IAEA Nuclear Security Series No. 4

Technical Guidance

Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage

IAEA
International Atomic Energy Agency

THE IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

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

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

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

ENGINEERING SAFETY ASPECTS OF THE PROTECTION OF NUCLEAR POWER PLANTS AGAINST SABOTAGE

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

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

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

IAEA NUCLEAR SECURITY SERIES No. 4

TECHNICAL GUIDANCE

ENGINEERING SAFETY ASPECTS OF THE PROTECTION OF NUCLEAR POWER PLANTS AGAINST SABOTAGE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2007

COPYRIGHT NOTICE

Printed by the IAEA in Austria
January 2007
STI/PUB/1271

IAEA Library Cataloguing in Publication Data

Engineering safety aspects of the protection of nuclear power plants against sabotage : technical guidance. — Vienna : International Atomic Energy Agency, 2007.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 4)
STI/PUB/1271
ISBN 92–0–109906–1
Includes bibliographical references.

1. Nuclear power plants — Security measures. 2. Sabotage. 3. Nuclear industry — Security measures. I. International Atomic Energy Agency. II. Series.

IAEAL 06–00467

FOREWORD

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

Since the attacks of 11 September 2001, the perception of the potential terrorist threat to nuclear installations has changed significantly. Within the nuclear industry, the immediate international response was to enhance security by augmenting the forces guarding installations, increasing physical protection by installing additional security devices, enhancing protection procedures, tightening access control, increasing standoff distances for surface vehicles, reviewing and updating emergency preparedness, and generally increasing awareness of the need for close cooperation, at all levels, between government and private sector entities concerning warning and response.

It was less clear what additional analyses could and should be performed to determine whether the structures, systems and components important to safety at nuclear power plants provide optimum physical protection against potential terrorist attacks and to identify any cost beneficial changes in the form of backfits. Many licensees of nuclear power plants around the world, in some cases mandated by their regulatory agencies, carried out calculations of the robustness of plant structures when subjected to aircraft impacts, taking into account dynamic and resulting fire effects. These calculations were generally limited to the performance of passive structures and systems.

In any terrorist attack or act of sabotage, the overarching concern is to achieve and maintain a safe shutdown condition, including continued availability of heat sinks and containment of radioactive material until the incident has been brought under control. This publication provides guidelines for the assessment of the engineering safety aspects of the protection of nuclear power plants against sabotage, including standoff attacks.

This publication is the result of extensive dialogue between safety and security specialists within and outside the IAEA. It also takes into account feedback from regulatory agencies and design organizations. It expands on more general concepts concerning the physical protection of nuclear material and nuclear facilities against sabotage. The two main outside contributors to drafting were J.J. Johnson and G.J.K. Asmis. The IAEA officer responsible for this publication was A. Gürpinar of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The protection of nuclear installations against malicious acts can take a number of different forms. This publication addresses only issues related to the sabotage of nuclear facilities, that is, the prevention or mitigation of sequences initiated by malicious acts that may have potential radiological consequences.

The guidelines in this report take into account the existing robustness of structures, systems and components (SSCs). It is important to note that nuclear installations in general, and nuclear power plants in particular, can be considered to be well protected against terrorist attacks. They have good physical protection systems (PPSs) and procedures, and they are designed to minimize the likelihood of an accident and, in the event of an accident, not to release radioactive material in an uncontrolled manner. Furthermore, nuclear power plants are specifically designed to handle internal and external extreme loads such as vibration, heat, overpressure and impact. The resistance of nuclear installations to extreme events depends on their particular site and design characteristics, for example, loads — and therefore the required resistance (capacity) — due to extreme winds, wind borne missiles, earthquakes, internal pressure from a loss of coolant accident (LOCA) and fires.

In the context of this publication, self-assessment (hereinafter referred to simply as 'assessment') is the assessment of the protection of a nuclear power plant against sabotage, including standoff attacks (i.e. specified threat scenarios), undertaken by the licensee together with the relevant local or State authorities.

1.2. OBJECTIVE

In the light of the current threat environment, the overall objective of this publication is to provide methods for evaluating — and, if necessary, for proposing corrective actions aimed at reducing (mainly through upgrades) — the risk related to any malicious act that, directed against a nuclear power plant, could endanger the health and safety of plant personnel, the public and the environment through exposure to radiation or the release of radioactive substances.

These guidelines describe a methodology for assessing the capacity of a selected subset of a nuclear power plant's safety related SSCs to withstand

sabotage induced events. The proposed methodology, which includes screening, applies existing safety margin assessment techniques in an integrated manner.

Specifically, the aims of this publication are to:

(a) Provide a link between the information in The Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev. 4) [1], general guidance on the physical protection of nuclear material and nuclear facilities against sabotage, and engineering safety aspects of protection against sabotage;
(b) Provide a link with general guidance on the identification of vital areas within nuclear facilities and on the development and maintenance of the design basis threat (DBT);
(c) Provide general guidelines for the assessment of nuclear facilities in relation to sabotage induced sequences;
(d) Use common terminology drawn from established (i.e. consensus) definitions or define new terms, when necessary, to clarify joint safety/security concepts;
(e) Propose a safety margin assessment approach that allows for the use of different acceptance criteria from the design process (e.g. best estimate versus design allowable);
(f) Provide for an assessment process so that decisions can be made by the operator (or regulator) of an installation concerning the need to enhance or upgrade the safety related SSCs, the physical protection measures or on- or off-site emergency procedures;
(g) Serve as a foundation document for future manuals, technical guides, investigative tools and services.

1.3. SCOPE

This publication covers all nuclear facilities, including nuclear power plants, research reactors, fuel fabrication plants, reprocessing plants and spent fuel storage facilities. However, the emphasis is on nuclear power plants because they involve the most complex analysis.

Events considered to be within this scope include those that:

(a) Involve forced intrusion into the protected area of the site (i.e. the area under the administrative control of plant management), such as by a ‘malicious vehicle’ (e.g. a truck loaded with explosives and carrying armed intruders).

(b) Are initiated by persons outside the site area. Such an event may involve missiles, the release of a toxic gas within the site area or an aircraft steered to hit the installation.
(c) Are initiated by insiders.
(d) Include multiple modes of attack, for example, combinations of the above events.

For reactor facilities, the malicious act may target either systems whose failure would cause core damage, leading to radiological consequences, or areas where nuclear fuel (fresh or spent) or radioactive material is kept or stored. For non-reactor facilities, targets of the second kind are the most relevant.

Events considered to be outside the scope of these guidelines include attacks:

(i) Whose sole aim is the theft of nuclear or other radioactive material;
(ii) That take place during the transport of nuclear material;
(iii) That involve only economic loss.

2. BACKGROUND

The methodology presented in this publication has been designed so that operating staff and safety specialists work in close cooperation with security specialists, those agencies responsible for emergency preparedness and other government agencies at all levels to provide defence in depth against sabotage initiated events. This section outlines this interrelationship and suggests policies and criteria to enable the detailed engineering evaluation described in Section 3 and the decision process described in Section 4.

The flow chart in Fig. 1 shows how all of the entities involved work together to protect the nuclear power plant in the case of a malicious act. A more detailed description of the flow chart, including an explanation of the boxes and decision points, is given in Appendix I.

Two types of threat are distinguished:

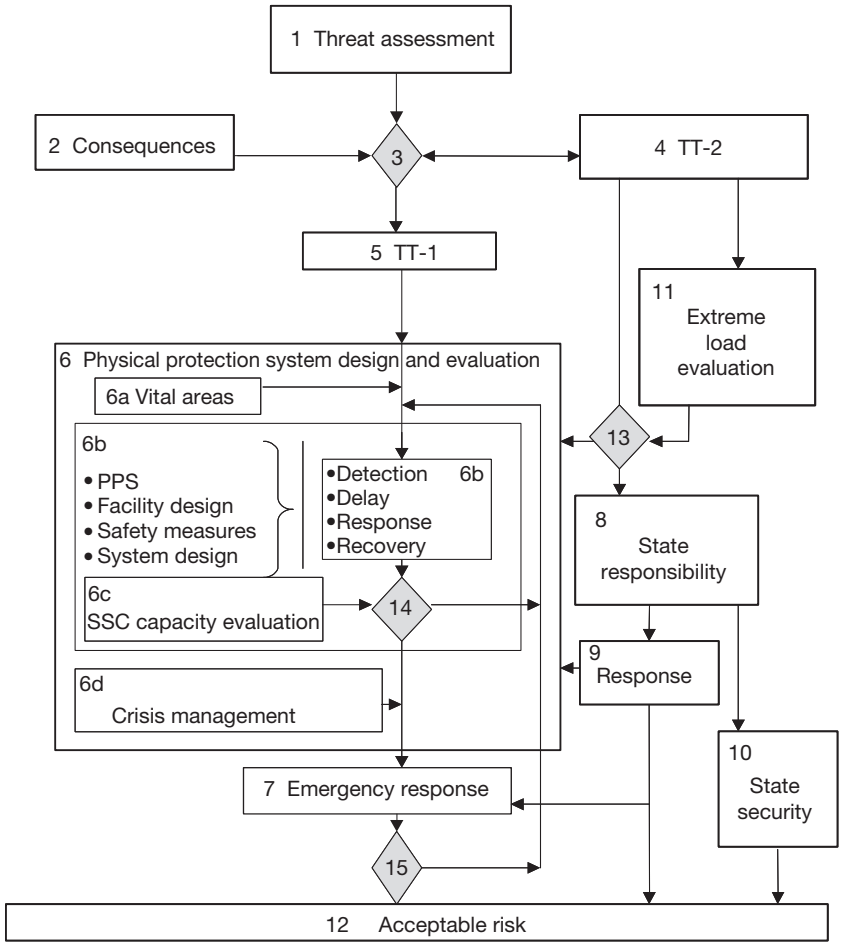

FIG. 1. Physical protection of nuclear material and nuclear facilities against sabotage.

(a) Threat type 1 (TT-1) refers to those threats posed to the nuclear power plant by insiders or by adversaries intending to intrude into the facility (with or without insider assistance).

(b) Threat type 2 (TT-2), in contrast, refers to threats that are initiated outside the plant boundary and do not require the presence of the adversaries on-site. Examples of this type of threat include standoff attacks such as shoulder launched missiles and malicious aircraft impacts.

This distinction is made to reflect differences in the ways engineering measures are used to counter each type of threat. For TT-2, these measures provide the main elements of protection against sabotage, whereas for TT-1, they provide an additional layer of defence in depth and their use needs to be closely coordinated with physical protection measures.

A consensus that has emerged in facing the challenges of the current threat environment is that cooperation across all national entities is needed. This includes government agencies such as the intelligence services, the armed forces, the police, local government authorities, municipalities and civil defence organizations.

Specific criteria are needed to perform risk assessments. Generally, these criteria are provided by the nuclear regulator. The following is a sample set of criteria:

(a) Is the nuclear power plant sufficiently robust to prevent immediate, uncontrolled release of significant amounts of fission products (i.e. catastrophic failure) in the event of an attack?
(b) Do the essential safety systems continue to perform their functions (e.g. to cool the nuclear fuel and contain the release of radioactive material), or can they be started and operated as needed?
(c) Following an attack, can the essential safety systems be operated until repairs can be carried out, even given related effects such as fire, smoke and structural damage?
(d) Are the design and operation of the nuclear power plant and the response procedures and capabilities such that any exposure of the public and facility personnel is minimized in the event of a large external attack?

Acceptance criteria for survival capabilities of safety SSCs, operator actions and functioning of emergency plans and procedures may be based on realistic (i.e. not conservative) assumptions.

A key criterion for the assessment has to do with the number of success paths and the behaviour limits of the SSCs on these success paths.

The evaluation methodology outlined in Section 3 provides a means to determine whether one or more safe shutdown paths exist to perform the required safety functions when subjected to a given threat scenario. In this publication, the term ‘success path’ refers to a minimal set of components for a subset of plant systems whose operability and survivability are sufficient to ensure that the plant performance criteria are met, as required and defined by the regulator or other governing body. A success path may include plant functions beyond safe shutdown if the metric of interest is radioactive release to the environment below an acceptable limit. The term ‘safe shutdown path’ is

defined here as a minimal set of components required to achieve and maintain a safe shutdown condition without consideration of containment or exposure of the public due to radioactive releases. While the terms 'safe shutdown path' and 'success path' are not necessarily identical, they are used interchangeably in this publication. Furthermore, the term 'performance criteria' is used to denote criteria related to the type of function (performance) required from the SSCs. The term 'acceptance criteria', in contrast, refers to the allowable behaviour limits for the SSCs in relation to the given function. Both are determined by the regulatory body.

The methodology can also be used for tiered acceptance criteria. For example, for scenarios resulting from the DBT, the acceptance criteria may be similar to the design parameters, that is, full safety system redundancy and the integrity of the safety related systems and structures are maintained. For scenarios that are beyond the DBT, acceptance criteria may allow the survival of only one success path and the use of realistic behaviour limits for the required SSCs.

The result of the assessment may be that, for a given threat scenario, no safe shutdown path is shown to be capable of meeting the acceptance criteria of the Member State. In this case, the Member State may decide to manage the situation on the basis of further measures such as off-site prevention and mitigation of the threat scenario, and appropriate response measures.

The criteria related to the number of required success paths prescribed by the regulatory authorities determine the complexity of the assessment process. For example, if the availability of only one success path is envisaged and realistic behaviour limits for the SSCs are allowed, then the number of SSCs to be evaluated will be relatively small (because there is only one path) and the screening process for robustness will be more straightforward. In most cases, safe shutdown is considered to be 'success' and the SSCs on this path constitute a 'safe shutdown equipment list' (SSEL). It is important to note that the assessment process is focused on the SSEL from the outset.

3. EVALUATION METHODOLOGY

3.1. OVERVIEW

Section 3 is organized as follows: Section 3.2 lists the input needed for the evaluation in terms of scenarios derived from the threat assessment; for the purposes of this report, the scenarios are identified as TT-1 or TT-2. Section 3.3 describes the process for screening TT-2 scenarios with regard to the specific nuclear power plant being evaluated. This process yields a set of threat scenarios for evaluation, specific considerations for the site and facility, and a ranking of these threats by level of perceived risk to the facility. Section 3.4 describes the conversion of the threat scenarios into engineering parameters for detailed evaluation. Section 3.5 summarizes the connection between the engineering safety evaluation and the PPSs and measures available at the plant. A brief discussion of vital area identification (VAI) and its relationship to the concepts of success paths and safe shutdown paths is also included. Section 3.6 details the methodology to be used for the engineering safety evaluations of the TT-1 and TT-2 scenarios. Elements of the methodology include success path identification, creation of the SSEL (components and their functional performance requirements), SSC capacity evaluation, establishment of assessment teams, the plant walkdown and documentation requirements. The evaluations in Section 3.6 indicate the capacities of the components of the SSEL to withstand malicious attacks; these capacities are considered in Section 4 with respect to decision making.

3.2. THREAT EVALUATION

The State defines the consequences with regard to which the nuclear threat is to be evaluated. In the case of sabotage, the criteria are related to the safety of plant personnel and the public, and the risk acceptance criteria are described in terms of radiological consequences [1].

The DBT describes the "attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated" [1].

Threats that may need to be considered by the plant but that are not included in the DBT are referred to as being 'beyond the DBT'. The distinction is made because acceptance criteria used for events beyond the DBT may

differ from those used for DBT events. All threats may also be described in terms of TT-1 and TT-2.

3.3. DEVELOPMENT OF SPECIFIC THREAT SCENARIOS

This step in the evaluation process aims at better defining the threat scenarios with regard to the specific facility being evaluated. This process may lead to the exclusion of some scenarios on the basis of the following considerations:

(a) *Site and installation characteristics:* The surrounding topography and vegetation may be sufficient to exclude certain scenarios of threats initiated outside the plant boundary. For certain types of threat, the location and layout of the plant site may limit the likelihood that particular on-site areas will be affected. For example, a plant's location in hills, mountains or a valley may limit the feasible approach angles and speed of large aircraft in an 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 taken into account. Similarly, 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. Research reactors tend to be located within research centres or on university campuses, which may make the identification of potential intruders or attackers difficult.

(b) *Type and number of facilities at the site:* A nuclear power plant may have several reactor units on-site, with the possibility of 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 plant boundary, such as those for spent fuel storage in fuel pools or dry cask storage. Research reactor sites may have associated laboratories, isotope production facilities and hot cells. All facilities at the site may require simultaneous physical protection when subjected to TT-2 attacks. The evaluation should take into consideration all on-site facilities and any interdependence of their safety systems. Such consideration includes consequence assessment of environmental discharges that are cumulative for all facilities on a site.

(c) *Design:* Nuclear power plants are designed for a wide range of extreme environmental loading conditions. The measures to defend against design basis internal and external events — such as fire, pipe whip, LOCA, earthquakes, extreme winds, explosions or aircraft impacts — provide an 'envelope' of protection for a nuclear power plant. It is important that this protection be taken into account when evaluating threat 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 item) or the sizing requirement derived from the loads.

(d) *Facility independent off-site security measures:* Administrative and other measures in force outside the plant boundary are called facility independent off-site security measures. 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 threat scenarios from consideration or to better define the parameterization of threat scenarios.

In the screening process for external events of a natural or an accidental human induced origin, two methods are generally used: screening by distance and magnitude, and screening by probability of occurrence. In the first method, the minimum distance and the maximum magnitude (i.e. the most conservative conditions) of the event are postulated with regard to the nuclear power plant site, and the potential damaging effects on plant safety are assessed. If the effects are found to be insignificant, the event is screened out with regard to the assessed parameter. For example, an attack scenario involving a vehicle containing explosives may be screened out on the basis of the effective barrier's distance from the safety related systems of interest. Screening by probability is generally more complex and uncertain, and may be applied to events not screened out by distance and magnitude. The probability level used for screening is generally one or two orders of magnitude smaller than that used for design purposes; 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. However, 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 events, depending on the saboteurs' objectives and capabilities, this assumption may not hold.

Sabotage events do not lend themselves to probabilistic screening on an absolute probability basis. However, Section 3.6.1 presents an approach utilizing the probabilistic safety assessment (PSA) tools adapted to address threats, where conditional end metrics are calculated and may provide the basis for screening individual threats. 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 plant layout, systems design and structural robustness.

Other actions that can be implemented at this stage to reduce the effort needed to evaluate the facility for the threat scenarios include the following:

(a) Threat scenarios can be grouped according to similarities in effects on the nuclear facility. One scenario or a composite of the grouped threat scenarios can be selected for detailed evaluation. Grouping threat scenarios in this way reduces them to a more manageable number. A panel of experts in threat definition and nuclear safety could be appointed for this activity.
(b) Structures, systems and components that have low capacity and safety importance can be screened out; for example, some structures may be identified as having low capacities and thus be excluded from consideration in the success path definition.

3.4. EXTREME ENVIRONMENT LOAD EVALUATION

The sabotage threat scenarios to be evaluated may be of two types, TT-1 or TT-2. The scenarios are described in sufficient detail such that the extreme environment associated with each can be specified.

The focus here is on the engineering safety aspects of the threat scenarios and the associated extreme environment. The list of potential threats encompasses internally and externally initiated events, and combinations of the two. In addition, multimode threats, as described herein, are identified and evaluated. It is expected that some of the threat scenarios will involve intruder attacks, either alone or as part of a multimode attack.

The objective of the extreme environment load evaluation is to provide the plant engineering organization with a matrix of environmental conditions produced by the threat scenarios, which can be applied to portions of or the entire facility. The result is an environment load table that specifies the environmental loads and load combinations to be considered by the plant engineering staff in evaluating the SSCs necessary for successful plant performance. Given this information, the plant engineering organization can

determine the facility's capability of resisting the threat. The environment load evaluation serves as the interface between the threat scenarios and the evaluation process; it includes only the engineering aspects, and not the details of the threat scenarios.

In the evaluation process, the inherent strengths of facilities due to the design and construction conditions should be recognized. In this process, the focus is on the SSCs required to safely shut down the facility and maintain it in a safe shutdown condition throughout the period required for recovery actions and for additional entities outside the plant to assist, if necessary. Structures, systems and components are designed and evaluated for a large number of environmental conditions:

— Structures generally provide one or more of the functions of pressure retention, shielding and confinement, and support to systems and components. Structures and structural elements are designed for the operating and accident conditions expected throughout the life of the facility. Operating loads include dead load, live load, atmospheric temperature, thermal loads, vibration, radiation effects, pressure retention and ageing effects (radiation, corrosion and other effects of material degradation). Structures are designed for accidental loads such as missile impact (internally or externally generated), extreme winds, flooding, earthquakes, explosions/blasts (internally or externally generated), extreme heat loads, extreme radiation effects, impulse loads due to pipe whip and other phenomena, and heavy load drops. Some of these loading conditions are considered in the design to act simultaneously.
— Systems are, in general, designed for a companion set of operating and accident conditions for structures. System design also includes considerations of redundancy of function and separation, segregation and diversity of trains and elements to provide high reliability for successful system performance under both normal operating and accident conditions.
— Components are generally designed for a companion set of operating and accident conditions for structures and systems. However, the environments for which components are designed, qualified and maintained are typically more extensive than those for structures and systems. Normal operating conditions comprise a wide range of specified conditions (e.g. temperature, humidity, radiation, cooling, vibration) under which components must function (e.g. pumps delivering fluid at a specified flow rate).

Therefore, the extreme environmental conditions specified in this task need to be evaluated in the light of the normal operating and accident

conditions of the design. It is important to clearly understand the design requirements of the SSCs — for example, to remain fully operable during an event, to be capable of being restored to operation within a specified time or to maintain structural integrity even if other SSC functions cannot be restored. Structures, systems and components have a significant inherent capacity to resist the extreme environmental conditions associated with threat scenarios.

The process of defining the engineering aspects of the threat scenarios to be evaluated is illustrated in the following series of tables. In Table 1 the threat scenarios are associated with extreme environments. For each threat scenario identified in Sections 3.2 and 3.3, the extreme environment potentially imposed on the facility is identified. The example used is purely hypothetical, and the extent of the phenomena and the parameters defined are not intended to be complete or necessarily accurate.

The columns of Table 1 are as follows:

— Threat scenario No. is a numerical identifier with values ranging between 1 and the total number of threat scenarios considered.
Example: Threat scenario No. 1 is assumed.
— Threat scenario description is a brief description of the threat scenario for identification purposes.
Example: The scenario involves the impact of a fully fuelled Boeing 767 flown into the nuclear power plant site.
— Physical loading conditions are numerical identifiers of the type and specifics of loading conditions imposed by the threat scenario. The identifiers correlate directly with Table 2 for impact, Table 3 for explosion/blast, Table 4 for heat/fire, Table 5 for hazardous material release and Table 6 for other environmental consequences. Table 6 provides guidance on the engineering disciplines required in the evaluation and background on why certain environmental load combinations need to be considered.
  - Impact refers to impact loading condition(s) identified by number and reference to Table 2.
    Example: Impact loading conditions 1 and 2 are assumed.
  - Explosion/blast refers to explosion/blast loading condition(s) identified by number and reference to Table 3.
    Example: No blast or explosion loads are associated with threat scenario No. 1 or considered to be ancillary effects of the aircraft impact.
  - Heat/fire refers to heat/fire loading condition(s) identified by number and reference to Table 4.
    Example: Heat/fire environmental loading condition 1 is assumed.

TABLE 1. EXAMPLE OF AN EXTREME ENVIRONMENT LOAD MATRIX

Threat scenario No.	Threat scenario description	Physical loading condition						
		Impact (Table 2)	Explosion/ blast (Table 3)	Heat/fire (Table 4)	Hazardous material release (Table 5)	Smothering (Table 6)	Flooding (Table 6)	Other (Table 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							

- Hazardous material release refers to hazardous material release condition(s) identified by number and reference to Table 5.
  Example: No hazardous material release condition is associated with threat scenario No. 1.
- Smothering, flooding and other phenomena are identified in Table 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.

Table 2 identifies the impact parameters to be used by plant engineering for the evaluation of SSCs. The threat scenario example from Table 1 is continued here for illustrative purposes only.

TABLE 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 fuelled	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									

The columns of Table 2 are as follows:

— Missile type/No. is the missile load identifier with values ranging between 1 and the total number of missile impact scenarios considered.
Example: Missile No. 1 is a fully fuelled Boeing 767 fuselage; missile No. 2, the engines of a Boeing 767.
— Description briefly describes the source of the loading condition.
Example: Missile No. 1 is the impact of a fully fuelled Boeing 767; missile No. 2 is the impact of the engines of the Boeing 767.
— Mass/weight refers to the mass/weight of the missile.
Example: Missile No. 1 is 200 000 kg, including fuel; missile No. 2 is 3500 kg per engine.
— Shape/configuration provides a more specific description of the missile, with dimensions specified if available.
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.
— 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.
Example: The impact angle range is from 0 to 30° from the horizontal.
— Impact velocity is the velocity of the missile, taking into account the physics and human capability necessary to achieve the objective.
Example: The impact velocity is 180 m/s.

— Relative hardness is an important parameter for assessing the effect of the missile on SSCs; it can be a qualitative or quantitative measure.
Example: The missile No. 1 fuselage is considered to be flexible; missile No. 2 is rigid.
— 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.
  - The missile impact causes a fire either by carrying a combustible or by impacting a combustible, such as a diesel oil tank.
  Example: Missile No. 1 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.
  - 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.
  Example: No explosions are assumed.
  - Other hazards can include, for example, intruders working in coordination with the missile attack.
  Example: No other hazards are identified.

Table 3 identifies a simplified set of parameters for explosion/blast loading conditions to be used by plant engineering for the evaluation of SSC capacity. In the example used here, no explosion/blast conditions were assumed. The columns in Table 3 are as follows:

— Explosion No. is the explosion/blast condition identifier with values ranging between 1 and the total number of blast conditions considered.
— Parameters in Table 3 are examples of descriptors of the explosives' characteristics. For general descriptions, TNT equivalent and reference

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

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

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 4 identifies the heat and fire characteristics to be used by plant engineering for the evaluation of the SSCs. The columns in Table 4 are as follows:

— Fire No. is the heat/fire condition identifier with values ranging between 1 and the total number of fire conditions considered.
Example: Heat/fire condition No. 1 is assumed.
— Description briefly describes the source of the fire.
Example: The source in the example is a Boeing 767 jet fuel fire.
— 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 threat scenario, the distribution of the combustibles within and outside the facility boundary is important. Two obvious distributions are the plant 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.
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 h maximum, with 5–7 h of residual fire at 300°C.
— 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.
Example: No internal fire sources are assumed.

Table 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.

The columns in Table 5 are as follows:

— Case No. is the hazardous material release number with values ranging between 1 and the total number of hazardous material release conditions considered.

TABLE 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 from Boeing 767	Yes	50 000 kg	1 000°C	1–8 h						
2											
3											

TABLE 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								

— Material description briefly describes the hazardous material.
— Quantity refers to the amount of the material released and the time frame over which the release occurs.
— Smothering effect — personnel provides an itemization of the physical effects on personnel (e.g. plant operating staff, security forces), including an indication of whether protective gear is required and the time frame of implementation.
— 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.
— Lethal or disabling effect — personnel identifies the potential effects on plant personnel.
— Duration is the time frame during which the hazardous material is present, with an indication of whether or not dispersion occurs.
— 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 plant yard.

Table 6 and the supporting data serve as the interface between the threat scenario definition and the evaluation requirements for the engineering safety experts. It contains the loading environment identifiers and the environmental load combinations to be considered. The table shown here is simplified for illustrative purposes. For each item in the SSEL, there is a set of loading conditions and load combinations to be considered.

3.5. OVERVIEW OF DESIGN AND EVALUATION OF PHYSICAL PROTECTION SYSTEMS

The PPS in a nuclear power plant is designed to protect the facility against the DBT. During a DBT event, the engineering safety aspects support the PPS and constitute an additional layer of defence in depth. A very brief description of a PPS is included here for completeness. The effective assessment and implementation of this procedure requires the integrated efforts of the PPS experts and those personnel responsible for engineering and operational safety.

3.5.1. Physical protection systems

Physical protection against sabotage requires a combination of hardware (security devices), procedures (including the organization of guards and the

TABLE 6. EXAMPLE OF AN EXTREME ENVIRONMENT LOAD DEFINITION MATRIX

Plant area	Vital area	Description	Physical loading condition						
			Impact	Explosion/ blast	Heat/fire	Hazardous material release	Smothering	Flooding	Other
Building 1									
2									
3									
Zone 1									
2									
3									
4									
Yard 1									
2									
SSEL item 1									
2									
3									

performance of their duties) and facility design (including layout). The physical protection measures are designed taking the nuclear facility's characteristics, the nuclear material, the State's DBT and the potential radiological consequences into account.

An effective PPS (see Box 6b in Fig. 1) performs the primary functions of:

(a) Deterrence;
(b) Detection and assessment;
(c) Delay;
(d) Response.

3.5.2. Vital area identification

A vital area is an "area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences" [1]. Box 6a in Fig. 1 shows the context for identifying the vital areas within a facility. By evaluating the consequences of malicious acts, safety experts, in close cooperation with security experts, identify potential sabotage targets within nuclear facilities that require protection to prevent unacceptable radiological consequences in the case of an attack [1]. The minimum complement of equipment, systems and devices may include all designated safety systems if required by the overall safety philosophy. Alternatively, the minimum set may be a subset of all equipment, systems and devices, again dependent on the criteria established by the State or its designee. The VAI process is complex, and many different methodologies may be used. The number and extent of the vital areas are facility specific.

As mentioned above, the VAI process involves target identification, which is the basis of PPS design. Target identification focuses on *what* to protect, while a PPS design addresses *how* to protect identified targets. Target identification does not consider whether the physical protection measures can be overcome or the difficulty of providing physical protection. In other words, target identification identifies areas, components or functions to be protected; the threat to these items and the ease or difficulty of protecting them against a threat is considered after the items have been identified.

The process of identifying a safe shutdown path may be integrated with the VAI process. If the overall safety philosophy for which the vital areas are identified is compatible with the overall safety philosophy for TT-2 events, then one-to-one correspondence between vital areas and SSEL equipment may exist. In this case, the close relationship between SSEL items and vital areas will be maintained. It is more likely, however, that the overall safety philosophy

for VAI and PPS design will differ from that for TT-2 events. In this case, a subset of vital areas containing SSEL items will be identified.

As with all sabotage related information, outcomes of the VAI process are sensitive and should be protected according to strict confidentiality rules.

3.6. FACILITY ASSESSMENT FOR TT-1 AND TT-2 EVENTS

3.6.1. Background

This procedure focuses on evaluating the engineering safety aspects of protection against TT-1 and TT-2 events. For TT-1 events, the effects on SSCs of bombs and other explosives transported and detonated by intruders are considered. In this case, it may be postulated that the PPS was not effective and that the engineering safety measures served as an additional layer of defence in depth. Although the following is equally valid for both TT-1 and TT-2 events, for purposes of illustration, the focus is on the latter.

The evaluation procedure may be viewed in terms of three alternatives:

(1) The first alternative is to demonstrate that the TT-2 extreme environmental conditions are encompassed within the design basis loading conditions. This approach may be applied to portions of the nuclear power plant's safety systems or to the entire plant. Further screening methods should be applied to exclude threat scenarios (see Section 3.3 for a discussion of screening by distance and magnitude or by probabilistic techniques). At this stage of the procedure, it may be possible to exclude threat scenarios by inspection if it is determined that the consequences of the scenario will not cause core damage. In addition, it may be possible to apply probabilistic screening techniques using PSAs of internal and external events performed for the facility in question. In the probabilistic screening approach, event trees are constructed for the threat scenarios of interest. At the base of each event tree is an initiating event corresponding to the threat scenario. Calculations of the conditional probability of the end states — such as conditional core damage probability (CCDP) or conditional large early release probability (CLERP) — should be made, with each end state being conditional on the occurrence of the threat scenario. If the CCDP or CLERP meets a conservative acceptance criterion, then the threat scenario may be excluded from further consideration. The likelihood of the threat scenario's occurrence does not enter into the evaluation, since even if the

probability is equal to one, the likelihood of core damage or containment failure is below the accepted threshold.

(2) The second alternative is to consult the results of PSAs of internal and/or external events, which may provide further insight into the degree of vulnerability of the nuclear power plant:

(i) Sensitivity studies performed on the system event trees/fault trees may identify vulnerability conditions of significant interest, including very vulnerable states and vulnerable states. A very vulnerable state is one where the qualitative results of the PSA show that there exists at least one minimal cut set comprising events expected to occur under the assumed threat scenario conditions that will lead to severe consequences such as core damage. A vulnerable state is one where the quantitative results of the PSA, based on sensitivity evaluations for combinations of assumed unavailable systems, show significant increases in the probabilities of accidents such as core damage. Both of these hypothetical cases serve to focus the evaluation on vulnerable plant operational states and conditions.

(ii) Existing PSAs of internal and external events, when modified to account for additional basic events and failure modes resulting from the threat scenarios, may provide significant insight into the robustness of the nuclear power plant due to redundancy, diversity and spatial separation of SSCs. This qualitative or quantitative assessment may provide confidence that, owing to the large number of simultaneous failures required to cause plant failure, specific threat scenarios may be eliminated.

(3) The third alternative is to perform a safety margin assessment to verify that the nuclear power plant is able to resist the threat scenarios and be safely shut down and maintained in a safe shutdown condition. This deterministic approach, referred to here as a sabotage margin assessment (SMA), is the subject of the remainder of this publication.

When evaluating the cost–benefit ratio of proposed physical and operational changes, the nuclear power plant's operational life should be considered in terms of (a) the effect of operations to date on the material condition of SSCs (ageing effects) and (b) the expected future life of the facility.

For non-reactor facilities (or for parts of facilities such as spent fuel pools), the parameter of interest is CLERP. Instead of safe shutdown, criteria such as maintenance of coolant circulation and fuel integrity could be used.

3.6.2. Sabotage margin assessment procedure

Generally, the SMA approach to evaluating the capacity of engineering safety features to resist TT-2 events comprises the following steps. The assumptions used in these steps may be different depending on whether or not the TT-2 event is included in the DBT or is beyond the DBT.

(a) Introduce into the evaluation process the extreme environment definition matrices (Table 6 and supporting data), which contain the definition of loading environments and load combinations for engineering evaluations. These extreme environments may include impact, explosion/blast, heat/fire, vibration, hazardous material release, flooding and other site specific conditions.

(b) Define the overall performance criteria for the nuclear power plant subjected to the extreme loading environments. For example, for a nuclear reactor subjected to a TT-2 event, the overall performance criteria may be defined as hot or cold shutdown for 24 h after the threat scenario is initiated. A further assumption is that additional aid from outside the plant boundary can be effectively mobilized within 24 h. In all cases, the Member State determines the performance criteria, including the duration of shutdown before additional aid from outside the plant boundaries can be mobilized.

(c) Define the assumptions that will be used in the engineering evaluation. Examples of assumptions for a nuclear power plant are:
   (i) Loss of off-site power;
   (ii) Operational state of the plant (e.g. full power, shutdown/refuelling);
   (iii) System criteria (e.g. redundancy of the safe shutdown path(s)).

(d) Define SSC capacity criteria.

(e) Define one or more safe shutdown or success paths.

(f) Verify that each candidate vital area set identified in the VAI process 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.

(g) Identify the SSCs that make up the safe shutdown path(s) and are required to function during and after the threat scenario event, given the aforementioned assumptions. Define the specific functions that these SSCs must perform during and after the event. Note that some threat scenarios may have such large affected areas or footprints that a simple screening of the overall plant site for likelihood of significant damage within the footprints may limit the number of SSCs to be evaluated.

Those SSCs within the footprint of the threat scenario may be reasonably assumed to fail, and their further detailed consideration is unwarranted.

(h) Evaluate SSC capacity when subjected to the extreme environmental loading conditions specified.

(i) Define a measure of plant capacity, such as the high confidence of low probability of failure (HCLPF) when subjected to the identified threat scenarios. Compare the plant HCLPF with the acceptance criteria.

3.6.3. Identification of the success path(s)

The basic aim of the SMA is to define one or more success paths that can be demonstrated to have adequate margins to perform the required function when subjected to the threat scenarios. SSCs on the success paths have the capacity to withstand the demand environments as designed or with modifications, and are specifically protected from adversaries. In general, several possible success paths may exist. The SMA approach is to select the success paths for which it is easiest to demonstrate adequate margins or capacity when subjected to extreme loads. In addition, the success paths should take into consideration plant operator training and established procedures, while recognizing that, for some threat scenarios, the damage to the plant may be so extensive that existing plant training and procedures may not be applicable or adequate. It is important that the selection of success paths take the requirements for the PPS into account. Consideration may be given to existing definitions of vital areas; alternatively, the vital areas could be redefined to encompass the SSCs of the success path. In either case, the number and location of vital areas should be efficient for protection purposes.

The success paths that are chosen will depend on how 'success' is defined. Depending on the performance criteria, 'success' may refer only to safe shutdown and removal of residual heat; this is commonly called the 'safe shutdown path'. The performance criteria define both what is meant by success (safe shutdown alone or with additional requirements) and the number of success paths required.

A tiered approach can be used for defining the success paths and the acceptance criteria for SSC performance. For example, a first tier would apply to threat scenarios that are not catastrophic, where evaluation criteria may be similar to design basis considerations — that is, full system redundancy (adherence to single failure criteria and redundant paths) and SSC performance behaviour limits at design levels. Two examples of such a threat are the impact of a light aircraft on-site and a vehicle bomb explosion at some distance from the plant. In these cases, it is feasible to restart the facility after

inspections have been performed. The DBT may or may not cover such events, depending on national practices.

A second tier would apply to events where only a single safe shutdown path (i.e. means to control the reactor, cool the fuel and contain the release of radioactive material) would need to be demonstrated; examples from this category include impacts by commercial and business aircraft. In such cases, structure and system acceptance criteria may be significantly relaxed, taking into account the ultimate capacity of the components.

A third tier would apply to very large events that could be catastrophic — for example, the impact of a large aircraft or of multiple missiles on-site. In these cases, response would include on- and off-site emergency measures. In all such cases, reactor shutdown must be ensured, although significant degradation of the engineered means to cool the nuclear fuel and contain the release of radioactive material may be permitted. In these cases, there is no expectation of restarting the facility.

Each of these cases leads to a different safe shutdown path or paths. For a less severe event, the safe shutdown path may encompass all or a portion of the safe shutdown path for a catastrophic event. Each safe shutdown path or success path comprises a subset of plant systems, including safety systems, support systems, containment and other structures, and 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. A success path is a minimum set of systems and operator actions, and typically does not comprise all safety systems. Success paths should be compatible with plant operations.

As mentioned in Section 3.6.2, acceptance criteria for systems and SSCs must be determined by the responsible organizations. For the purposes of this publication, the number of safe shutdown paths is immaterial. The discussion focuses on the SSEL, which is assembled from the systems performance criteria (see Section 3.6.4).

For a nuclear power plant, the SSCs that constitute the safe shutdown path should perform four functions when subjected to the threat scenario(s) under consideration, namely:

(a) Reactor reactivity control;
(b) Reactor coolant pressure control;
(c) Reactor coolant inventory control;
(d) Decay heat removal.

If, in the course of the assessment, the successful performance of one or more of these functions cannot be demonstrated, means for restoring and

maintaining containment integrity and reducing radiological release should be considered.

Documentation of the safe shutdown path(s) generally includes a list of systems (front line and support) 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.

The safe shutdown path identification process results in:

(a) The identification of safe shutdown path(s) and the justification for their selection;
(b) A list of the front line and support systems that make up the safe shutdown path(s) and their characteristics;
(c) Dependency tables listing the direct dependencies between front line systems and support systems, and dependencies between support systems.

3.6.4. Safe shutdown equipment list

The SSCs on the safe shutdown paths are identified and listed in the SSEL. The SSEL database should include the SSC name, component type, manufacturer, design conditions, function, physical location within a vital area, newly defined or expanded threat demand environment and physical loading conditions (direct or indirect impact effects; direct or indirect blast effects; heat and fire loading; vibration; effects of smothering on operability, including smoke effects from fire; and flooding from an internal or external source). This database summarizes the evaluation of each item in the SSEL for the demand environments under consideration. The extreme environment loads given in Table 6 and its supporting data are identified for each of the items in the SSEL. It is expected that the SSEL for a commercial nuclear power plant will contain a few hundred SSCs; other facility types may have significantly fewer items in their SSELs.

Table 8 in Appendix II illustrates an acceptable format for the database. The composite SSEL presented in the table provides guidance, direction, the road map for the evaluation of the SSCs in the SSEL and initial documentation for the team review. The SSC capacity evaluation is performed both in the office, generally using analytical techniques and data, and in the plant during the plant walkdown (see Appendix II for a detailed description of a plant walkdown).

3.6.5. Safe shutdown equipment list and vital areas

The equipment and structures listed in the SSEL are those items that must function in order to safely shut down the nuclear power plant and maintain it in a safe shutdown condition. Therefore, these items should be located in vital areas, that is, areas within the facility that are protected by the PPS. If the evaluation is being performed at an operating plant with a functional PPS, it is expected that the majority of the SSEL items will be located in previously identified vital areas. However, one result of the safe shutdown path identification process is the revisiting of vital area designations. If events beyond the DBT are considered in the assessment, some areas not previously designated as vital (i.e. not protected under DBT assumptions) may need to be added; similarly, some areas previously designated as vital may no longer need to be defined as such.

3.6.6. Capacity evaluation of structures, systems and components

Once the safe shutdown paths have been determined, the required SSCs are converted into the SSEL for evaluation. For each structure and component in the SSEL, the functional requirements for achieving system performance success are specified. The loading or demand environments for the SSEL components associated with the threat scenarios are described by Table 6 and the supporting data. These loadings or demands are physical, such as impact forces, heat, humidity, blast pressures, vibration and smothering gases. The failure modes to be identified, evaluated and verified relate directly to these loadings. 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.

In evaluating capacity, considerable flexibility may be necessary. Engineering judgement based on experience is combined with experimental data and analysis to obtain the capacities of SSCs along a given success path. For items in the ‘disposition 1’ category (see Section II.5.2 in Appendix II), available data may need to be supplemented with experimental data. Careful documentation is required to ensure that all items and operator actions on the success path have been thoroughly evaluated and meet the environmental conditions of the threat scenario under consideration.

Capacity evaluations may also be performed to determine the HCLPF of components in the SSEL when subjected to the threat scenario. For a given success path, the HCLPF of the success path is assumed to be the lowest HCLPF component on the path. This is a conservative estimate of the plant HCLPF that is adequate for evaluation purposes. The probabilistic definition

of the HCLPF is 95% confidence of less than about a 5% probability of failure. The development of HCLPF values to represent the capacity of SSEL items is well documented and used extensively when evaluating nuclear power plants for seismic events beyond the design basis [2].

HCLPF values can be estimated using either probabilistic or deterministic techniques. For the probabilistic approach, the extreme environmental demand is conditional on the occurrence of the threat scenario. The demand can be generated from analysis or experimental data. For example, for a jet fuel fire, the environmental demand is a distribution in time and space of heat loads over the affected plant area. These distributions include uncertainty estimates — either separate aleatoric and epistemic uncertainties or a composite uncertainty. In the fully probabilistic approach, fragility functions are likewise developed and described probabilistically. Hence, for the jet fuel fire example, the failure of structures, or of specific structural elements, can be related to the heat load imposed and its duration. These fragility functions include uncertainty estimates. For PSA methods, the fragility functions (probabilistically described) are developed for all basic events in the event trees/fault trees. For the probabilistic approach, HCLPF values and the extreme environmental demand functions are combined probabilistically with the fragility functions, and the HCLPF value is conditional on the occurrence of the threat scenario.

A second, more common, approach is to estimate HCLPF values deterministically. Deterministic estimates of the environmental loading conditions, which are conditional on the occurrence of the threat scenario, are calculated targeting a specific non-exceedance probability, such as 84% or approximately the median plus one standard deviation. Deterministic estimates of fragility values are established, again targeting a specific non-exceedance probability. These two scalar values are then compared. If the environmental demand does not exceed the fragility value, then the HCLPF value is at least as high as the environmental demand, or at least as high as the threat scenario parameters. For the jet fuel fire example, if the heat load is less than the failure estimate due to heat loads for the SSEL item being considered, then the SSEL item has a HCLPF at least as high as the threat scenario parameters (e.g. for the impact of a Boeing 767 on the plant site for the parameters defined in Tables 1 and 4). Performing the assessment for all items in the SSEL allows an estimate to be made of the plant HCLPF for the given threat scenario.

The deterministic approach is preferred because, as is the case with seismic evaluations of SSCs, once the rules are established, engineers without training in probabilistic methods can perform the evaluations. Rules for dealing with the various modes of terrorist attack need to be further developed, which can be easily done using the guiding principles of the beyond design basis evaluations, in particular for beyond design basis earthquakes.

Guidance on the engineering evaluation of various modes of extreme events can be found in numerous IAEA and other publications. In particular, Ref. [3] addresses the hazards of, for example, aircraft impacts, external fires, explosions, hazardous materials and floods. It also provides a list of references on technical evaluation approaches and introduces the concept of HCLPF for explosion risks. Other IAEA publications expand on various hazards, generally of accidental origin, where engineering evaluation methods are applicable.

The steps in the SSC capacity evaluation include:

(a) Plant familiarization, many aspects of which are accomplished during the determination of safe shutdown path(s), the generation of the SSEL and the determination of the loading environment of SSEL components. Additional familiarization with plant specific documents for the SSCs of interest is performed during this step.
(b) In-office and in-plant evaluations of items in the SSEL. In-plant evaluations refer to the walkdowns discussed in Section 3.6.8 and in Appendix II. In-office evaluations refer to the assembling of design and qualification data for the specific items in the SSEL. Calculations should be made as necessary to determine the loading environment and the failure or capacity of the items.
(c) Confirmation of assumptions made in all phases of the evaluation during the plant walkdown.
(d) Documentation.
(e) Generation of the SSEL, with HCLPF estimates for all environmental loading conditions considered in the evaluation.

3.6.7. Composition of the sabotage margin assessment team

The SMA team comprises:

(a) Plant experts knowledgeable about plant systems, security, operations and engineering, who are responsible for converting the threat scenarios (the TT-2 events) into specific extreme loading conditions in different areas of the plant (see Sections 3.3 and 3.4). This activity should be treated as strictly confidential, with the extreme loading conditions produced being passed on to relevant experts for evaluation.
(b) Experts in security (PPSs) supplemented with experts in plant operations and on-site emergency management. This aspect of the assessment team is not discussed here, although it is briefly described in Appendix II.
(c) Experts in engineering safety assessment, system design, engineering (civil, structural, fire, electrical, mechanical, instrumentation and control)

and plant operations. This aspect of the assessment team is the focus of this publication, and the related activities ultimately screen out certain SSCs with regard to the relevant extreme loading conditions and identify those for which more detailed analysis is required.

Other experts in areas such as missiles, aircraft or demolition are helpful in the evaluations.

Procedures need to be in place to minimize the disclosure of confidential information, especially to the experts responsible for evaluating SSC capacity when subjected to specific environmental loading conditions. One goal is to keep threat information separate from plant condition information, particularly when informing the relevant experts — who do not need to know threat specifics — of environmental loading conditions. This is accommodated by the SMA approach.

3.6.8. Plant walkdown

Appendix II describes a plant walkdown in detail. The main objectives of a plant walkdown are 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 SSEL, 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, and to document the results of the walkdown (see Section II.2).

4. DECISION METHODOLOGY

Section 3 presents a method for evaluating the capacity of the engineering aspects of nuclear power plants to withstand malicious attacks. More specifically, the methodology described provides decision makers with a list of critical SSCs on the success path(s) that must be protected and that have quantified capacities with regard to threat scenarios included in or beyond the DBT. These scenarios can be either TT-1 or TT-2 events.

The disposition status of identified vulnerabilities or items with unacceptably low capacities should be addressed by identifying as many approaches to the successful mitigation of adverse consequences as is practical. The assessment and resolution of issues should take defence in depth into

account and consider all available options with respect to safety and security on-site; available off-site resources should also be identified, such as those for emergency preparedness and firefighting (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 threats). In addition, all other government security programmes should be considered in deciding upon the appropriate actions.

The decision making process is shown in Fig. 1 and described in detail in Appendix I. It identifies crisis management as a task in the evaluation process; this includes accident mitigation, with containment performance and other mitigation measures.

There are four major decision points in the road map for achieving acceptable overall risk in relation to malicious acts (for details see Appendix I, which also contextualizes upgrading decisions). For identified vulnerabilities, plant management has a number of options, such as enhancing the PPS, upgrading the plant's crisis management capabilities, providing for an improved layout and introducing engineered changes to SSCs.

A list of factors that must be taken into consideration in the decision making process is presented in Table 7.

It may be necessary to discuss with State authorities how to respond to certain threat scenarios for which protection based on plant resources (e.g. engineering upgrades and enhancements of physical protection) is problematic. The State authorities may decide to implement additional off-site prevention or response measures.

5. CONCLUDING REMARKS

The guidelines in this publication are based on the premise that the design, layout and safety infrastructure built into existing nuclear facilities may be of considerable benefit in mitigating the effects of malicious acts. However, this benefit may not apply uniformly to all threats and all required safety functions.

The evaluation process described in these guidelines, together with the proposed model for the interaction of specialists in the operation of nuclear facilities, nuclear safety engineering and physical protection, provides plant management and other stakeholders with the robustness and vulnerability

TABLE 7. DECISION DRIVERS

Decision step	Evaluation result
Severity of assessed vulnerabilities	Sabotage is successful and the mitigation systems, if any exist, do not provide the desired level of protection from radiological release. Sabotage is unsuccessful, but the remaining safety margins are unacceptably small or uncertain. Security system disrupts but does not prevent the act of sabotage.
Plant options	Physical protection upgrade: actions and improvements aimed at preventing challenges to items in the vital areas (or on the success path). Safety system upgrade: includes redundancy, diversity and separation measures. Structural strengthening: efforts targeting the survival of a given item in the event of extreme loads due to a malicious act. Operator action: If there is some warning time before the malicious act or the sabotage event, reactor shutdown or other actions may be appropriate; if there is no warning time, operator action during or after the attack may be essential in diagnosing the event and responding, if this is not done automatically.
Optimization	Decisions to allocate the resources required for upgrades and changes are based on estimated improvements in the capacity to either prevent the act of sabotage or eliminate its ability to initiate a release of radioactive substances. Specifically, decisions are based on: (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.
Use of available severe accident management capabilities	Facilities may have mitigating features (e.g. accident management procedures) originally intended to minimize accident consequences that go beyond the applicable design basis and thus have the potential to mitigate the radiological consequences of successful sabotage. These may need to be enhanced to more fully address 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. These capabilities need to be complemented with other intervention measures (e.g. response force, firefighting team).
Off-site features and capabilities	Use of physical barriers, exclusion zones and surveillance of access roads to the nuclear installation by police may reduce the potential for and severity of attacks (e.g. reference distance for vehicle bombs).

information needed to make decisions concerning upgrades or implementing other means to reduce the risk to the public.

These guidelines have been designed to benefit a wide range of international regulatory regimes in managing the risks at their nuclear facilities and countering potential threats to nuclear installations given the new realities of acts of sabotage in the twenty-first century.

Appendix I

PHYSICAL PROTECTION FLOW CHART DESCRIPTION

Figure 1 in Section 2 of this publication presents a flow chart showing how all of the entities involved work together to protect a nuclear power plant in the event of a malicious attack. This appendix provides detailed descriptions of the boxes and decision points in Fig. 1.

Box 1

The threat assessment is defined here as an analysis that documents the credible motivations, intentions and capabilities of potential adversaries that could cause undesirable consequences involving nuclear facilities or nuclear material during its use, storage or transport. The result of the threat assessment process describes the credible threats.

Box 2

Consequences are defined here as the potential level of impact on the interests of the public, the State, key interest groups and the international community. Consequences can be defined in relation to the level of a potential release of radioactive substances and potential exposure to radiation. Concern about these consequences will influence the decision making process in the development of a DBT.

Diamond 3

For a given threat environment and potential consequences of the failure of the nuclear power plant, different types of threat scenario need to be considered. Depending on the Member State's practice, these may be within the DBT or they may be considered to be beyond the DBT. In terms of the way these threats affect the nuclear power plant, they may be classified as TT-1 or TT-2. Threat type 1 events involve the intrusion of adversaries into the protected area, whereas TT-2 events involve standoff attacks. At this point, it must be decided which threat scenarios should be included in the list of potential threats and to which category (TT-1 or TT-2) each belongs.

Box 4

Threat type 2 (TT-2) describes standoff threat scenarios.

Box 5

Threat type 1 (TT-1) describes threat scenarios involving adversaries who intrude, or intend to intrude, into the protected area.

Box 6

Physical protection against sabotage requires a combination of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout). Here, facility design refers to aspects of the plant configuration that facilitate the process of detection, delay, response, recovery and/or robustness of the SSCs to extreme loads, as well as design measures to cope with severe accidents.

Box 6a

A vital area lies "inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences" [1]. In designating such areas, consideration should be given to the plant safety design, the location of the plant and the DBT. The methods used for VAI depend on the complexity of the facility, available safety documentation (SAR, PSA, etc.) and plant walkdowns organized for this purpose.

Box 6b

The PPS should be designed to detect and delay a malicious act included in the DBT and to respond to it appropriately. These primary functions are typically provided by physical protection measures such as detection and access control systems, barriers and response forces. An analysis of the facility design — including an evaluation of existing safety measures and consideration of the spatial separation and redundancy of systems — provides a basis for the design of appropriate physical protection measures. To design an appropriate response, the immediate on-site actions of the operator related to recovery of disabled systems need to be taken into consideration.

Box 6c

If the DBT includes malicious acts resulting in extreme loads on plant SSCs, a capacity evaluation of these SSCs needs to be carried out. The acceptance

criteria to be used in this evaluation should be determined by the competent authority.

Box 6d

Post-core-damage crisis management involves plant actions to mitigate consequences. Such actions should consider the possibility of continued adversary presence at the site aimed at hindering or disrupting the mitigation activities.

Box 7

An emergency response is required to mitigate off-site radiological consequences of a malicious act that has led, or has the potential to lead, to the loss of control over the nuclear process through the loss of the designated safety systems. It includes all actions performed by State organizations (in cooperation with the operating organization) to cope with the situation, including specific measures to counter malicious acts aimed at disrupting and disabling emergency response.

Box 8

The responsibility for physical protection rests with the State, which in turn should ensure that the prime responsibility for the implementation of physical protection of nuclear material and facilities rests with the holders of the relevant licences. The DBT is used by the competent authority to evaluate physical protection measures and by the operator to plan and design these measures.

Box 9

The response by State authorities or organizations may include the active response to an attack on the facility. Response also includes the actions of emergency organizations in the State.

Box 10

State security includes measures that acknowledge a credible threat as being beyond the DBT. These measures should be considered together with the emergency response capabilities in order to keep the remaining risk at an acceptable level. The spectrum of measures can include intelligence, air traffic security and military defence.

Box 11

An extreme load evaluation is undertaken when a credible threat that is not an element of the DBT becomes an actual subject of concern and the State's PPS cannot be implemented in the short term. A re-evaluation of the facility capacity needs to be carried out using realistic (i.e. less conservative) margins. The evaluation may result in a decision concerning the feasibility of continuing operations. Taking into account events beyond the DBT and the results of the extreme load evaluation, the competent authority may decide to include these events in the physical protection evaluation process (possibly with different and less conservative acceptance criteria) and/or to take on part of the responsibility for protection.

Box 12

The term risk in this context refers to the likelihood that a threat will be able to bring about an undesirable consequence. Risk can be reduced, but it cannot be eliminated. All judgements and decisions imply the acceptance of a degree of risk. There is no database of malicious acts that allows the calculation of risk as a product of the probability of a successful attack (based on statistics) and the ensuing consequences. However, some States have chosen to estimate a conditional risk — that is, the risk of undesirable consequences given that an attack occurs.

Diamond 13

After the list of TT-2 events has been created and some evaluation of these extreme loads has been performed, a decision needs to be made regarding the sharing of responsibilities in protecting the nuclear power plant against specific threat scenarios and the response to such attacks. In particular, the protection measures may be shared between the plant management and local and/or State authorities. The arrow pointing to the left indicates that part of the responsibility that is expected from plant management.

Diamond 14

At this point, a decision needs to be made regarding whether or not the PPS, in combination with the engineered safety systems (the SSCs), is capable of protecting the nuclear power plant against TT-1 events and those parts of TT-2 events for which the plant management has responsibility. If this is the case, then the other layers of defence in depth (in particular crisis management,

which is mainly the responsibility of plant management) need to be considered. Otherwise, the PPS and the SSC capacities should be re-evaluated after upgrades have been implemented.

Diamond 15

At this final decision point, the State must decide whether, with the implementation of all available layers of defence in depth, the risk from the particular threat has been reduced to an acceptable level. In this decision, the roles played by the plant and the State authorities — including security and response agencies — are taken into consideration.

Appendix II

PLANT WALKDOWN

II.1. ASSESSMENT GUIDELINES: OVERVIEW

This publication was developed to assist in capacity evaluations of nuclear facilities subjected to DBT events and events beyond the DBT. The focus of this publication is on engineering safety aspects. Aspects concerning the PPS — specifically, response to intruder threats — are addressed elsewhere. The concept of in-plant evaluations or plant walkdowns is, however, included here.

The assessment process comprises the following steps:

(1) Threat evaluation: Encompassing threat assessment, consequence criteria and the decision process, threat evaluation is a complete identification and evaluation of previously and newly defined threats, which are then categorized for inclusion in the plant evaluation. Engineering safety aspects of the protection against DBTs and threats beyond the DBT are the subject of these guidelines.

(2) Specification of threats beyond the DBT: This task evaluates threats beyond the DBT for applicability to the nuclear facility under assessment, resulting in a list of threat scenarios for evaluation. Additional screening may be performed at this stage of the assessment.

(3) Extreme environment load evaluation: This step serves as the interface between the threat scenarios and the definition of the loading environment for evaluation by the plant engineering organization. The matrix of environmental conditions produced by the threat scenarios can be applied to portions of or the entire facility. The resulting environment load matrix (see Table 6) and its supporting data define the engineering safety loading environments.

(4) Sabotage margin assessment. The methodology presented in this report is called the sabotage margin assessment (SMA) procedure. With appropriate assumptions and acceptance criteria, it is equally applicable to the engineering safety aspects of DBTs and threats beyond the DBT. The SMA is based on:

   (i) Input within the extreme environment definition matrices (Table 6 and supporting data).

   (ii) Overall performance criteria for nuclear facilities subjected to extreme loading environments. For example, for a nuclear reactor subjected to a threat beyond the DBT, the overall performance

criteria may be defined as hot or cold shutdown for 24 h after the threat scenario is initiated. A further assumption is that additional aid from outside the plant boundary can be effectively mobilized within the 24 h period. The Member State determines the performance criteria, including the duration of plant shutdown before aid from outside the plant can be mobilized.

(iii) Assumptions on which the DBT or beyond DBT engineering evaluation will be performed — for example, loss of off-site power, the operational state of the facility (full or partial operation), system criteria (redundancy) and SSC capacity criteria (code or relaxed).

(iv) Definition of one or more safe shutdown or success paths.

(v) Identification of those SSCs that are on the safe shutdown path(s) and that are required to function during and after the threat scenario, given the aforementioned assumptions, and the definition of the specific functions these SSCs must perform during and after the event. The SSCs are itemized in the SSEL (see Table 8 for an acceptable format for the SSEL).

(vi) Evaluation of SSC capacity (items in the SSEL) when subjected to the extreme environmental loading conditions specified. For the SMA, the measure of capacity is the HCLPF when subjected to the identified threat scenarios. This step entails in-office and in-plant evaluations; the latter constitute the plant walkdown, which is the subject of this appendix.

(vii) Definition of a measure of plant capacity, such as the HCLPF when subjected to the identified threat scenarios. The plant HCLPF is compared with the acceptance criteria.

II.2. PLANT WALKDOWN OBJECTIVES

The main objectives of the plant walkdown are to:

(a) Review the screening performed early in the process or in the evaluation phase itself to verify its appropriateness;

(b) Identify new and review proposed easy-fix concepts, confirm their effectiveness and verify that the threat scenarios (or demand environments) to which they apply are likely to be effectively thwarted;

(c) Review identified success paths and the SSCs in the SSEL, confirm the required functions of the SSCs during and after the attack, confirm the demand environments to which the SSCs are subjected for each threat scenario, identify or confirm failure modes of concern as a function of the

threat, and identify robust SSCs that may be excluded from further consideration;

(d) Verify as-built or current conditions with design information, including plant systems, engineering and PPSs;

(e) Group similar SSCs and their demand environments for further analysis after the plant walkdown;

(f) Review vital area definitions and boundaries to evaluate their applicability to the SSEL and to define representative configurations for further evaluation;

(g) Document the results of the walkdown.

II.3. SECURITY SENSITIVE INFORMATION

All related information and documentation containing physical protection information — whether on an individual basis or assembled for the purpose of assessing engineering safety aspects of the physical protection of nuclear facilities — is to be considered security sensitive information and safeguarded appropriately. The walkdown team and support personnel (e.g. administrative support) should consist of trusted experts with appropriate clearances on whom background checks have been completed.

II.4. PLANT WALKDOWN TEAMS

Plant walkdown teams consist of members of the operator's staff, consultants with specific expertise and, potentially, regulators. 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 State authorities, as necessary, to define or clarify the elements of the threat 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 that should 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 plant operations: Plant operations personnel are an essential component of the team, and their expertise should be available throughout the plant walkdown activities.

This publication focuses on engineering safety. Aspects of the DBT and threats beyond the DBT that are the responsibility of PPS personnel may be evaluated independently or in conjunction with the engineering safety aspects. When 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 DBTs or threats beyond the DBT include multimode attacks that encompass combined threats.

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

II.5. PLANT WALKDOWN PROCEDURE

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

II.5.1. Walkdown preparation

(a) Plant familiarization:

(i) General plant documentation should be assembled, including safety analysis reports, system descriptions, piping and instrumentation diagrams (P&IDs), electrical one-line drawings, operating procedures, plant general arrangement drawings, plant mechanical and electrical equipment location drawings, PSAs for internal and external events, and any other beyond design basis assessments;

(ii) Limited PPS information should be assembled, in particular, designated vital areas for the items in the SSEL;
(iii) Plant access requirements should be met, including radiation protection, safety practices and security practices (adherence to the 'as low as reasonably achievable' (ALARA) principle is required).

(b) Plant documents on safe shutdown paths and the SSCs in the SSEL should be consulted or created, and the environmental demand on each item in the SSEL, including physical and security demands, should be defined.

(c) A database of the SSEL should be prepared summarizing the evaluation of each item in the SSEL for the demand environments. It is expected that the SSEL of a commercial nuclear power plant will comprise a few hundred items. Other facility types may have significantly fewer items in their SSELs.

(d) Individual SSC data sheets should be prepared containing some of the above mentioned information. If necessary, the data should be supplemented with field and office generated SSC specific evaluations, including field notes; safety, security and engineering analyses performed; and field modifications.

(e) An in-plant walkdown plan should 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.

Table 8 illustrates a format that can be used for the SSEL database. The columns of Table 8 are as follows:

— SSEL No. is a unique numerical identifier for the SSC that may contain location, system or other information.
— SSC name contains descriptive information on the SSC (e.g. auxiliary building, diesel generator 1A, etc.).
— SSC ID No. is a plant specific identifier.
— Description briefly describes the SSC.
— Threat scenario No. is an identifier that is linked to a master list of threat scenarios to be evaluated.
— Location refers to a series of location identifiers to aid in planning the in-plant walkdown and evaluating the consequences of the threat. It may include VAI for PPS evaluation.
— Physical loading conditions are identifiers of the type of loading conditions to be considered that provide guidance on the experts

TABLE 8. EXAMPLE OF A COMPOSITE SAFE SHUTDOWN EQUIPMENT LIST (SSEL)

SSEL No.	SSC name	SSC ID No.	Description	Threat scenario No.	Location				Physical loading condition				
					Building	Elevation	Room / compartment	Vital area	Impact	Explosion/ blast	Heat/ fire	Smothering	Flooding

required and in-plant walkdown access, and on combined loading conditions to be evaluated (e.g. impact plus fire).

- Impact refers to direct and indirect impact effects to be considered in the evaluation. Direct impact effects are conditions such as direct missile impact; indirect impact effects are conditions such as scabbing of concrete and vibration induced loadings.
- 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.
- Heat/fire refers to heat from a fire or direct flame effects on the SSC.
- 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 should be evaluated.
- Flooding from internal or external sources may need to be evaluated.

Table 9 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 9 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 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.

II.5.2. Preliminary screening walkdown

The preliminary screening walkdown should achieve the following objectives:

(a) Determine the location and accessibility of each SSEL item in the plant;
(b) Identify any other SSCs needed for safe shutdown, which should then be added to the SSEL;

TABLE 9. 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: _____

TABLE 9. EXAMPLE OF A SCREENING EVALUATION WORK SHEET (SEWS) FOR PHYSICAL LOADING CONDITIONS (cont.)

Smothering:

Smoke: _____

Toxic chemicals: _____

Other: _____

Flooding:

Internal: _____

External: _____

Other: _____

_____

Comments:

[Summary notes concerning the evaluation]

Attachments:

Field walkdown notes

Interaction hazard evaluations

- Spatial interactions: falling, proximity, etc.
- Spray/flooding interactions

Photos of SSCs and key evaluation elements

Calculations, supporting material, etc.

Specific component evaluation worksheets when available and appropriate

(c) Review and validate screening of SSCs with respect to capacity considerations;
(d) Identify potential easy-fixes;
(e) Group all the components located within or on larger items of equipment;
(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.

The preliminary screening walkdown visually examines those SSCs that are accessible. There are three alternative disposition categories for each item on the SSEL:

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

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

II.5.3. Detailed screening walkdown

The detailed screening walkdown is to be performed for all SSCs whose capacity for the defined environmental loading scenarios has not been verified. This includes in-plant 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 judgement as to whether or not the component requires further analysis or modification.

(b) For SSCs in the second category, plant modifications are clearly warranted. In these cases, the walkdown engineers suggest that the modifications be implemented.

The detailed screening walkdown should be properly documented. It is advisable to supplement the documentation with photographic and/or video records. Table 8 is an acceptable form of summary documentation for the entire SSEL. The SSC evaluations may be documented using the form given in Table 9, with supporting material attached.

Confidentiality of the documentation should be strictly maintained, with distribution on a need to know basis only.

II.6. SPECIAL TOPICS

Type and number of co-located facilities at the site

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 plant 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. All co-located facilities may require simultaneous physical protection when subjected to events beyond the DBT. The evaluation should take 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.

Interactions

The plant walkdown is a key tool for identifying spatial interactions that could potentially affect the performance of SSEL items subjected to a specific threat and that could render this equipment inoperable. A major concern in these areas is ‘housekeeping’. The identification and assessment of potential interactions requires good judgement from the walkdown team.

Falling

Falling is the structural integrity failure of a non-safety or safety related item that could hit and damage a safety related item. For the interaction to be a

threat to an SSEL item, the impact must contain considerable energy and the target must be vulnerable.

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 should 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

Proximity interactions are defined as conditions where two or more items 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. [4].

Spray and flood

Spray and flood can result from failure of piping, systems or vessels that are not properly supported or anchored. Inadvertent spray hazards to SSEL items 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 threats throughout the plant site, particularly in buildings and compartments, the walkdown should evaluate 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 should be backfitted, usually by adding support to reduce deflections and impact or stress. An alternative is to protect the target — in this case, the SSC.

Large tanks may be potential flood sources. The walkdown team, with the assistance of plant personnel, should assess the potential consequences of a flood source failure and the ability of the floor drainage system to mitigate the consequences of a source failure.

REFERENCES

[1] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev. 4 (corr.), IAEA, Vienna (1999).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Evaluation of Existing Nuclear Power Plants, Safety Reports Series No. 28, IAEA, Vienna (2003).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

DEFINITIONS

The definitions given below apply specifically to terms appearing in this report and many not necessarily conform to definitions adopted elsewhere for international use.

assessment. See 'self-assessment'.

capacity. An 'absolute' measure of the robustness of SSCs subjected to a particular threat that can include physical, operational and administrative attributes. Capacity is defined relative to a specific metric. Code capacity is a measure of a plant design feature relative to the code. Failure capacity is a measure of the robustness of SSCs subjected to a particular threat.

capacity evaluation. The process of establishing the capacity of SSCs, operational procedures, PPSs, etc., when subjected to a particular threat. An example is the establishment of the failure capacity, strength or robustness of structures and components to impact, impulse, explosion, vibration, steam and/or loading conditions. Capacity evaluation may identify vulnerabilities and systems interactions; items under evaluation are usually found to be considerably more robust than the design limits.

design basis threat (DBT). The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated (definition from Ref. [1]).

high confidence of low probability of failure (HCLPF). The probabilistic definition of the HCLPF is 95% confidence of less than about a 5% probability of failure. HCLPF values can be estimated using probabilistic or deterministic techniques. The deterministic approach is preferred because, once rules governing the definition of demand and capacity are established, engineers without training in probabilistic methods can perform the evaluations.

margin. A relative measure of expected performance versus a specified criterion or metric. It can be measured and expressed deterministically or probabilistically. One measure of margin is the relationship between capacity and loading condition. For example, for a structural element, a ratio of blast pressure demand and pressure capacity to failure (D/C) of less than one indicates that there is margin to failure.

safety margin. A measure of the expected performance of the plant as a system when measured against a safety metric and when subjected to a particular threat. Intermediate results include the expected performance of SSCs when subjected to a particular threat and can be defined as the minimum ratio of capacity to demand for SSCs on the success path.

scenario. A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes). Safety analysts use accident scenarios to describe and model plant response to potential accidents. An accident scenario, which usually has an initiating event superimposed on a proposed plant configuration, can be used to model system response, including various operator actions as appropriate.

screening. A type of analysis aimed at eliminating from further consideration factors that are less significant for protection or safety, in order to concentrate on the more significant factors. This is typically achieved by consideration of very pessimistic hypothetical scenarios. Screening is done in various disciplines using a variety of tools:

(a) In threat assessment, screening is used to eliminate certain possible terrorist acts because of, for example, the existence of other State protective strategies, the perceived low capability level of the adversaries, strong protective forces and/or the low probability of the event.
(b) Site and plant screening may exclude certain threat scenarios because of, for example, site location or the inherent robustness of the design.

self-assessment. Referred to simply as ‘assessment’ in this report, self-assessment is the evaluation process performed by the operating organizations, with the assistance of external agencies and consultants as needed, to identify and correct safety and security problems that hinder the achievement of the organization’s safety and security objectives. The end result of self-assessment activities may be risk reduction strategies that include changes and upgrades to the nuclear facility. This is considered to be the first step of a more formal review (e.g. regulatory review) by an external organization.

success path. A minimal set of components for a subset of plant systems — including safety systems, support systems, containment structures and operator actions — whose operability and survivability are sufficient to ensure the safe shutdown of a nuclear power plant, removal of residual heat, containment as required and the necessary continued control actions for the threat scenario under consideration.

threat assessment. The process of analysing systematically the hazards associated with facilities, activities or sources within or beyond the borders of a State in order to identify:

(a) Those events and the associated areas for which protective actions may be required within the State;
(b) The actions that would be effective in mitigating the consequences of such events.

The term threat assessment does not imply that any threat, in the sense of an intention and capability to cause harm, has been made in relation to such facilities, activities or sources.

threat beyond the DBT. A threat identified in the assessment that, while not included in the DBT, remains credible. Threats beyond the DBT need to be taken into account to ensure the physical protection of nuclear facilities.

threat scenario. A scenario whose initiating event is an act of sabotage.

threat type 1 (TT-1). A threat posed to the nuclear facility by insiders or by adversaries intending to intrude into the facility to commit their act (with or without insider assistance). In general, the PPS of the facility is designed to counter this type of threat. The DBT considers many threats of this type.

threat type 2 (TT-2). A threat posed to the nuclear facility initiated outside the plant boundary that does not require the presence of the adversaries on-site. Examples of this type of threat include standoff attacks such as shoulder launched missiles and malicious aircraft impacts. It is normally difficult for the facility's PPS to counter this type of attack, as it is not designed for this purpose. For many, but not all, nuclear facilities, a TT-2 is considered to be beyond the DBT.

vital area. An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences (definition from Ref. [1]). A protected area is an area under surveillance containing category I or II nuclear material and/or vital areas surrounded by a physical barrier

walkdown. Techniques to enable a team of experienced engineers, operators, security and safety personnel, and technicians to quickly understand plant configuration and procedures based on thorough in-plant inspections and the review of existing documents such as design drawings, operating procedures, safety analysis reports and PSA reports (e.g. level 1, level 2, level 3, fire PSA, seismic PSA, shutdown PSA).

CONTRIBUTORS TO DRAFTING AND REVIEW

Asmis, G.J.K.	Consultant, Canada
Beck, D.	Sandia National Laboratories, United States of America
Contri, P.	International Atomic Energy Agency
Ek, D.	Sandia National Laboratories, United States of America
Godoy, A.	International Atomic Energy Agency
Gürpinar, A.	International Atomic Energy Agency
Gutschmidt, W.D.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Hagemann, A.	International Atomic Energy Agency
Jalouneix, J.	Institut de radioprotection et de sûreté nucléaire, France
Johnson, J.J.	Consultant, United States of America
Kim, S.C.	International Atomic Energy Agency
Lambright, J.	Lambright Technical Associates, Inc., United States of America
Kluegel, J.U.	Kernkraftwerk Gösgen-Däniken AG, Switzerland
Kostarev, V.	CKTI-Vibroseism Co., Ltd, Russian Federation
Kovalev, K.	MINATOM, Russian Federation
Krutzik, N.	Consultant, Germany
Kwak, S.M.	Compuserve, Republic of Korea
Lojk, R.	Canadian Nuclear Safety Commission, Canada
Moses, C.	Canadian Nuclear Safety Commission, Canada

Murray, A.	Australian Nuclear Science and Technology Organisation, Australia
Nishida, S.	Japan Nuclear Energy Safety Organization, Japan
Ostropikov, V.	Federal Atomic Energy Agency, Russian Federation
Park, C.K.	Korea Atomic Energy Research Institute, Republic of Korea
Skelton, S.	Office for Civil Nuclear Security, United Kingdom
Tang, W.	Beijing Institute of Nuclear Engineering, China
Tardiff, A.	Nuclear Regulatory Commission, United States of America
Yagi, T.	Nuclear Material Control Center, Japan
Wieland, B.	Consultant, Switzerland

Consultants Meetings

Vienna, Austria: November 2002, September 2003, December 2003, April 2004

Advisory Group Meetings

Vienna, Austria: April 2004, October 2004

Review by the Advisory Group on Nuclear Security (AdSec)

Vienna, Austria: April 2004, October 2004

NUCLEAR FORENSICS SUPPORT
IAEA Nuclear Security Series No. 2 (Technical Guidance)
STI/PUB/1241 (67 pp.; 2006)
ISBN 92-0-100306-4 Price: €26.00

MONITORING FOR RADIOACTIVE MATERIAL IN INTERNATIONAL MAIL TRANSPORTED BY PUBLIC POSTAL OPERATORS
IAEA Nuclear Security Series No. 3 (Technical Guidance)
STI/PUB/1242 (39 pp.; 2006)
ISBN 92-0-100406-0 Price: €23.00

IDENTIFICATION OF RADIOACTIVE DEVICES AND SOURCES
IAEA Nuclear Security Series No. 5 (Technical Guidance)
STI/PUB/1278 (135 pp; 2007)
ISBN 92-0-111406-0 Price: €45.00

SEISMIC EVALUATION OF EXISTING NUCLEAR POWER PLANTS
Safety Reports Series No. 28
STI/PUB/1149 (60 pp.; 2003)
ISBN 92-0-101803-7 Price: €18.00

EXTERNAL EVENTS EXCLUDING EARTHQUAKES IN THE DESIGN OF NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. NS-G-1.5 (Safety Guide)
STI/PUB/1159 (105 pp.; 2003)
ISBN 92-0-113603-X Price: €27.00

PROTECTION AGAINST INTERNAL FIRES AND EXPLOSIONS IN THE DESIGN OF NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. NS-G-1.7 (Safety Guide)
STI/PUB/1186 (63 pp.; 2004)
ISBN 92-0-103304-4 Price: €15.00

The product of extensive dialogue among safety and security specialists, this publication provides guidance for evaluating the engineering safety aspects of the protection of nuclear power plants against sabotage, including standoff attacks. The guidance takes into account the robustness of existing structures, systems and components, and emphasizes those aspects of sabotage protection that work synergistically with the protection against extreme external events such as earthquakes and tornadoes and external accidents. The publication introduces a defence in depth approach to sabotage protection, with layers comprising safety and security related systems and activities, and promotes self-assessment by the licensee in cooperation with the competent authorities.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 92–0–109906–1
ISSN 1816–9317