented. It is advisable to supplement the documentation with photographic and/or video records. TABLE II-2 is an

acceptable form of summary documentation for the entire SSEL. The SSC evaluations may be documented using the form given in TABLE II–2, with supporting material attached.

II–18. Confidentiality of the documentation is to be strictly maintained, with distribution on a need to know basis only.

SPECIAL TOPICS

Interactions

II–19. The facility walkdown is a key tool for identifying spatial interactions that could potentially affect the performance of SSEL. A major concern in these areas is ‘housekeeping’. The identification and assessment of potential interactions requires good judgement from the walkdown team.

Falling

II–20. Falling is the structural integrity failure of a non–safety or safety related SSC that could hit and damage a safety related SSC. For the interaction to be a danger to an SSEL SSC, the impact must contain considerable energy and the target must be vulnerable.

II–21. For example, a light fixture falling on a 10 cm diameter pipe may not be a credible damage threat to the pipe. However, the same light fixture falling on an open relay panel is an interaction that could cause damage and is to be addressed. Scabbing of concrete due to missile impact on a building element (wall, diaphragm or roof) may be a viable failure mode for delicate equipment in the range of the falling concrete. Unreinforced masonry walls are a common source of falling interaction. Masonry walls are generally located close enough to the safety related equipment that their failure could lead to equipment damage.

Proximity

II–22. Proximity interactions are defined as conditions where two or more SSCs are close enough that the behaviour of one may have consequences for the other(s). The most common example of proximity interaction is fires or explosions; these interactions are discussed in Ref. [3].

Spray and flood

II–23. Spray and flood can result from the failure of piping, systems or vessels that are not properly supported or anchored. Inadvertent spray hazards to SSEL SSCs are most often associated with wet fire protection piping systems. The most common source of spray is leakage caused by impact induced failures of sprinkler heads. Since fire and heat are potential safety threats throughout the facility site, particularly in buildings and compartments, the walkdown evaluates the vulnerability to spray of all SSEL components. Generally, design evaluations of fire and fire suppression systems will have taken spray vulnerabilities into account. If spray sources can reach equipment sensitive to water spray, then the source is back fitted, usually by adding support to reduce deflections and impact or stress. An alternative is to protect the target — in this case, the SSC.

II-24. Large tanks may be potential flood sources. The walkdown team, with the assistance of facility personnel, assesses the potential consequences of a flood source failure and the ability of the floor drainage system to mitigate the consequences of a source failure.

Type and number of co-located facilities at the site

II-25. A nuclear power plant site may have several reactor units, possibly with interdependent safety or support systems; multi-unit sites often assume the availability of companion unit systems when addressing non-common-cause events. In addition, other critical facilities may be present within the site boundary, such as spent fuel storage in fuel pools or dry cask storage. Research reactor sites may have associated laboratories, isotope production facilities and hot cells. The evaluation takes all on-site facilities into consideration, including any interdependence of their safety systems. Such consideration includes consequence evaluation of environmental discharges that are cumulative for all facilities at the site.

ANNEX III: EXAMPLE OF EXTREME ENVIRONMENT LOAD EVALUATION

III-1. TABLE III-1 contains an example for the evaluation of the load resulting from an air craft crash, more detailed and general guidance for the assessment (e.g. including structures) is contained in Reference [28]. Depending on the State’s threat assessment and sabotage attack scenarios to be considered, these accidental events could be taken for evaluating extreme sabotage attack scenarios.

TABLE III-1. EXAMPLE OF AN EXTREME ENVIRONMENT LOAD MATRIX

Sabotage attack scenario No.	Sabotage attack scenario description	Physical loading condition						
		Impact (Table III-2)	Explosion/blast (Table III-3)	Heat/fire (Table III-4)	Hazardous material release (Table III-5)	Smothering (Table III-6)	Flooding (Table III-6)	Other (Table III-6)
1	Impact of fully fuelled Boeing 767 flown into nuclear power plant site	1, 2	None	1	None	None	None	None
2	Shoulder launched missile fired into reactor building							
3	Truck explosion at site gate							

III-2. The columns of TABLE III-1 are as follows:

- (a) Sabotage attack scenario No. is a numerical identifier with values ranging between 1 and the total number of scenarios considered. Example: Sabotage attack scenario No. 1 is assumed.
- (b) Sabotage attack scenario description is a brief description of the sabotage attack scenario for identification purposes. Example: The scenario involves the impact of a fully fueled Boeing 767 flown into the nuclear power plant site.

(c) Physical loading conditions are numerical identifiers of the type and specifics of loading conditions imposed by the sabotage attack scenario. The identifiers correlate directly with TABLE III–2 for impact, TABLE III–3 for explosion/blast, TABLE III–4 for heat/fire, TABLE III–5 for hazardous material release and TABLE III–6 for other environmental consequences. TABLE III–6 provides guidance on the engineering disciplines required in the evaluation and background on why certain environment load combinations need to be considered.

(d) Impact refers to impact loading condition(s) identified by number and reference to TABLE III–2. Example: Impact loading conditions 1 and 2 are assumed.

(e) Explosion/blast refers to explosion/blast loading condition(s) identified by number and reference to TABLE III–3. Example: No blast or explosion loads are associated with sabotage attack scenario No. 1 or considered to be ancillary effects of the aircraft impact.

(f) Heat/fire refers to heat/fire loading condition(s) identified by number and reference to TABLE III–4. Example: Heat/fire environment loading condition 1 is assumed.

(g) Hazardous material release refers to hazardous material release condition(s) identified by number and reference to TABLE III–5. Example: No hazardous material release condition is associated with sabotage attack scenario No. 1.

(h) Smothering, flooding and other phenomena are identified in TABLE III–1 as examples for future consideration. Smothering, choking and depriving SSCs of necessary air for operation are suggested as potential concerns; for example, lack of air to diesel generators could prevent startup and operation. Smothering due to firefighting techniques (foam) may need to be evaluated. Flooding of the site from internal or external sources also may need to be evaluated; for example, sabotage of an upstream dam could release a large quantity of water to flood the site.

III–3. TABLE III–2 identifies the impact parameters to be used by facility engineering for the evaluation of SSCs. The sabotage attack scenario example from TABLE III–1 is continued here for illustrative purposes only.

TABLE III–2. EXAMPLE OF AN IMPACT PARAMETER DEFINITION MATRIX

Missile type/No.	Description	Mass/weight	Missile impact				Ancillary effect		
			Shape/configuration	Impact angle	Impact velocity	Relative hardness	Fire	Explosion/blast	Other
1	Boeing 767 fuselage, fully	200 000 kg	Flexible	Less than 30° from horizontal	180 m/s	Flexible	1	None	None
2	Boeing 767 engines as projectiles	3 500 kg	3 m diameter/rigid cylinder	Less than 30° from horizontal	180 m/s	Rigid	None	None	None
3									

--	--	--	--	--	--	--	--	--	--

III-4. The columns of TABLE III-2 are as follows:

- (a) Missile type/No. is the missile load identifier with values ranging between 1 and the total number of missile impact scenarios considered.
- (b) Description briefly describes the source of the loading condition.
- (c) Mass/weight refers to the mass/weight of the missile
- (d) Shape/configuration provides a more specific description of the missile, with dimensions specified if available. The example, Missile No. 1, is described as a flexible fuselage, with dimensions to be determined; for missile No. 2, the engines are assumed to be rigid, with dimensions as shown.
- (e) Impact angle refers to the angle or range of potential impact angles, taking into account the physics and human capability necessary to achieve the objective.
- (f) Impact velocity is the velocity of the missile, taking into account the physics and human capability necessary to achieve the objective.
- (g) Relative hardness is an important parameter for assessing the effect of the missile on SSCs; it can be a qualitative or quantitative measure.
- (h) Ancillary effects are effects that are consequential to the direct impact — such as spalling or scabbing of concrete — that have an ancillary effect on components in the neighbourhood of the impact. They may be specified in other places in the specification, such as fire in the example used here.
- (i) The missile impact causes a fire either by carrying a combustible or by impacting a combustible, such as a diesel oil tank. Missile No. 1 in the example is associated with heat/fire condition 1, which is a jet fuel fire resulting from an aircraft impact. Missile No. 2 has no related fire condition.
- (j) The missile impact causes an explosion/blast either because the missile is carrying explosives, which detonate upon impact, or because the missile impacts an explosive storage facility.
- (k) Other hazards can include, for example, intruders working in coordination with the missile attack.
- (l) TABLE III-3 identifies a simplified set of parameters for explosion/blast loading conditions to be used by facility engineering for the evaluation of SSC capacity. In the example used here, no explosion/blast conditions were assumed. The columns in TABLE III-3 are as follows:
- (m) Explosion No. is the explosion/blast condition identifier for the of blast conditions considered in the example.

(n) Parameters in TABLE III-1 are examples of descriptors of the explosives' characteristics. For general descriptions, TNT equivalent and reference distance (measured from a facility reference point) are the most general information. Specific information about the incident and reflected waves would be developed for individual nuclear power plants under evaluation. The details are a function of numerous site-specific characteristics.

TABLE III-3. EXAMPLE OF AN EXPLOSION/BLAST PARAMETER DEFINITION MATRIX

Explosion No.	Description	TNT equivalent	Reference distance	Pressure pulse	
				Incident	Reflected
1					
2					
3					

III-5. TABLE III-4 identifies the heat and fire characteristics to be used by facility engineering for the evaluation of the SSCs.

TABLE III-4. EXAMPLE OF A HEAT/FIRE PARAMETER DEFINITION MATRIX

Fire No.	Description	Fire source outside facility					Fire source or combustibles inside facility				
		Combustible/ignition	Quantity	Heat potential/temperature	Duration of burn	Other	Building / yard	Quantity	Type	Ignition likelihood	Duration of burn
1	Jet fuel fire	Yes	50 000 kg	1 000°C	1-8 h						
2											
3											

III-6. The columns in TABLE III-4 are as follows:

- (a) Fire No. is the heat/fire condition identifier with values ranging between 1 and the total number of fire conditions considered.
- (b) Description briefly describes the source of the fire.
- (c) Entries in the 'Fire source outside facility' category define the fire hazard assuming the source is outside the facility. For an aircraft impact or other similar sabotage attack scenario, the distribution of the combustibles within and outside the facility boundary is important. Two obvious distributions are the facility yard and penetration into buildings. Others include those distributions outside the facility boundaries that could inhibit access by emergency responders and others. Examples of important parameters are the quantity and type of combustible,

estimates of heat potential and temperature, and duration of burn. As example, jet fuel from a Boeing 767 is spilled and ignited; there is no penetration into buildings. The quantity of fuel is 50 000 kg. The duration of burn at high temperature (1000°C) is 1 hour maximum, with 5–7 hours of residual fire at 300°C.

(d) Entries in the ‘Fire source or combustibles inside facility’ category define the fire hazard assuming the source is inside the facility or that the fire is ignited inside as a consequence of an outside source. Examples of important parameters are type and quantity of combustible, location and estimated duration of burn.

III–7. TABLE III–5 identifies important parameters for hazardous material release conditions at the nuclear power plant. Hazardous material releases in conjunction with other modes of simultaneous attack appear to be credible; the other modes could include adversaries protected against the effects of the chemical releases. No hazardous material release was assumed in the example.

TABLE III–5. EXAMPLE OF A HAZARDOUS MATERIAL RELEASE DEFINITION MATRIX

Case No.	Material description	Hazardous material loading condition						
		Quantity	Smothering effect — personnel	Smothering effect — components	Lethal or disabling effect — personnel	Duration	Extent of penetration	Other
1								
2								
3								
4								

III–8. The columns in TABLE III–5 are as follows:

- (a) Case No. is the hazardous material release number with values ranging between 1 and the total number of hazardous material release conditions considered.
- (b) Material description briefly describes the hazardous material.
- (c) Quantity refers to the amount of the material released and the time frame over which the release occurs.
- (d) Smothering effect — personnel provides an itemization of the physical effects on personnel (e.g. facility operating staff, security forces), including an indication of whether protective gear is required and the time frame of implementation.
- (e) Smothering effect — components identifies the potential effects on components of smothering or choking, for example, whether emergency diesel generators could be adversely affected by the atmospheric dispersion of a particular chemical.

(f) Lethal or disabling effect — personnel identifies the potential effects on facility personnel.

(g) Duration is the time frame during which the hazardous material is present, with an indication of whether or not dispersion occurs.

(h) Extent of penetration describes the extent to which the hazardous material migrates into buildings through flow paths, including heating, ventilation and air conditioning systems, or remains in the facility yard.

III–9. The extreme environment definition matrices, TABLE III–6, contains the definition of loading environments and load combinations for engineering evaluations.

TABLE III–6. EXAMPLE OF AN EXTREME ENVIRONMENT LOAD DEFINITION MATRIX

Plant area	Vital	Descriptio	Physical loading condition						
			Impa	Explosion/ blast	Heat/fir	Hazardous material	Smotherin	Flooding	Other
Building 1									
2									
3									
Zone 1									
2									
3									
4									
Yard 1									
2									
SSEL item 1									
2									
3									