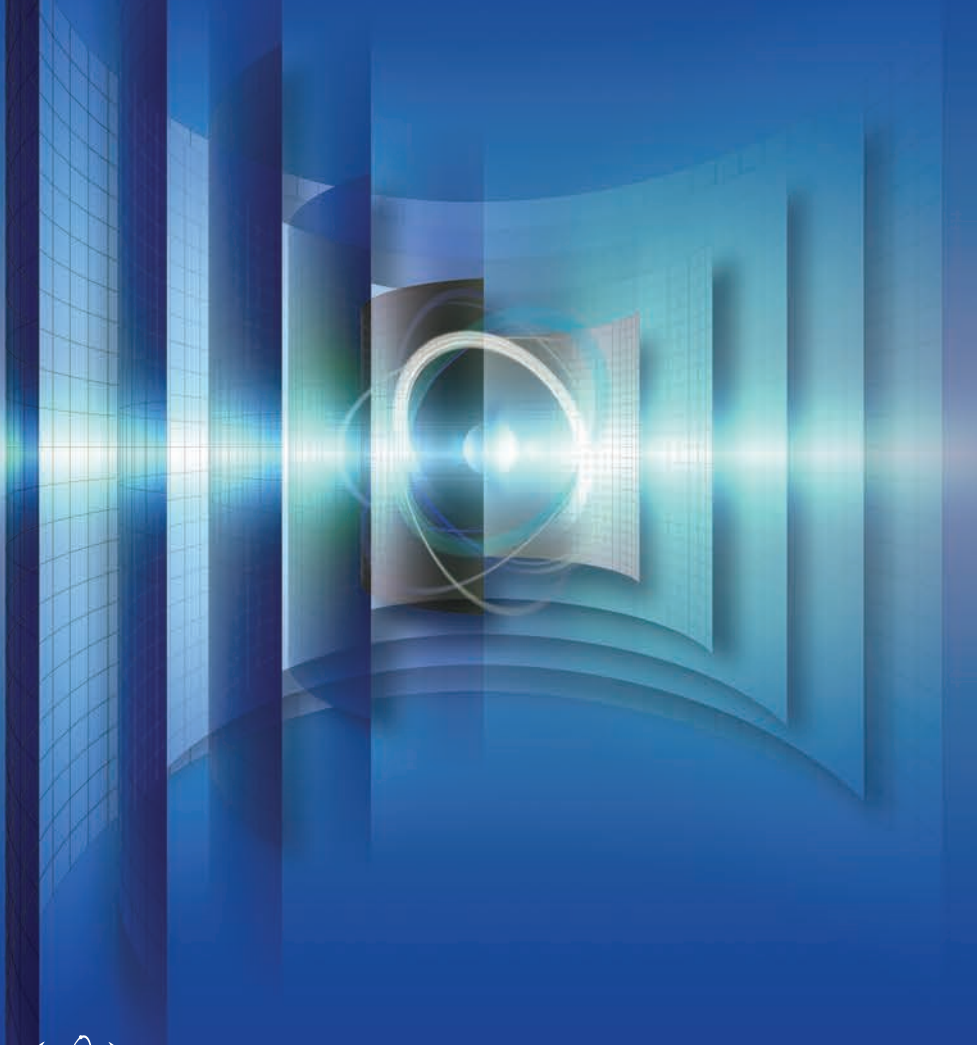
IAEA Nuclear Security Series No. 27-G

Implementing Guide

Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss 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.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

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. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (IMPLEMENTATION OF INFCIRC/225/REVISION 5)

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

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

PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (IMPLEMENTATION OF INFCIRC/225/REVISION 5)

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2018

COPYRIGHT NOTICE

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

Printed by the IAEA in Austria
April 2018
STI/PUB/1760

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Physical protection of nuclear material and nuclear facilities (implementation of INFCIRC/225/Revision 5) / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2018. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 27-G| Includes bibliographical references.
Identifiers: IAEAL 18-01138 | ISBN 978–92–0–111516–4 (paperback : alk. paper)
Subjects: LCSH: Nuclear facilities — Security measures. | Radioactive substances — Law and legislation. | Radioactive substances — Safety regulations.
Classification: UDC 341.67 | STI/PUB/1760

FOREWORD

by Yukiya Amano
Director General

The IAEA's principal objective under its Statute is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." Our work involves both preventing the spread of nuclear weapons and ensuring that nuclear technology is made available for peaceful purposes in areas such as health and agriculture. It is essential that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. The central role of the IAEA in facilitating such cooperation and providing assistance to States is well recognized. The IAEA's role reflects its broad membership, its mandate, its unique expertise and its long experience of providing technical assistance and specialist, practical guidance to States.

Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

Guidance is developed with the active involvement of experts from IAEA Member States, which ensures that it reflects a consensus on good practices in nuclear security. The IAEA Nuclear Security Guidance Committee, established in March 2012 and made up of Member States' representatives, reviews and approves draft publications in the Nuclear Security Series as they are developed.

The IAEA will continue to work with its Member States to ensure that the benefits of peaceful nuclear technology are made available to improve the health, well-being and prosperity of people worldwide.

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION 1

Background (1.1–1.3) 1
Objective (1.4) 1
Scope (1.5–1.7) 2
Structure (1.8–1.9) 3

2. OBJECTIVES OF A STATE'S PHYSICAL PROTECTION REGIME (2.1–2.5) 4

3. ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (3.1–3.4) 6

State responsibility (3.5–3.7) 7
Assignment of physical protection responsibilities (3.8–3.11) 8
Legislative and regulatory framework (3.12–3.49) 10
International cooperation and assistance (3.50–3.54) 20
Identification and assessment of threats (3.55–3.63) 22
Risk based physical protection systems (3.64–3.103) 24
Sustaining the physical protection regime (3.104–3.119) 40
Planning and preparedness for and response to nuclear security events (3.120–3.126) 45

4. DEVELOPING, IMPLEMENTING AND MAINTAINING AN INTEGRATED PHYSICAL PROTECTION SYSTEM FOR NUCLEAR FACILITIES (4.1–4.3) 47

General responsibilities of the operator (4.4–4.13) 47
Security organization (4.14) 50
Process for developing and implementing a physical protection system (4.15–4.22) 51
Identifying the requirements for a physical protection system (Phase 1) (4.23–4.32) 54
Design and evaluation of the physical protection system (4.33–4.59) 58
Key functions of a physical protection system (4.60–4.70) 66

Locating and recovering missing or stolen nuclear material (4.71–4.75) 68
Mitigating or minimizing radiological consequences of sabotage (4.76–4.82) 71
Physical protection measures (4.83–4.123) 72
Nuclear material accounting and control for nuclear security (4.124–4.132) 85
Security of sensitive information (4.133–4.139) 87
Protection of computer based systems (4.140–4.146) 89
Safety–security interface (4.147–4.153) 90
Security plan (4.154–4.161) 93

APPENDIX I: THE SECURITY PLAN 97
APPENDIX II: EXAMPLE CONTINGENCY PLAN 108
APPENDIX III: THE ADDITION OR AGGREGATION OF NUCLEAR MATERIAL 110
APPENDIX IV: CROSS-REFERENCES TO RECOMMENDATIONS 115

REFERENCES 119

1. INTRODUCTION

BACKGROUND

1.1. The IAEA Nuclear Security Series provides guidance for States to assist them in establishing and sustaining a national nuclear security regime and in reviewing and, when necessary, strengthening that regime. The series also provides guidance for States in fulfilling their obligations and commitments under binding and non-binding international instruments.

1.2. The physical protection of nuclear material and nuclear facilities is a major part of the nuclear security regime for those States that have such material and facilities. IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [1] was issued by the IAEA in 2011. As indicated by the title, that Recommendations publication also serves as Revision 5 of IAEA INFCIRC/225, the guidance for States on meeting their obligations under the Convention on the Physical Protection of Nuclear Material and, since the 2005 amendment to that convention entered into force, under the amended convention.

1.3. This publication is the lead Implementing Guide in a suite of guidance to States on implementing the recommendations [1]. Several existing implementing guides and technical guidance publications address specific subjects relevant to the physical protection of nuclear material and nuclear facilities, such as design basis threats, measures against insider threats, nuclear security culture and the identification of vital areas. This Implementing Guide introduces some of those major aspects, provides an overview of their role in physical protection and, when appropriate, refers to the thematic guides for more specific guidance.

OBJECTIVE

1.4. The objective of this publication is to provide guidance and suggestions to assist States and their competent authorities in establishing, strengthening and sustaining their national physical protection regime and implementing the associated systems and measures, including operators' physical protection systems. Some parts of this publication intentionally are not specific in referring to the assignment of responsibilities between the State and its competent authorities, in recognition of the differences among States in this regard. States

should be precise and complete in assigning physical protection responsibilities to their competent authorities and documenting those responsibilities.

SCOPE

1.5. This Implementing Guide applies to the physical protection of nuclear facilities and nuclear material in use and storage against:

(a) The unauthorized removal of nuclear material with the intent to construct a nuclear explosive device;
(b) The sabotage of nuclear material and nuclear facilities resulting in radiological consequences.

This Implementing Guide also provides some suggestions regarding associated measures that may contribute to a coordinated response in the location and recovery of missing nuclear material and the mitigation or minimization of the radiological consequences of sabotage at nuclear facilities.

1.6. This publication does not include detailed guidance on:

(a) The physical protection of nuclear material during transport outside the nuclear facility (such protection is addressed in specific guidance [2]);
(b) Protection against the unauthorized removal of nuclear material for potential off-site dispersal (such protection is addressed in guidance on the security of radioactive material [3]).

This Implementing Guide does not provide detailed guidance on nuclear security considerations in site selection for a facility or in the design of facilities. Integrating physical protection principles as early as possible in a facility's lifetime is commonly referred to as 'security by design'.

1.7. States may decide to require nuclear material and nuclear facilities in their territory to be protected on a variety of other grounds, such as the economic importance of these targets, issues relating to reputation or the potential consequences of loss of nuclear power generation. This publication does not provide guidance on addressing these additional concerns.

STRUCTURE

1.8. The structure of this Implementing Guide is intended to follow, broadly, the structure of the parent Recommendations publication [1] but does not do so exactly:

(a) The protection of nuclear material during transport outside of a nuclear facility is not within the scope of this guide.
(b) This guide describes, in a single section, an integrated, risk based approach to protection against the unauthorized removal of nuclear material and protection against sabotage. In the Recommendations publication [1], these two issues are presented in two separate sections.

1.9. The structure of this publication is as follows. After this introduction, Section 2 describes the objectives of physical protection and the overall approach to managing the risks of the unauthorized removal of nuclear material and the sabotage of nuclear facilities. Section 3 provides guidance for the State and its competent authorities on the physical protection elements of the nuclear security regime; this guidance is based on the fundamental principles set out in the Recommendations publication [1]. Section 4 provides guidance on the operator's physical protection system and describes a systematic, integrated approach. Appendix I gives an annotated outline of the typical contents of an operator's security plan. Appendix II provides similar guidance for the contingency plan. Appendix III provides a description of nuclear material aggregation that can be used to categorize nuclear material and determine the appropriate level of protection against unauthorized removal. Appendix IV presents a table of paragraph cross-references between the Recommendations publication [1] and this Implementing Guide.

2. OBJECTIVES OF A STATE'S PHYSICAL PROTECTION REGIME

2.1. The four objectives of a State's physical protection regime[1] specified in Ref. [1] are also listed in the Amendment to the Convention on the Physical Protection of Nuclear Material and in the Physical Protection Objectives and Fundamental Principles endorsed by the IAEA Board of Governors and the General Conference in September 2001:

> "2.1. The overall objective of a State's nuclear security regime is to protect persons, property, society, and the environment from *malicious acts* involving *nuclear material* and other radioactive material. The objectives of the State's *physical protection regime*, which is an essential component of the State's nuclear security regime, should be:
>
> — **To protect against *unauthorized removal*.** Protecting against theft and other unlawful taking of *nuclear material*.
> — **To locate and recover missing *nuclear material*.** Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen *nuclear material*.
> — **To protect against *sabotage*.** Protecting *nuclear material* and *nuclear facilities* against *sabotage*.
> — **To mitigate or minimize effects of *sabotage*.** Mitigating or minimizing the radiological consequences of *sabotage*.
>
> "2.2. The State's *physical protection regime* should seek to achieve these objectives through:

[1] Historically, the term 'physical protection' has been used to describe what is now known as the 'nuclear security of nuclear material and nuclear facilities', and Ref. [1] (which is also Revision 5 of INFCIRC/225) uses the term 'physical protection' throughout (including the use of the term 'physical protection regime' for those aspects of a nuclear security regime related to the unauthorized removal of nuclear material or the sabotage of nuclear material or nuclear facilities). To aid recognition of this publication as guidance on the implementation of INFCIRC/225/Revision 5, the term 'physical protection' is used here to refer to those aspects of nuclear security related to measures against the unauthorized removal of nuclear material or the sabotage of nuclear material or nuclear facilities. Hence, for example, a State's 'physical protection regime' comprises those parts of its nuclear security regime that relate to such measures.

— Prevention of a *malicious act* by means of deterrence and by protection of sensitive information;
— Management of an attempted *malicious act* or a *malicious act* by an integrated system of *detection*, delay, and response;
— Mitigation of the consequences of a *malicious act*.

"2.3. The objectives mentioned above should be addressed in an integrated and coordinated manner taking into account the different risks covered by nuclear security" [1].

2.2. From a nuclear security perspective the two primary risks associated with the use of nuclear material and nuclear facilities are those of the unauthorized removal of nuclear material, for potential use in a nuclear explosive device, and the sabotage of the material and/or facility resulting in unacceptable radiological consequences. The management of these risks is the primary basis for nuclear security in relation to nuclear material and nuclear facilities. If a State has decided to accept nuclear material and nuclear facilities within its borders, that State has also accepted responsibility for the protection of those materials from unauthorized removal and for the protection of those facilities and materials from sabotage resulting in a release of radionuclides.

2.3. Reference [1] recommends that States adopt a risk management approach to achieve the above objectives relating to protection against unauthorized removal and sabotage. This approach should address the three aspects for characterizing risk: threat, potential consequences and vulnerability. Reference [1] contains recommendations relating to:

(a) Threat assessment and the design basis threat;
(b) Potential consequences of the unauthorized removal of nuclear material (determined using a material categorization table) and of sabotage (determined using an approach of grading radiological consequences), thereby facilitating the use of a graded approach and the application of proportionate physical protection measures;
(c) Addressing, through an effective physical protection system, the vulnerabilities of targets within a nuclear facility that could otherwise be exploited by a threat to successfully complete a malicious act.

2.4. By implementing the recommendations of Ref. [1], the State should be able to appropriately manage the risk arising from malicious acts directed at nuclear material or at a nuclear facility. However, to appropriately manage such a risk the

State needs to set its own detailed nuclear security objectives, taking into account the graded approach.

2.5. To reduce risk, the operator of a nuclear facility may replace nuclear material that is more attractive to adversaries with nuclear material that is less attractive, design the facility to use nuclear material and/or have other characteristics that would result in lesser radiological consequence in the event of sabotage, and/or build more robust physical protection systems. Additionally, competent authorities for intelligence and nuclear security may work closely together to detect and interrupt adversaries planning malicious acts before such plans are carried out at a nuclear facility. Implementing all of the fundamental principles within the State's nuclear security regime and implementing appropriate physical protection measures at nuclear facilities serves the overall objective of protecting the nuclear facility from malicious acts.

3. ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES

3.1. Reference [1] defines a physical protection regime as:

> "A State's regime including:
>
> — The legislative and regulatory framework governing the physical protection of *nuclear material* and *nuclear facilities*;
> — The institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework;
> — Facility and transport *physical protection systems*."

3.2. The State's nuclear security regime should also provide for appropriate management of the interfaces between physical protection and nuclear material accounting and control and between physical protection and safety. The State has the responsibility to ensure that nuclear material accounting and control, safety and nuclear security requirements do not conflict with one another, and that these elements support one another as far as possible.

3.3. This section:

(a) Lists the fundamental principles and other essential elements of the State's nuclear security regime relevant to the physical protection of nuclear material in use and storage and of nuclear facilities, as presented in Refs [1, 4];
(b) Provides guidance on the State's implementation of each principle as it applies to the physical protection of nuclear material and nuclear facilities.

3.4. To meet the objectives of a State's nuclear security regime for nuclear material and nuclear facilities, the State should develop requirements for the establishment, implementation, maintenance and sustainability of its physical protection regime. The responsibilities of a State in this regard are addressed in three separate sections (3, 4 and 5) in Ref. [1], but implementing guidance is consolidated here in this single section.

STATE RESPONSIBILITY

> "**The responsibility for the establishment, implementation and maintenance of a *physical protection regime* within a State rests entirely with that State. (FUNDAMENTAL PRINCIPLE A: Responsibility of the State)**
>
> "3.1. The State's *physical protection regime* is intended for all *nuclear material* in use and storage and during *transport* and for all *nuclear facilities*. The State should ensure the protection of *nuclear material* and *nuclear facilities* against *unauthorized removal* and against *sabotage*" [1].

3.5. The State fulfils its responsibility by establishing a legislative and regulatory framework, delegating regulatory responsibility to one or more competent authorities and assigning primary responsibility for implementing physical protection systems to nuclear facility operators.

3.6. A comprehensive nuclear security regime for nuclear material extends beyond its use and storage (including at nuclear facilities) to its physical protection during transport. The State should ensure that a comprehensive physical protection system for transport is also established, implemented and maintained. Such a system should apply to the on-site movement of Category I and II nuclear material between two protected areas. The operator of a nuclear facility, as the shipper or receiver of nuclear material, may also have certain

responsibilities for the physical protection of nuclear material being transported into or out of the facility. Further guidance is provided in Ref. [2].

3.7. Paragraph 3.2 of Ref. [1] states that:

> "The State's *physical protection regime* should be reviewed and updated regularly to reflect changes in the *threat* and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of *nuclear material* and *nuclear facilities*."

An example of a reason for reviewing and updating the physical protection regime would be a decision to construct a nuclear power plant in a State whose only existing nuclear facility is a research reactor containing only Category III nuclear material. The higher level of physical protection needed for the nuclear power plant would necessitate a review of the regime. Another example would be a change in the threat, as described in paras 3.55–3.63.

ASSIGNMENT OF PHYSICAL PROTECTION RESPONSIBILITIES

> "3.8. The State should clearly define and assign physical protection responsibilities within all levels of involved governmental entities including response forces and for *operators* and, if appropriate, carriers. Provision should be made for appropriate integration and coordination of responsibilities within the State's *physical protection regime*. Clear lines of responsibility should be established and recorded between the relevant entities especially where the entity responsible for the armed response is separate from the *operator*" [1].

3.8. The State should assign physical protection responsibilities to relevant competent authorities and other government entities in relation to at least the following:

(a) Development and maintenance of the design basis threat and/or threat assessment;
(b) Licensing/authorization of nuclear facilities and of nuclear material in use and storage;
(c) Inspection and evaluation of physical protection systems;
(d) Response to nuclear security events, including response forces and emergency response organizations;
(e) Management of interfaces with nuclear material accounting and control;

(f) Management of interfaces with nuclear safety;
(g) Management of information and computer security relevant to physical protection of nuclear facilities and of nuclear material in use and storage;
(h) Determination of the trustworthiness of personnel;
(i) Enforcement actions related to non-compliance with licensing requirements and physical protection regulations.

3.9. The State may consider establishing appropriate arrangements for coordinating actions to meet these responsibilities, such as a committee of governmental entities with assigned physical protection responsibilities that meets regularly for the purpose of promoting communication, cooperation and coordination.

3.10. As part of the State's responsibilities for physical protection, clear lines of responsibility should be established for the appropriate competent authorities that provide the response forces for nuclear security events at nuclear facilities. Coordination between guards, response forces and relevant competent authorities should be promoted, and in particular, coordination between the guards and response forces should be regularly exercised.

3.11. Each State will define its own response objectives and may have different approaches or strategies for using response forces. These definitions, approaches and strategies may depend on the type of nuclear material and nuclear facilities being protected and the potential intentions of adversaries (e.g. theft, sabotage). Response strategies for nuclear facilities with significant targets for theft and/or sabotage are:

(a) Denial of access, in which the goal is for the response force to prevent adversaries from gaining access to the target area;
(b) Denial of task, in which the goal is for the response force to stop the adversaries (including any insiders involved) before they are able to successfully complete their task;
(c) Containment, in which the goal is for the response force to prevent adversaries from removing material beyond a specific point, such as the boundary of the limited access area, thus preventing it from becoming out of regulatory control.

> "**The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of *nuclear facilities* and *transport* to verify compliance with applicable requirements and conditions of the licence or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions. (FUNDAMENTAL PRINCIPLE C: Legislative and Regulatory Framework)**
>
> "3.9. A State should take appropriate measures within the framework of its national law to establish and ensure the proper implementation of the State's *physical protection regime*" [1].

Regulatory approaches

3.12. States should develop and implement regulations consistent with the State's legislative framework. The exact nature and content of regulations will depend on the decisions taken by a State about the manner in which the regulatory function is carried out, including the number of competent authorities involved in supervising the physical protection regime.

3.13. The State is responsible for conducting threat assessments, and a designated competent authority may be responsible for developing a design basis threat, in consultation with other relevant authorities as applicable. In either case, the competent authority uses its threat information as the basis for developing overall requirements and performance objectives, as well as evaluation criteria for compliance or effectiveness. In applying the graded approach, the competent authority defines physical protection objectives and/or requirements for protecting each category of nuclear material and for preventing each level of potential radiological consequences (at or above the threshold for unacceptable radiological consequences) at nuclear facilities.

3.14. The State should ensure that its nuclear security regime is and remains based on a current evaluation of the threat, because the physical protection of nuclear material and nuclear facilities needs to be effective against the threat. There are three distinct approaches to specifying requirements within the

regulatory framework to address the threat. These approaches are the performance based approach, the prescriptive approach and an approach combining elements of the prescriptive and performance based approaches. Either approach, or a combination, may be useful depending on the situation, but the recommendations in Ref. [1] concerning evaluations and performance testing are mostly relevant to the performance based approach, whether used alone or in combination with the prescriptive approach.

3.15. The performance based approach is a more quantitative approach to ensuring and verifying the effectiveness of physical protection and may be particularly useful when protecting higher risk nuclear material against unauthorized removal and protecting nuclear material and facilities against sabotage. This does not necessarily mean that the prescriptive approach alone is not suitable for such cases; however, prescriptive requirements are often more easily applied to a compliance verification of individual physical protection measures rather than to a demonstration of systematic effectiveness through performance testing. Whichever approach is used, the requirements or objectives will need to be specified and the effectiveness of the resulting measures verified by the competent authority.

3.16. The regulatory requirements specified by the competent authority should be focused on addressing the threat identified in the threat assessment or the design basis threat. The design basis threat serves as the basis for developing the physical protection system. The physical protection system for a nuclear facility should be designed by the operator according to the applicable regulatory requirements and should be approved by the competent authority.

3.17. The performance testing of individual physical protection measures and of the physical protection system is recommended in Ref. [1] for nuclear facilities holding Category I or Category II nuclear material and for nuclear facilities, including nuclear power plants, the sabotage of which could lead to high radiological consequences.

Performance based approach

3.18. In the performance based approach, the State defines physical protection objectives on the basis of a threat assessment and, when applicable, a design basis threat, taking into account the graded approach. The State requires that the operator design and implement a physical protection system that meets those objectives, achieving a specified level of effectiveness in protecting against malicious acts and providing contingency responses.

3.19. The performance based approach allows flexibility for the operator to propose a facility specific combination of physical protection measures. For instance, an operator could develop a physical protection system that provides only a short adversary delay time but compensates with a rapid and effective response. The adequacy of these measures is tested against the threat assessment or design basis threat to ensure that the set of performance based measures meets the objectives for the physical protection system.

3.20. An advantage of the performance based approach is that it recognizes that an effective physical protection system can be achieved by many combinations of physical protection measures and that each facility and its operational circumstances may be different. The use of the performance based approach should identify options for a physical protection system that satisfies the physical protection objectives and requirements and also takes account of site specific conditions.

3.21. The performance based approach depends on the competent authority and the operator both having sufficient security expertise to, respectively, establish requirements and implement systems on the basis of physical protection evaluations. The performance based approach also necessarily involves the State providing some sensitive information from the threat assessment or design basis threat to the operator, and the operator should therefore be capable of providing adequate protection of this sensitive information.

Prescriptive approach

3.22. In the prescriptive approach, the State establishes specific physical protection measures that it considers necessary to meet its defined physical protection objectives for each category of nuclear material and each level of potential radiological consequences. The outcome is a set of 'baseline' measures for the operator to implement.

3.23. The advantages of the prescriptive approach include simplicity of implementation for both the State and the operator, elimination of the need for the State to transmit sensitive information to the operators in the form of a threat assessment or a design basis threat, and ease of inspection and evaluation. The use of the prescriptive approach may be particularly appropriate in cases in which both the threat level and the potential consequences are low. An example is Category III nuclear material stored or used in a relatively low threat environment. The prescriptive approach may also be more appropriate in cases

where conducting a detailed threat assessment or establishing a design basis threat is not practicable.

3.24. The prescriptive approach may lack the flexibility to address specific circumstances. Furthermore, with this approach the operator does not have the responsibility to ensure that the security measures implemented are sufficient: the prime responsibility for addressing risks belongs to the State, as the State prescribes exactly what physical protection measures are needed to address the threat. The operator only has responsibility for the effectiveness of the individual physical protection measures when operating and maintaining the physical protection system.

Combined approach

3.25. The combined approach includes elements from both the prescriptive and the performance based approaches. There are many ways of applying the combined approach, of which two are the following:

(a) The State may require the application of a performance based approach for nuclear material with the most significant potential consequences of malicious use and allow the application of a prescriptive approach for nuclear material for which the potential consequences of malicious use are comparatively less significant.
(b) The State may require that a set of prescriptive requirements be followed to address certain defined aspects of security (e.g. protecting sensitive information, establishing trustworthiness); these requirements would supplement measures to address all other aspects derived using the performance based approach.

3.26. The main advantage of the combined approach is the flexibility it allows. The limitations of a combined approach will be similar to those associated with the prescriptive and performance based approaches and will depend on the specific implementation chosen by the State. However, a well executed combined approach may provide an appropriate balance and reduce the effects of the limitations associated with each of the other approaches.

Physical protection system evaluation, including performance testing: Requirements of the State

3.27. The recommendations in Ref. [1] emphasize the importance of evaluating physical protection systems, including performance testing. For example:

(a) The legislative and regulatory framework should "**provide for the establishment of applicable physical protection requirements and include a system of evaluation**" (Ref. [1], Fundamental Principle C).
(b) The legislative and regulatory framework should "ensure that evaluations include exercises to test the *physical protection system*, including the training and readiness of *guards* and/or *response forces*" (para. 3.13 of Ref. [1]).
(c) The competent authority should "ensure that evaluations based on *performance testing* are conducted by *operators* at *nuclear facilities*" (para. 3.21 of Ref. [1]).
(d) The sustainability programme "should encompass: …*Performance testing* and operational monitoring" (para. 3.57 of Ref. [1]).

3.28. All operators of nuclear facilities should conduct evaluations, including performance testing, of the physical protection system for their facilities; these evaluations should take into account the systems for nuclear material accounting and control, information security and computer security.

3.29. The evaluation of physical protection systems generally consists of testing and analysis. Testing may be conducted at the component, subsystem or system level and may include hardware/equipment, software, people and procedures. Analysis may include qualitative and/or quantitative methods and may involve the use of modelling and simulation. Modelling and simulation methods may include manual or computer based mathematical models, computer combat simulations, tabletop exercises, limited scope and full scope response force exercises, and force-on-force exercises. Evaluations of physical protection systems should always include some exercises.

3.30. The different methods will need different amounts of data (with different quality requirements), provide different types of information, have different limitations and need different levels of resources. Using the graded approach, the competent authority should establish a minimum set of physical protection system evaluation measures, including performance testing requirements. These regulatory requirements could address roles and responsibilities, required and/or allowed methods, documentation requirements, and requirements for the frequency of evaluation and testing. For example, some tests and exercises may be required at least on an annual basis; more comprehensive exercises (such as force-on-force exercises) may be conducted less frequently but should be required at least every two to three years.

3.31. The competent authority should review the physical protection system evaluations, including performance testing, for example by verifying that the data and methods supporting the evaluation and testing are correct and that the results of the evaluation and testing correctly characterize the physical protection system.

3.32. The competent authority may consider using an independent third party with appropriate expertise to conduct performance testing. One example would be to perform delay tests of sample barriers using the adversary capabilities defined by the threat assessment or the design basis threat.

Licensing and other procedures to grant authorization

> "3.12. The State should license activities or grant authorization only when such activities comply with its physical protection regulations. The State should make provisions for a detailed examination, made by the State's *competent authority*, of proposed *physical protection measures* in order to evaluate them for approval of these activities prior to licensing or granting authorization, and whenever a significant change takes place, to ensure continued compliance with physical protection regulations" [1].

3.33. Primary responsibility for implementing measures for the physical protection of nuclear material rests with each operator; control over physical protection by the State is exercised primarily through government or regulatory licensing (or authorization). The licence should be an official document authorizing the operation of a facility or the carrying out of an activity (such as the transport of nuclear material into and out of the nuclear facility). A primary task of the State is to define licensing requirements in relation to physical protection systems and to consider whether to approve applications for new licences and renewals or amendments to existing licences. The operator's security plan is submitted by an applicant as part of the licensing process for the operation of a nuclear facility, and compliance with the approved security plan should be a condition of the licence.

3.34. Licensing is an ongoing process throughout all stages of the life of a nuclear facility. The licence may be modified, suspended or revoked — depending on circumstances and the operator's performance — but always by and under the control of the State.

3.35. The State should license facilities and activities only when they comply with the State's physical protection requirements. It is suggested that any licence issued include:

(a) The designation of the specific facility or activities licensed;
(b) Any specific requirements, conditions, time limits or other constraints;
(c) An explicit statement of the responsibilities of the licensee.

3.36. The State should ensure, before a licence is issued and before nuclear material is introduced into a facility, that the competent authority has received, assessed and approved the applicant's or operator's security plan for the facility or activity to be licensed. The assessment should be supported by a review of the physical protection system proposed for the facility. Should any deficiencies be identified, the State may withhold the granting of the licence until these deficiencies are corrected and the physical protection system is verified to be acceptable. Alternatively, the State may approve the licence with conditions requiring that the deficiencies be corrected within a specified time.

3.37. Further guidance on the licensing process is provided in Ref. [5].

Regulatory enforcement

3.38. Enforcement of physical protection regulations and licensing conditions through an effective legal and regulatory framework is a necessary part of a State's physical protection regime. For the protection of nuclear material and nuclear facilities, the State should assign to an appropriate competent authority the power to initiate legal proceedings or impose sanctions in accordance with the law. Such sanctions may include the suspension or revocation of a licence and/or other penalties against individuals or organizations.

Competent authority

> "**The State should establish or designate a *competent authority* which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State's *competent authority* and those of any other body in charge of the promotion or utilization of nuclear energy. (FUNDAMENTAL PRINCIPLE D: *Competent Authority*)**" [1].

3.39. Effective independence means the ability of the competent authority responsible for nuclear security to enforce the requirements and regulations necessary for nuclear security without interference from those responsible for the promotion or utilization of nuclear energy or other nuclear applications. The operations, funding and staffing of the competent authority should be independent of bodies associated with such promotion or utilization. To perform its functions and to discharge its responsibilities in a manner commensurate with the nature and number of nuclear facilities and activities to be regulated, the competent authority will need to have access to sufficient financial resources and to employ sufficient qualified and competent staff. It is suggested that the competent authority develop human resource plans that identify the necessary levels of staffing and training to adequately perform the competent authority's functions.

Role of competent authority in requiring security plans

> "3.27 …The *competent authority* should review and approve the security plan, the implementation of which should then be part of the licence conditions" [1].

3.40. The competent authority should effectively communicate to licence applicants and operators those requirements that they must satisfy to design and implement a physical protection system that will be acceptable to the competent authority under the State's legislative and regulatory framework for physical protection. An important element is the operator's development of and compliance with the security plan, appropriate to the category of nuclear material being protected and the levels of the potential radiological consequences of sabotage. It is suggested that the competent authority issue instructions to operators concerning requirements for a security plan that should ensure that all elements of the State's physical protection requirements are addressed.

3.41. The security plan is the primary documentation describing the physical protection system intended to meet the requirements specified by the competent authority. The State should specify what information in the security plan needs to be protected as sensitive information and how it should be protected. An annotated suggested outline for a comprehensive security plan is presented in Appendix I.

Role of competent authority in establishing an inspection programme

> "3.20. The State's *competent authority* should be responsible for verifying continued compliance with the physical protection regulations and licence conditions through regular inspections and for ensuring that corrective action is taken, when needed" [1].

3.42. The objective of an inspection programme is to verify that the physical protection measures actually in place are in compliance with regulatory requirements and applicable licence conditions. This process should include verifying that the approved security plan is being implemented effectively. In cases of non-compliance with regulatory requirements or licence conditions, regulatory and/or enforcement action should be considered, and relevant and proportionate measures or sanctions may be applied.

3.43. The competent authority needs to ensure that its inspectors have the necessary qualifications, training and experience to carry out their roles. The competent authority may specify qualification and training requirements for inspectors.

3.44. The inspection programme should include both announced and unannounced inspections to provide assurance that the operator maintains arrangements in accordance with the approved security plan at all times, not only when it is known that an inspection will occur. Inspections may occur at any time, during or outside normal working hours, and may include all routine and non-routine operational activities undertaken at the nuclear facility at that time (e.g. during reactor shutdown for maintenance and refuelling). It is suggested that the inspection programme ensure that all physical protection measures, including technical, procedural and administrative provisions, are reviewed and verified. Inspections should be carried out in a manner that does not unduly impede or affect facility operations. If the inspection identifies any deficiencies in the physical protection system, the competent authority should ensure that compensatory measures are employed by the operator to provide adequate protection until the deficiency has been corrected and a sufficiently effective system has been achieved.

3.45. When inspectors identify non-compliance or other issues of concern, subsequent inspection procedures should include verification that the operator has taken all the corrective actions required. It is suggested that these actions be graded and acted on in a manner commensurate with the category of nuclear material present and the potential consequences of sabotage. Inspectors will need

to monitor progress and verify follow-up actions to be assured that corrective actions have been completed to an acceptable standard and that effective protection has been achieved. The competent authority should approve corrective actions, and these actions should be included in an updated security plan. In some cases, the return to normal operating conditions after corrective actions may only need the competent authority to be notified, rather than explicit approval from the competent authority.

3.46. The number of inspections planned for a specific facility may be determined by the competent authority on the basis of the category of material being protected, the level of the potential radiological consequences of sabotage, the threat assessment or the design basis threat, and any other relevant factors. The operator's history of compliance may also be taken into account in determining the frequency of inspections. Reactive inspections may also be necessary from time to time, for example after a nuclear security event at a nuclear facility or a change in the threat.

Timely reporting of nuclear security events

> "3.22. The State's *physical protection regime* should include requirements for timely reporting of *nuclear security events* and information which enables the State's *competent authority* to be informed of any changes at *nuclear facilities* or related to *transport* of *nuclear material* that may affect *physical protection measures*" [1].

3.47. The State should determine the types of event that the operator is required to report to the competent authority and acceptable time periods within which the events must be reported. The competent authority should receive timely information about any significant events concerning unauthorized actions that affect the physical protection of nuclear material or nuclear facilities, for example:

(a) Actual or attempted intrusion into the facility or into a designated area;
(b) Attempted or actual unauthorized removal, loss or unauthorized movement of nuclear material, whether involving external adversaries or insiders;
(c) Attempted or actual acts of sabotage;
(d) Discovery of prohibited items;
(e) Deviation from the approved security plan (e.g. loss of power supply to physical protection equipment or weather damage to fences);
(f) Events involving individuals that must be reported in accordance with the State's trustworthiness policy;

(g) Loss or unauthorized disclosure of sensitive information;
(h) Compromise or attempted compromise of computer systems used for physical protection, nuclear safety or nuclear material accounting and control systems (see Ref. [6] for further guidance).

3.48. The competent authority may be required to inform other government entities and participate in a coordinated response to the nuclear security event. The operator or competent authority may be required to investigate the incident to prevent a reoccurrence and to learn from the experience. Enforcement action may also be required.

Responsibility of the licence holders

> "**The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of *nuclear material* or of *nuclear facilities* rests with the holders of the relevant licences or of other authorizing documents (e.g. *operators* or *shippers*). (FUNDAMENTAL PRINCIPLE E: Responsibility of the Licence Holders)**" [1].

3.49. This topic is addressed in paras 4.4–4.13 on general responsibilities of the operator.

INTERNATIONAL COOPERATION AND ASSISTANCE

3.50. Each State should consider whether, under what circumstances and to what extent it may cooperate with other States, including the appropriate sharing of information and knowledge derived from the national nuclear security regime. This decision should consider the need to protect sensitive nuclear security information and comply with any international obligations or agreements to share information.

3.51. Reference [1] provides two recommendations and one suggestion regarding international cooperation and assistance, specific to the physical protection of nuclear facilities, as detailed in the following three paragraphs.

3.52. As stated in para. 3.33 of Ref. [1]:

> "In the case of *unauthorized removal* or *sabotage* or credible threat thereof, the State should provide appropriate information as soon as possible to other States which appear to it to be concerned, and to inform, where appropriate, the International Atomic Energy Agency and other relevant international organizations."

Information may be provided on a voluntary basis to the IAEA. In the case of the unauthorized removal of nuclear material, the affected State may benefit particularly from assistance from neighbouring States in locating and recovering the missing nuclear material if it may have entered or passed through those States. Detection of the material will depend on the system(s) for the detection of nuclear and other radioactive material out of regulatory control in the State where the material is or through which it passed. Further guidance on this issue can be found in Ref. [7].

3.53. As stated in para. 3.32 of Ref. [1]: "States should inform the International Atomic Energy Agency, and other States as applicable, of appropriate points of contact for matters related to the physical protection of *nuclear material* and *nuclear facilities*." State points of contact for physical protection are especially important in the case of unauthorized removal or sabotage to facilitate the communication of essential information quickly and accurately to neighbouring States and other concerned parties, either directly or through the IAEA[2]. These points of contact may also be useful in communicating other important information relevant to physical protection, such as information about new threats of common concern.

3.54. As stated in para. 3.31 of Ref. [1]: "States are encouraged to cooperate and consult, and to exchange information on physical protection techniques and practices, either directly or through the International Atomic Energy Agency and other relevant international organizations." States with operating nuclear facilities have gained experience with physical protection and have accumulated good practices and lessons learned. Sharing this type of information among States can benefit the global community by helping to raise the overall level of physical protection of nuclear material. Although some facility specific sensitive

[2] For a nuclear security event resulting in a nuclear or radiological emergency, the provision of information about the event and the provision of assistance should be dealt with through the operational arrangements developed by the IAEA under the early notification and assistance conventions and the IAEA safety standards in emergency preparedness and response.

information may not be shared, much useful information can be shared through workshops, training programmes and conferences. The IAEA is a useful vehicle for sharing such information without a need for attribution.

IDENTIFICATION AND ASSESSMENT OF THREATS

> "**The State's physical protection should be based on the State's current evaluation of the threat. (FUNDAMENTAL PRINCIPLE G: Threat)**
>
> "3.34. The appropriate State authorities, using various credible information sources, should define the *threat* and associated capabilities in the form of a *threat assessment* and, if appropriate, a *design basis threat*. A *design basis threat* is developed from an evaluation by the State of the threat of *unauthorized removal* and of *sabotage*" [1].

3.55. A threat assessment is an evaluation of the existing threats that describes the motivations, intentions and capabilities of potential adversaries to commit malicious acts. The threat assessment includes consideration of threats of terrorism and of other criminal or intentional unauthorized acts involving or directed against nuclear material and nuclear facilities, particularly the unauthorized removal of nuclear material and the sabotage of nuclear material and nuclear facilities. The threat assessment also considers both external and insider threats. The threat assessment makes use as appropriate of domestic, transnational and global sources of information on the threats.

3.56. States will have different levels of ability to identify and evaluate threats. Some States have extensive and sophisticated security and intelligence capabilities that can assist the State in understanding the nature and extent of threats, including those that might be directed towards nuclear material and nuclear facilities. In other cases, general information about the national threat (e.g. areas of civil unrest, criminal activities, terrorist presence) and international threats will need to be understood and evaluated to identify the potential threat within the State.

3.57. A competent authority should be assigned overall responsibility for the development of the threat assessment, which will need cooperation between all the State agencies that have responsibility for understanding and responding to the threat (e.g. intelligence services, police, military, customs and border control, local law enforcement agencies). As this work will require the use of sensitive

information, appropriate information security measures should be applied to the threat assessment and any resulting design basis threat.

3.58. Further guidance on threat assessment and on defining a design basis threat on the basis of the threat assessment is given in Ref. [8]. The guidance includes considerations concerning the decision of whether to use a design basis threat or an alternative threat statement. (The "alternative threat statement" noted in Ref. [8] represents a less rigorous approach in defining the threat for the design of physical protection systems.)

3.59. A design basis threat may be used by the competent authority in different ways. Under the performance based approach, a design basis threat may be used by the operator for the design of the physical protection system and by the competent authority for the evaluation of the physical protection system. Under the prescriptive approach, a threat assessment may be sufficient for the competent authority to define the physical protection measures that the operator will be required to implement, except where Category I nuclear material is held and/or the sabotage of the nuclear facility could potentially lead to high radiological consequences. In these latter cases, the State's physical protection requirements should be based on a design basis threat specifically for the unauthorized removal of Category I nuclear material and the sabotage of nuclear material and nuclear facilities.

3.60. Paragraph 3.36 of Ref. [1] states that:

> "When considering the threat, due attention should be paid to *insiders*. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The *physical protection system* should be assisted by nuclear material accountancy and control measures to deter and detect the protracted theft of *nuclear material* by an *insider*."

The IAEA has published specific guidance [9] to assist States in addressing insider threats.

3.61. Consideration should be given in the threat assessment and the design basis threat to possible attacks on computer based systems, including instrumentation and control and other systems necessary for nuclear safety, nuclear material accounting and control, and the physical protection system. Such systems include databases, access controls and alarm management systems. When reviewing

threats to such systems, consideration should be given not only to attacks aimed simply at disabling or destroying systems but also to less direct attacks, such as the manipulation and falsification of data. Consideration should also be given to the potential capabilities of the adversary, from the perspective of both insider threats and external threats. Reference [6] provides more guidance on this type of threat.

3.62. The threat assessment or design basis threat should include consideration of possible stand-off attacks (para. 3.40 of Ref. [1]), carried out at a distance from the nuclear facility. Such attacks do not involve the adversary having access to the target or needing to overcome the physical protection system. Examples of stand-off scenarios include the use of portable missile launchers or malicious aircraft impacts. The State should determine which types of stand-off attack need to be considered by the operator.

3.63. The State should continually review the threat and evaluate the implications of any changes in the threat assessment or the design basis threat. For example, the State may decide annually whether the review of the threat necessitates an update of the threat assessment. Nuclear security events within the State or elsewhere may lead to the State updating the threat assessment before the scheduled periodic review. The State should review its physical protection requirements in the light of any change to the threat assessment or the design basis threat. The operator will then need to review its physical protection system (including a review of potential sabotage targets), and any resulting changes to the design of the physical protection system should be submitted to the competent authority for approval before implementation.

RISK BASED PHYSICAL PROTECTION SYSTEMS

> "3.41. The State should ensure that the State's *physical protection regime* is capable of establishing and maintaining the risk of *unauthorized removal* and *sabotage* at acceptable levels through risk management. This requires assessing the *threat* and the potential consequences of *malicious acts*, and then developing a legislative, regulatory and programmatic framework which ensures that appropriate effective *physical protection measures* are put in place" [1].

3.64. In nuclear security, the assessment of risk includes the consideration of threats, the likelihood that malicious acts could be successfully carried out by those threats and the potential consequences of such acts.

3.65. The State should use a risk management approach to ensure that its physical protection requirements and operators' measures to meet them are keeping the risk associated with unauthorized removal or sabotage at what the State considers an acceptable level. Risk management involves periodically evaluating the threats and the potential consequences of malicious acts and ensuring that appropriate physical protection systems are put into place to prevent, or sufficiently reduce the likelihood of, a successful malicious act.

3.66. Risk management takes into account an assessment of risk, which may be quantitative or qualitative. A quantitative assessment of risk involves determining the risk associated with a particular event as a function of quantitative expressions of the probability of the event occurring and the expected consequences of the event if it were to occur. However, quantifying the probability of a malicious act being attempted, or of an attempt being successful, is very difficult. For the purposes of planning physical protection measures, it may be sufficient to assume that an attempt to carry out a malicious act is certain to occur. In this case the risk is called conditional risk, where the condition is that a malicious attack is attempted. Conditional risks may be useful for providing an upper bound to a quantitative assessment of the risk and for comparing risks in cases in which the likelihood of an attempt is not a distinguishing factor (e.g. for comparing different physical protection options against the same risk).

3.67. In the absence of quantitative methods to determine the nuclear security risk, qualitative risk management approaches may be used to inform decisions on physical protection. Qualitative risk management involves considering the likelihood of an attempt and of the success of such an attempt without attempting to quantify these likelihoods as probabilities; instead, qualitative risk management takes account of the vulnerability of the target(s) to the threat and of the potential consequences of a successful attempt. This approach can be used to identify combinations of factors indicating a high risk (e.g. high threat likelihood, high-level adversary capabilities, severe consequences) and where efforts should be focused to reduce the risk most effectively. Similarly, combinations of factors indicating a low risk may illustrate where security measures might not need to be so stringent.

3.68. The State determines the criteria for acceptable performance of the physical protection system against unauthorized removal, usually in relation to the design basis threat, because the State must accept the residual risk of any failure of the physical protection system. The State should also determine thresholds for unacceptable radiological consequences and high radiological consequences to use as the basis of the performance requirements for the physical protection

system against sabotage. If the potential radiological consequences are less severe than the unacceptable radiological consequences defined by the State, measures to protect safety related equipment and devices by controlling access to them and securing them should be provided (more detail is provided in paras 3.93–3.95). Risk management practices provide a means to inform the appropriate application of physical protection measures through the use of a graded approach, as described further in paras 3.70–3.101.

3.69. A risk assessment may identify risks that need to be further evaluated to determine whether additional measures are required to reduce them. Risk can be managed through, for example, improving deterrence (e.g. enhancing the visibility of robust physical protection measures), strengthening physical protection measures (e.g. providing additional defence in depth) and reducing potential consequences (e.g. changing the amount, type, dilution, chemical or physical form of the nuclear material). The safety implications of such changes should also be considered.

Graded approach

> "**Physical protection requirements should be based on a *graded approach*, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the *nuclear material* and potential consequences associated with the *unauthorized removal* of *nuclear material* and with the *sabotage* against *nuclear material* or *nuclear facilities*. (FUNDAMENTAL PRINCIPLE H: *Graded Approach*)**" [1].

3.70. The development of the State's physical protection requirements and regulations should be structured around a graded approach, which is used to provide higher levels of protection against events that could result in more significant consequences.

3.71. To grade protection against the unauthorized removal of nuclear material for use in a nuclear explosive device, the category of the nuclear material, as defined in Table 1 (adapted from Ref. [1]), reflects the relative difficulty of using that category of material to produce a nuclear explosive device. Category I nuclear material should be protected with the most stringent levels of physical protection; nuclear material below Category III need to be protected only in accordance with prudent management practice (para. 4.12 of Ref. [1] and footnote c of Table 1).

TABLE 1. CATEGORIZATION OF NUCLEAR MATERIAL *(adapted from table 1 of Ref. [1])*

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (^{235}U)	Unirradiated[b]			
	– Uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– Uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10 kg or more	Less than 10 kg but more than 1 kg
	– Uranium enriched above natural but less than 10% ^{235}U			10 kg or more
3. Uranium-233 (^{233}U)	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage, and transport, taking all relevant factors into account.)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content)[d,e]	

Note: This table is not to be used or interpreted independently of the text of Ref. [1].

[a] All plutonium except that with isotopic concentration exceeding 80% in ^{238}Pu.

[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[e] Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h (100 rad/h) at 1 m unshielded.

3.72. For protection against sabotage, the State needs to consider the potential radiological consequences of such acts and apply a graded approach. The State should consider how to protect nuclear facilities while taking into account the potential for sabotage to cause unacceptable radiological consequences. The State should also ensure that protection measures are required for the targets within the facilities which if subject to sabotage would produce such consequences.

3.73. The State should also consider the use of a graded approach in defining the requirements for other physical protection measures, such as the confidentiality of sensitive information and the trustworthiness of individuals.

Graded levels of physical protection based on consequence of unauthorized removal

Nuclear material categorization for unauthorized removal

> "4.5. The primary factor in determining the *physical protection measures* against *unauthorized removal* is the *nuclear material* itself. Table 1 categorizes the different types of nuclear material in terms of element, isotope, quantity and irradiation. This categorization is the basis for a *graded approach* for protection against *unauthorized removal* of *nuclear material* that could be used in a nuclear explosive device, which itself depends on the type of nuclear material (e.g. plutonium and uranium), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity" [1].

3.74. Table 1, adapted from Ref. [1], specifies the types of nuclear material (e.g. plutonium or uranium), irradiation levels, isotopic compositions (i.e. content of fissile isotopes) and quantities that establish the thresholds for three categories (I–III) and, implicitly, a fourth category: 'below Category III'.

3.75. The categorization in Table 1 makes use of four attributes of nuclear material cited in para. 4.5 of Ref. [1], namely nuclear material type, isotopic composition, quantity and irradiation. Table 1 does not describe how to use the other attributes mentioned in that paragraph, such as physical and chemical form and degree of dilution, as a basis for graded protection against unauthorized removal. However, Ref. [1] indicates that a State can take into account all of these attributes.

Categorization of irradiated fuel

3.76. Row 4 of Table 1 effectively defines irradiated fuel as material irradiated in a reactor with a radiation level greater than 1 Gy/h (100 rad/h) at 1 m unshielded. This row indicates that irradiated fuel that was composed before irradiation of depleted or natural uranium, thorium or uranium enriched to less than 10% ^{235}U belongs in Category II, despite none of these fuels being placed higher than Category III before irradiation. The reason for this change in categorization is that during irradiation in a reactor, plutonium (mostly ^{239}Pu) is produced in uranium based fuels and ^{233}U is similarly produced in thorium fuel. The percentage of plutonium or ^{233}U produced as a result of irradiation is relatively small (typically around 1% of the total weight of fuel in the case of plutonium). However, as this irradiated fuel is typically stored in large quantities, it contains a quantity of nuclear material (more than 2 kg of plutonium or ^{233}U) sufficient to place it in Category I. In common with the guidance in footnote e of Table 1, such irradiated fuel may be reduced by one category (to Category II) because of its reduced attractiveness due to the high radiation levels it causes.

3.77. Row 4 of Table 1 also states that, on evaluation of the specific circumstances, States may assign a different level of physical protection to the above mentioned irradiated fuels while in domestic use, storage and transport. An example of such circumstances is a location (such as a post-irradiation examination facility) at which only a small number of irradiated fuel rods are held. Because of the small quantity of material, the irradiated fuel rods may contain less than 2 kg plutonium or ^{233}U, in which case it would be appropriate to protect the irradiated fuel as Category III nuclear material. (Records maintained for nuclear material accounting and control will confirm whether these lower quantities are indeed present, as the records should contain an estimate of the quantity of plutonium or ^{233}U within irradiated fuel, as well as the quantity of other nuclear material in this fuel.)

3.78. Footnote e of Table 1 states that other fuel that is Category I or II before irradiation may be reduced by one category after it becomes irradiated fuel. This footnote is applicable in the following circumstances, for the reasons stated:

(a) The common plutonium based fuels, mixed oxide fuel and fast reactor fuel, typically contain around 7% and 30% plutonium, respectively. Although irradiation in a reactor will reduce the plutonium content to some extent, it will not substantially reduce the overall content by weight of plutonium in the irradiated fuel. Since such fuel is usually stored in large amounts, the quantity of plutonium in the irradiated fuel in a typical storage location

will be sufficient to place it in Category I. This fuel may be reduced by one category to Category II, in accordance with footnote e of Table 1, because its high radiation levels make it less attractive to adversaries.

(b) Irradiation in a reactor of high enriched uranium fuels (i.e. those containing uranium enriched to 20% ^{235}U or more) will reduce the ^{235}U content by a few per cent. However, this reduction will not normally diminish the enrichment level to below 20%. Thus, the irradiated fuel will continue to comprise mostly uranium enriched to 20% or more. As a result, irradiated high enriched uranium fuel held at one location that in total contained 5 kg or more ^{235}U before irradiation may be reduced from Category I to Category II, and high enriched uranium fuel that contained more than 1 kg but less than 5 kg ^{235}U before irradiation may be reduced from Category II to Category III, in accordance with footnote e of Table 1. This reduction in category reflects the materials' reduced attractiveness due to their radiation level.

(c) Similarly, irradiation in a reactor of fuels originally containing uranium enriched to at least 10% ^{235}U but less than 20% ^{235}U (e.g. research reactor fuel, which is commonly enriched to around 19.5% ^{235}U before irradiation) will not normally reduce the ^{235}U enrichment level to below 10%. The irradiation of fuel enriched to these levels does not produce a quantity of plutonium above the threshold for Category III because of the relatively small amounts of fuel used in research reactors. Hence, the categorization of this fuel, once irradiated, is determined primarily by the quantity and enrichment level. Therefore, if the total quantity of this fuel held at one location contained 10 kg or more ^{235}U before irradiation, it may be reduced from Category II to Category III once it becomes irradiated fuel.

3.79. The option for States to assign irradiated fuel to a different category of physical protection from that indicated in Table 1 (footnote d) does not necessarily apply to irradiated fuel that originally contained a Category I or II quantity of plutonium or uranium enriched to 10% or more. Radiation levels of all types of irradiated fuel will reduce over time, which may necessitate reconsideration of the categorization of material that was reduced by one category on the basis of footnote e and row 4 of Table 1.

3.80. As noted above, States have the option under footnote e of Table 1 to reduce by one category the physical protection measures against the unauthorized removal of nuclear material if that nuclear material has a total external radiation dose rate in excess of 1 Gy/h at a distance of 1 m from any accessible surface without intervening shielding. This criterion is the dose rate at which an individual attempting to handle the material would begin to suffer

serious deterministic health effects from radiation exposure within a time period of less than 1 h. Under simple theft scenarios, it was originally assumed that a radiation dose rate at this level would act as an effective deterrent to the theft of radioactive material. However, some contemporary adversaries have proved their willingness to risk death to achieve their missions and thus may not be deterred by the effects of radiation exposure from handling irradiated fuel. States should therefore carefully consider whether or not the provision in footnote e is an acceptable modification in determining their physical protection requirements.

Considerations in setting graded protection requirements based on material form or dilution

3.81. Many States have historically used a three factor method to categorize unirradiated nuclear material for the purpose of applying appropriate physical protection against unauthorized removal. Under this method, for any nuclear material, the fissile element (plutonium or uranium), the isotopic composition and the quantity are the three factors considered in determining the level of physical protection required to protect against unauthorized removal. This method is simple to implement, but in some situations it may result in excessive protection requirements for the material being protected. It is therefore suggested that the State consider other attributes of the material that might provide additional impediments to an adversary in potential theft scenarios; these impediments might include the dilution or wide separation of the nuclear material.

3.82. The recommendations in Ref. [1] recognize the need for the consideration of other factors:

(a) For nuclear material in general, the categorization from Ref. [1]:

> "is the basis for a *graded approach* for protection against *unauthorized removal* of *nuclear material* that could be used in a nuclear explosive device, which itself depends on the type of nuclear material (e.g. plutonium and uranium), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity" (para. 4.5 of Ref. [1]).

(b) For waste: "*Nuclear material*, which is in a form that is no longer usable for any nuclear activity, minimizes environmental dispersal and is practicably irrecoverable, may be protected against *unauthorized removal* in accordance with prudent management practice" (para. 4.7 of Ref. [1]).

(c) For irradiated fuel, footnote e of Table 1 allows for a reduction of category based on radiation level.

3.83. The presence of nuclear material in a dilute form will force an adversary to acquire much larger total amounts of material to obtain a significant quantity of nuclear material. The adversary may also have more difficulty in recovering the nuclear material, needing to perform more processing steps to convert the nuclear material to a form usable to construct a nuclear explosive device. Given these additional challenges for the adversary, a State may wish to consider the level of dilution when categorizing nuclear material. Possible additional parameters for categorization could be the concentration of nuclear material and the homogeneity of the concentration within the material. This could encourage the processing and storage of nuclear material in forms that are less attractive to an adversary.

3.84. If the material itself is considered to have intrinsic factors reducing its attractiveness to adversaries, or other characteristics which may be considered in determining appropriate protection, an evaluation of the likely effect of these factors should be performed and documented before such factors are used to modify the physical protection measures indicated by the three factor method of categorization.

Additional considerations based on adding nuclear material together

> "4.8. In determining the levels of physical protection in a facility, which may consist of several buildings, the *operator* may identify, in agreement with the State's *competent authority*, part of the *nuclear facility* which contains *nuclear material* of a different category and which is therefore protected at a different level than the rest of the *nuclear facility*. Conversely, consideration may need to be given to adding together the total amount of *nuclear material* contained in a number of buildings to determine the appropriate protection arrangements for this group of buildings" [1].

3.85. When assigning physical protection levels for a nuclear facility, a group of buildings or a group of rooms against the unauthorized removal of nuclear material, consideration may need to be given to aggregating (adding together) the total amount of nuclear material within the facility, the group of buildings or the group of rooms. The method used for nuclear material aggregation is an important element in deciding on, and increasing if necessary, the required levels of physical protection.

3.86. Paragraph 4.8 of Ref. [1] addresses the possibility that quantities of nuclear material may be removed by the adversary from several locations or buildings during a single attack.

3.87. In some facilities, nuclear material of the same type (e.g. uranium enriched to more than 20% ^{235}U) may be located in several different buildings, for different purposes or at different stages of a process. For example, there may be 4 kg of such material in one building and another 4 kg of similar material in another building within the same protected area. Considered individually, each quantity of material would be placed in Category II. However, if the whole 8 kg could be taken by an adversary during a single attack, the material should be designated as Category I and the physical protection system should be correspondingly robust.

3.88. Nuclear material of different types (e.g. plutonium, ^{233}U, uranium with different levels of enrichment in ^{235}U) may be collocated in the same nuclear facility. The total amount of nuclear material in the facility should be considered in determining the categorization of the nuclear material in any specific location within the facility and, hence, in identifying the appropriate physical protection measures to apply to the nuclear material. There are several possible formulas for calculating the category for aggregated quantities of different nuclear material, and the State should decide which approach it will use. One approach for aggregating different types of nuclear material uses a set of formulas derived from Table 1: this approach is described in Appendix III.

3.89. Enhanced protection against unauthorized removal from different locations within a nuclear facility might not be required if the competent authority approves a determination by the operator that the unauthorized removal of separate quantities of materials from the different locations by a single adversary is unlikely because:

(a) The separate locations are protected by separate physical protection systems and guards and/or response forces are able to effectively counter attacks by adversaries at all locations;
(b) The separate locations are managed by and under the control of different groups of employees, thereby limiting the threat from an insider to any one of the locations.

3.90. The operator may also consider how much nuclear material an adversary could acquire in a specified time period to inform the decision on what level of physical protection is considered appropriate for an aggregated amount. The operator should then (a) propose appropriate physical protection measures

to reduce an adversary's ability to aggregate nuclear material or (b) apply appropriate physical protection measures if the aggregation of nuclear material results in a higher category.

Graded levels of physical protection based on consequences of sabotage

> "3.44. …For protection against *sabotage*, the State should establish its threshold(s) of *unacceptable radiological consequences* in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection" [1].

3.91. Unlike the categorization described in Table 1 for the unauthorized removal of nuclear material, there is no simple classification scheme for sabotage targets: the category assigned to nuclear material on the basis of the risk of unauthorized removal is not a useful indicator of the potential consequences of the sabotage of the material or of the facility the material is in. For example, fresh high enriched uranium fuel (Category I) is of great concern in relation to its possible theft but is of very little concern from a sabotage perspective because the radiation levels from the material and the potential radiological consequences of its release are low. However, high enriched uranium fuel that has been irradiated in a reactor may be a lesser concern in relation to theft, because the high radiation levels from fission and activation products would make theft difficult and dangerous, but such fuel may be a more attractive target for sabotage because of the potential radiological consequences from the release of those fission and activation products.

3.92. The State should establish the regulatory basis for physical protection against sabotage, which should include the State defining the threshold for unacceptable radiological consequences. This basis should then be used by the operator to develop physical protection measures against sabotage. As noted in paras 3.93–3.95, States should also define the threshold for high radiological consequences, above which it is recommended that vital areas are identified and protected at a higher level, as specified in paras 5.20–5.42 of Ref. [1].

Unacceptable radiological consequences and high radiological consequences

3.93. The potential consequences of sabotage are considered in relation to a level above which radiological consequences are defined by the State to be unacceptable. The definition of unacceptable radiological consequences may be quantitative or qualitative. The unacceptable radiological consequences are defined by the State and may include criteria for the release of radionuclides (e.g. the total activity

release or the release of specified radionuclide(s) exceeding some identified level), dose criteria (e.g. a release sufficient to lead to the radiation dose to an individual at some defined location exceeding a defined limit) and design limits (e.g. sabotage that may result in significant core damage in a reactor). The same unacceptable radiological consequences should apply to the potential radiological consequences of sabotage for all radioactive material at nuclear facilities. The State's definition of unacceptable radiological consequences will, in turn, permit the identification of targets the sabotage of which could lead to such consequences and that should therefore be protected. Defining consequences considered to be unacceptable radiological consequences (and high radiological consequences; see below) will include safety considerations and should be determined in close consultation with safety authorities. For example, the definitions of unacceptable radiological consequences and high radiological consequences might be linked to criteria used for emergency preparedness and response [10, 11].

3.94. The threshold of unacceptable radiological consequences may be set at a level corresponding to a relatively small release of radionuclides in a localized area within the nuclear facility. Targets with the potential to cause only these lesser consequences may require a correspondingly low level of protection. At the other extreme, targets for which sabotage could potentially result in a substantial radiological release significantly affecting the population and environment beyond the boundaries of the nuclear facility need the highest level of protection. Such a severe event is referred to in Ref. [1] as having high radiological consequences.

3.95. Therefore, the State should also define the threshold for high radiological consequences. If the potential radiological consequences of sabotage are assessed to be greater than or equal to the high radiological consequences threshold, vital areas need to be identified and protected as recommended in paras 5.20–5.42 of Ref. [1], using the design process described in paras 5.9–5.19 of Ref. [1]. If the radiological consequences fall between the unacceptable radiological consequences and high radiological consequences thresholds, the State may define graded protection requirements on the basis of the potential radiological consequences, and protection should be provided using the design process described in paras 5.9–5.19 of Ref. [1]. If the potential radiological consequences are below the unacceptable radiological consequences threshold, the operator should still protect safety related equipment and devices by controlling access to them and securing them, as recommended in para. 5.7 of Ref. [1]. The relationship between unacceptable radiological consequences and high radiological consequences and the levels of protection are represented in Fig. 1.

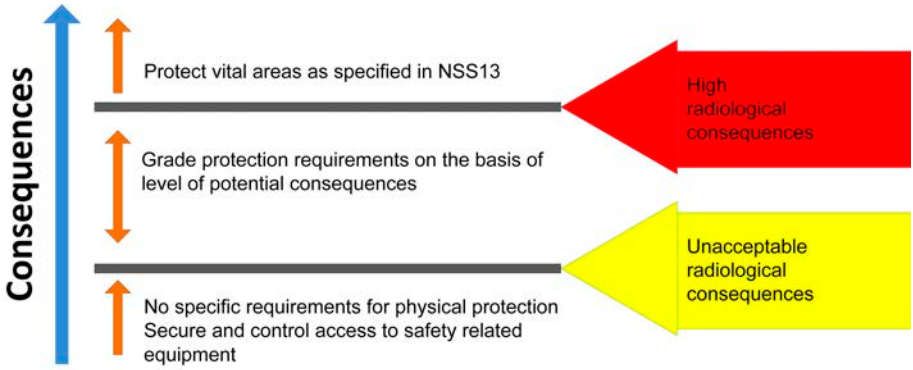


FIG. 1. Relationship between unacceptable radiological consequences and high radiological consequences and graded levels of protection. NSS13 — IAEA Nuclear Security Series No. 13.

Ranges of potential radiological consequences of sabotage

3.96. Assessment of the attractiveness of sabotage targets to potential adversaries is based on the State's thresholds for unacceptable radiological consequences and high radiological consequences and is independent of the category of nuclear material defined on the basis of the threat of unauthorized removal. The potential radiological consequences resulting from sabotage will depend on the inventory of radioactive material and the ease with which the material can be dispersed (which in turn will depend on the dispersal mechanism anticipated to result from the sabotage and the form of the material). Potential radiological consequences resulting from sabotage may be graded to reflect several ranges of severity, each range requiring correspondingly graded levels of protection.

3.97. The likelihood that a sabotage event will result in unacceptable radiological consequences at a nuclear facility depends on the characteristics of the facility (e.g. the type of installation and the facility's use, design, construction, operation and layout) and on the sabotage act itself. The factors that should be taken into account when determining whether or not unacceptable radiological consequences are possible at a facility include the characteristics described below (as applicable):

(a) The amount, type, physical form and status of radioactive material at the nuclear facility (e.g. solid or liquid form, in process or storage).
(b) The intrinsic risk (e.g. of criticality) associated with the physical processes and chemical processes that normally take place at the nuclear facility.

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

3.98. One method of developing a graded approach for protection against sabotage involves the State defining levels of radiation exposure at the boundary of the nuclear facility as thresholds for unacceptable radiological consequences and for high radiological consequences, together with the corresponding levels of performance required of physical protection applied to radioactive material that could, in the event of sabotage, give rise to radiological consequences at these levels. The operator is then required to carry out an assessment of all possible sabotage targets to determine for each target whether dispersal of the relevant inventory of radioactive material would cause radiological consequences above these defined levels. The outcome of this assessment is used to identify the levels of protection needed for different areas of the facility, taking into account the capabilities of the adversaries.

3.99. Table 2 shows another example of how graded physical protection levels for different ranges of potential radiological consequence might be set. This less sophisticated approach provides a starting point for developing a physical protection system against sabotage on the basis of consequence levels corresponding to the suggested emergency preparedness categories for facilities and activities described in IAEA Safety Standards on preparedness for a nuclear or radiological emergency [10–12]. The table is based on the assumption that the inventory of radioactive material that might be released during a sabotage attack increases as the thermal power level of the reactor increases. This approach is more applicable to the prescriptive approach of regulation.

3.100. Table 2 outlines three thresholds for the potential radiological consequences of sabotage as an example approach for ranking facilities. Using this table, a State may determine that the potential radiological consequences of sabotage of a nuclear power plant at consequence level A are high radiological consequences and would require the identification of vital areas [13]. Consequence levels B and C would represent unacceptable radiological consequences that are important, but of less concern than high radiological consequences, and physical protection systems for these levels of potential consequences may include a protected area. Further information about how to determine potential radiological consequences of sabotage for nuclear power plants is given in Ref. [14]. The methods described in Ref. [14] may be applied to other types of nuclear facility.

3.101. Reference [8] suggests that a design basis threat be developed and implemented whenever a State needs greater assurance that the physical protection of nuclear material and nuclear facilities is adequate to prevent unacceptable radiological consequences. In the example above, a design basis threat should be used when developing protection for consequence level A targets for which high radiological consequences may occur, as recommended in para. 3.37 of Ref. [1]. The design basis threat could also be used for consequence level B targets and for consequence level C targets at the discretion of the State.

Defence in depth[3]

> "**The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives. (FUNDAMENTAL PRINCIPLE I: *Defence in Depth*)**
>
> "3.45. State requirements for physical protection should be based on the concept of *defence in depth*. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures

[3] The term 'defence in depth' is used in this publication, as defined for nuclear security contexts in Ref. [1], to mean the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised. This definition describes a concept that is similar in principle to that of 'defence in depth' in safety, but it should be noted that the specific definition is not the same as that used in the IAEA Safety Standards Series.

TABLE 2. EXAMPLE OF GRADED APPROACH TO SABOTAGE PROTECTION REQUIREMENTS

Consequence level A	Consequence level B	Consequence level C *
Sabotage could give rise to severe deterministic health effects off-site, such as: — Facilities with inventories of dispersible radioactive material sufficient to result in severe deterministic effects off-site — Reactors with power levels exceeding 100 MW(th) (e.g. a nuclear power plant, a nuclear powered ship, a research facility) — Spent fuel pools that may contain some recently discharged fuel and a total of more than about 0.1 EBq of Cs-137 (equivalent to the inventory in a 3000 MW(th) reactor core)	Sabotage could result in doses to persons off-site that warrant urgent protective actions off-site, such as: — Facilities with inventories of dispersible radioactive material sufficient to result in doses warranting urgent protective actions off-site — Reactors with power levels of 100 MW(th) or less, but more than 2 MW(th) — Spent fuel pools requiring active cooling — Facilities with potential for uncontrolled criticality within 0.5 km of the site boundary	Sabotage could result in doses or contamination that warrants urgent protective action on-site, such as: — Facilities with inventories of radioactive material sufficient to result in doses warranting urgent protective action on-site — Facilities with potential, if shielding lost, of direct external (shine) dose rates of more than 100 mGy/h at 1 m — Facilities with potential for an uncontrolled criticality more than 0.5 km from the off-site boundary — Reactors with power levels of less than or equal to 2 MW(th)

* Potential consequences falling below level C call for protection at least in accordance with prudent management practices.

(including the organization of *guards* and the performance of their duties) and facility design (including layout)" [1].

3.102. The State should require that the defence in depth approach be followed in the design of the physical protection system for each of the functions of detection, delay and response. For each function, the system should be designed with independent capabilities so that the failure of one capability does not mean loss of that function. For example, detection may rely on observation by personnel and/or the use of electronic measures. Delay may be provided by multiple independent and diverse physical barriers that must be overcome to gain access to the target (such as fences, barricades and hardened buildings). Response may be provided by on-site guards and local police as well as on-site and off-site response forces.

3.103. Combining the graded approach with the application of defence in depth would require the use of more layers and more effective components in the physical protection measures (detection, delay and response) for theft targets in higher categories and sabotage targets with more significant potential consequences.

SUSTAINING THE PHYSICAL PROTECTION REGIME

3.104. Sustaining the nuclear security regime is one of the essential elements set out in IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [4]. Sustainability depends on those features that contribute to an enduring, effective nuclear security regime. Reference [1] recognizes four elements that particularly contribute to sustaining physical protection:

(a) Nuclear security culture: the definition of nuclear security culture explicitly includes the phrase "sustain nuclear security".
(b) Quality assurance: a process that provides confidence that the physical protection requirements are satisfied on a continuing basis.
(c) Confidentiality: the prevention of the disclosure of sensitive information that could compromise physical protection.
(d) Sustainability programme: a programme that specifically addresses the maintenance, resources and infrastructure — financial, human and technical — needed for effective physical protection.

Nuclear security culture

> "**All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization. (FUNDAMENTAL PRINCIPLE F: Security Culture)**" [1].

3.105. Guidance on nuclear security culture is provided in Ref. [15], in which nuclear security culture is defined as: "The assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security."

3.106. The development of a strong nuclear security culture involves individuals in a diverse range of disciplines and organizations who need to work together to be effective. All organizations need to apply the State's nuclear security policy, which is developed in harmony with the State's legal and regulatory framework. Organizations need to develop appropriate management structures, allocate sufficient resources and put in place appropriate management systems. The managers of these organizations have a key role to play in influencing culture through their leadership and management practices, which include motivating staff and seeking continuous improvement. The outcome of an effective nuclear security culture should be that all individuals adopt a strict and prudent approach to physical protection, are vigilant, have a questioning attitude and react quickly and correctly when the need to do so arises.

Quality assurance

> "**A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied. (FUNDAMENTAL PRINCIPLE J: Quality Assurance).**
>
> "3.52. The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements" [1].

3.107. A quality assurance programme provides a mechanism for acquiring data through a process or system, systematically comparing the acquired data with a standard and monitoring the process or system. The goal of the programme is to reduce errors and omissions. Quality assurance is one element of an integrated management system.

3.108. To ensure the continuous effectiveness of the established physical protection system, it is suggested that the competent authority and operators:

(a) Maintain the quality assurance aspects of the management policy and programme that are applicable to the physical protection of nuclear material and nuclear facilities against unauthorized removal and sabotage;
(b) Make their responsibilities on quality assurance known and understood in a statement of policy to demonstrate their commitment to it and, as appropriate, provide guidelines to staff, setting out the organization's objectives on quality;
(c) Design the management programme in such a way as to provide direct reporting on quality assurance to the highest management level in the organization;
(d) Develop management programmes for their respective organizations that require the identification and evaluation of deficiencies and the creation and tracking of corrective action plans.

3.109. It is suggested that operators have management programmes which ensure that physical protection systems designed to meet performance based requirements have adequate supporting documentation to demonstrate their effectiveness. This information is particularly important when establishing compensatory measures and implementing corrective actions. Such programmes should also ensure that nuclear security events will be reported in a timely manner to the competent authority (see paras 3.47 and 3.48).

3.110. It is also suggested that management programmes encompass all security related activities (technical, procedural and administrative) and be reviewed and updated periodically. Management programmes play a significant role in the configuration management of the physical protection system to ensure the continuity of these systems and provide a rationale for decisions to make changes.

Confidentiality

> "**The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which**

could compromise the physical protection of *nuclear material* and *nuclear facilities*. (Fundamental Principle L: Confidentiality)

> "3.53. The State should take steps to ensure appropriate protection of specific or detailed information the unauthorized disclosure of which could compromise the physical protection of *nuclear material* and *nuclear facilities*. It should specify what information needs to be protected and how it should be protected, using a *graded approach*" [1].

3.111. Guidance for States on information security is provided in Ref. [16]. According to this guidance:

> "2.5. Sensitive information is information, the unauthorized disclosure (or modification, alteration, destruction or denial of use) of which could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport. Such information may refer, for example, to the nuclear security arrangements at a facility, the systems, structures and components at a facility, the location and details of transport of nuclear material or other radioactive material, or details of an organization's personnel."

3.112. The State sets the information security requirements for the operator to meet; these requirements are based on guidance and policies from national security authorities. The State defines what constitutes sensitive information and, using a graded approach, defines associated information security requirements for the holders of such sensitive information. An example of a categorization scheme for nuclear security information is provided in Ref. [16].

3.113. Protecting the confidentiality, availability and integrity of information depends on applying security measures to sensitive information to ensure that it is not obtained or modified by unauthorized individuals or organizations. Information security includes the system, programme and set of rules in place to ensure the protection of information in any form. Information security includes, as a minimum, the following:

(a) Security of information on physical and electronic media;
(b) Security of computer based systems (computer security);
(c) Security of communication systems and networks;
(d) Security of information about facility employees and third parties (e.g. contractors, vendors);
(e) Security of intangible information (e.g. knowledge of the above).

3.114. Organizations with sensitive information should ensure that the State's information security policy is enforced and that all employees are fully aware of the need for security and follow their organization's rules.

3.115. Each organization needs to establish its internal policy, plans and procedures for protecting the confidentiality, integrity and availability of its sensitive information in compliance with the national information security policy.

3.116. Paragraph 3.54 of Ref. [1] states that:

> "Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

Information to be protected may include the location and characteristics of sabotage and theft targets, information about the design and operation of the physical protection system — including possible vulnerabilities in the protection system and certain aspects of nuclear material accounting and control — and details in the contingency plans of response force tactics and actions.

3.117. The State should clearly define the provisions that an operator should follow in ensuring the confidentiality of information relating to the physical protection system. These provisions should identify information that needs to be protected and the required level of protection commensurate with the sensitivity of the information and the consequences of its loss. The operator's measures to meet these provisions should be documented in the operator's security plan and periodically evaluated by the operator and the competent authority.

3.118. Paragraph 3.55 of Ref. [1] states that: "Sanctions against persons violating confidentiality should be part of the State's legislative or regulatory system." Information about sanctions against persons violating confidentiality should be communicated to individuals who are given authorized access to sensitive information and should be severe enough to act as a deterrent against such actions. States should make such offences punishable by appropriate penalties that take into account the potentially grave nature of those offences.

Sustainability programme

3.119. The State should ensure that the legal and regulatory framework supports the sustainability of the physical protection infrastructure, systems and measures as part of the nuclear security regime. Two good practices are for the State to provide the infrastructure for the training of both the State's and the operator's physical protection personnel and, whenever practical, to provide facilities for the testing and evaluation of physical protection equipment. Such testing can inform the State and the operators about practices to sustain physical protection measures and equipment at the necessary levels of performance.

PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

> "***Contingency* (emergency) *plans* to respond to *unauthorized removal* of *nuclear material* or *sabotage* of *nuclear facilities* or *nuclear material*, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned. (Fundamental Principle K: *Contingency Plans*)**" [1].

3.120. This fundamental principle may imply that contingency plans are the same as emergency plans. In practice, there are differences among States in the definition and use of these terms. In Ref. [1], the contingency plan is part of the overall nuclear security plan and relates to the response of physical protection personnel to nuclear security events involving malicious acts. In IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [10], the emergency plan relates to the response to a nuclear or radiological emergency, whether that emergency is caused by an accident or by a malicious act. However, the implementation of the contingency plan and the emergency plan will require a coordinated response of physical protection, nuclear material accounting and control, and safety personnel.

3.121. During the response to a nuclear security event, it is essential that all organizations involved in that response are prepared to respond appropriately at local and national levels. Measures that a State should take to plan and prepare for, and respond to, a nuclear security event are described in Ref. [4]. The State and the operator have shared and complementary responsibilities for planning and preparing for and responding to nuclear security events to locate and recover missing nuclear material and to mitigate and minimize the effects of sabotage. For actions to locate and recover nuclear material after a theft, the operator may

have limited authority outside the nuclear facility, and the State is therefore likely to have the primary responsibility for off-site response to the event. In this regard, the responsibilities need to be clearly assigned between the operator and other governmental organizations.

3.122. The goals of contingency planning are to ensure a timely and effective response at all levels to any nuclear security event comprising a malicious act that involves or is directed at a nuclear facility and to maintain physical protection during other events, such as an accident involving a release of radionuclides, a medical emergency or a natural disaster. The correct actions need to be taken and decisions made at the right time to adequately respond to the event and resolve the situation. In the event of a nuclear or radiological emergency, arrangements should be made to ensure the continued effectiveness of the physical protection system during the implementation of the emergency plan.

3.123. The State and the competent authority should ensure that the contingency plan contained in the operator's security plan is consistent with that developed at the State level. This consistency may be assisted by the development of agreements (written records, such as memorandums of understanding or other protocols) between the government entities involved in response and the operator; these agreements would clearly identify, for example, the roles and responsibilities of each entity. The necessary level of coordination could be achieved by, for example, conducting joint training and exercises using practice scenarios and the appropriate contingency plans.

3.124. The State, the appropriate competent authorities and the operator should have a comprehensive set of contingency plans that address different types of nuclear security event. Examples of such events that may require contingency plans are provided in Appendix I.

3.125. The State should ensure that exercises are conducted regularly to help verify the effectiveness of the contingency plans within the framework of the overall nuclear security regime. These exercises should include scenarios for both unauthorized removal and sabotage that are within the scope of the threat assessment or the design basis threat.

3.126. Additional guidance regarding the appropriate response for the location and recovery of nuclear material out of regulatory control (e.g. as a result of theft) is provided in Ref. [7].

4. DEVELOPING, IMPLEMENTING AND MAINTAINING AN INTEGRATED PHYSICAL PROTECTION SYSTEM FOR NUCLEAR FACILITIES

4.1. This section provides guidance on implementing the recommendations [1] addressed to the operator for the physical protection of nuclear material and nuclear facilities against unauthorized removal and sabotage. These recommendations are generally found in paras 3.23–3.30 and sections 4 and 5 of Ref. [1].

4.2. Reference [1] recommends implementing the physical protection requirements to protect against both the unauthorized removal of nuclear material and sabotage in an integrated manner, implying that the physical protection system should be a single system, effective against both threats. Furthermore, Ref. [1] recommends designing the physical protection system in a manner that will ensure effectiveness against whichever risk, unauthorized removal or sabotage, requires the more stringent physical protection requirements (paras 4.4, 5.3 and 5.17 of Ref. [1]).

4.3. This section provides a suggested approach to designing a single physical protection system effective against the threat of both unauthorized removal and sabotage. The phased approach to design presented in this section applies principles of systems engineering to physical protection — identifying physical protection requirements, designing systems to meet these requirements and evaluating the effectiveness of the resulting physical protection system — which are not covered in detail in Ref. [1]. There may be other ways to define elements of a systematic engineering approach for physical protection, but the process presented in this section is consistent with the methodology promoted by the IAEA and is intended to provide users with a basic framework for designing and implementing their physical protection systems.

GENERAL RESPONSIBILITIES OF THE OPERATOR

> "**The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of *nuclear material* or of *nuclear facilities* rests with the holders of the relevant licences or of other authorizing documents**

(e.g. *operators* or *shippers*). (FUNDAMENTAL PRINCIPLE E: Responsibility of the Licence Holders)

.....

"3.25. The *operator*, *shipper* and carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site *response forces*" [1].

4.4. In fulfilling these responsibilities, operators should comply fully with the provisions of the State's legal and regulatory framework. These provisions may require the operator to conclude agreements (such as memorandums of understanding, protocols or other types of written record) with local law enforcement, national police, military and other organizations, such as local and national emergency responders, intelligence and other domestic security organizations.

4.5. The operator has primary responsibility for the development and implementation of the physical protection system for nuclear material at its facilities. The operator should prepare a facility specific security plan (see paras 4.154–4.161). Appendix I provides a suggested format for the security plan.

4.6. Paragraph 3.30 of Ref. [1] states that:

"Whenever the *physical protection system* is determined to be incapable of providing the required level of protection, the *operator*, *shipper* and/or carrier should immediately implement compensatory measures to provide adequate protection. The *operator* and/or *shipper* should then — within an agreed period — plan and implement corrective actions to be reviewed and approved by the *competent authority*."

Compensatory measures are short term actions taken to compensate for degraded or inoperable security related structures, systems and components until they can be repaired or replaced. One approach to providing compensatory measures is to add extra guards and/or response forces to compensate for the deficiency as soon as it is identified. It is suggested that compensatory measures be documented and approved and that arrangements for necessary coordination between the State, the competent authority, the operator and the response forces be agreed before the measures are implemented.

4.7. Paragraph 3.28 of Ref. [1] states that:

> "For a *new nuclear facility*, the site selection and design should take physical protection into account as early as possible and also address the interface between physical protection, safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other."

Careful consideration needs to be given to the implications for nuclear security of the siting of nuclear facilities. Local infrastructure, site layout and other local conditions might all influence nuclear security. Site layout, particularly for nuclear facilities with multiple nuclear installations, may need to account for the space requirements of the physical protection measures to provide adequate defence in depth.

4.8. The design of new nuclear facilities should take into account the needs of nuclear security. Design approaches to achieving these ends are termed 'security by design'. Implementing such approaches may lead to reduced physical protection costs over the lifetime of the nuclear facility and may simplify the task of maintaining an effective physical protection system over that lifetime.

4.9. The intent of security by design is to design a new nuclear facility so that the required level of security is provided in a cost effective way that is compatible with operations, safety, and nuclear material accounting and control. Security by design is best implemented through a structured approach in which a State's nuclear security objectives are considered and fully taken into account in design decisions for the entire lifetime of the facility, starting with the planning of the facility and continuing through the design, construction, operational and decommissioning phases.

4.10. A good practice is to start integrating the design of the physical protection system into the overall design of the nuclear facility as early as possible in the process. Early consideration includes making decisions concerning the siting and layout of the facility, taking account of how those decisions may influence the design and effectiveness of physical protection systems. It is important to minimize conflicts with other design requirements while taking advantage of opportunities for complementary and synergetic design, for example by eliminating potential vulnerabilities by suitable engineering.

4.11. The highest levels of the operator's management need to be aware of and endorse the integration of physical protection measures into facility operations.

It is equally important that management encourages a strong nuclear security culture as described in Ref. [15] and discussed briefly in paras 3.105 and 3.106.

4.12. For an integrated approach to the implementation of physical protection, the operator of a nuclear facility identifies all potential targets for unauthorized removal and sabotage and implements all the required protection measures in a graded manner based on the State's regulatory approach. Depending on the type of nuclear facility, either the sabotage or the unauthorized removal targets may require a higher level of protection, but in all cases the appropriate levels of protection should be implemented for all targets. This approach is what is intended by the recommendation to apply the "more stringent applicable requirements" in paras 4.4 and 5.3 of Ref. [1].

4.13. Nuclear security considerations in the construction of nuclear facilities are not specifically addressed in the Recommendations publication [1]. However, good practice suggests that before construction, the operator (or applicant) should identify how physical protection will be implemented during all construction phases. If there is already a nuclear facility adjacent to the site on which the new facility is to be constructed, any additional physical protection measures to protect the existing, operating facility should be identified and implemented by both operators in close coordination before construction commences. (Similarly, if construction work is undertaken to extend or modify an existing nuclear facility, additional physical protection measures should be taken to protect the existing parts of that facility.) Safety and quality assurance audits can also be used to protect against sabotage by detecting any acts intended to facilitate future sabotage, such as the deliberate introduction of defects or hidden devices. At the end of the construction phase, a final assessment is suggested to confirm the effectiveness of the physical protection arrangements before commissioning commences.

SECURITY ORGANIZATION

4.14. The duties and responsibilities for security should be established within the framework of the integrated management system and may be divided into three complementary units:

(a) A security management unit that has the overall responsibility for physical protection and includes managers who interface with the competent authority and the facility management (including human resource managers),

planners who are responsible for developing and maintaining the security plan, designers who are responsible for designing or updating the physical protection system to satisfy the competent authority's requirements, and analysts who are responsible for evaluating the performance of the physical protection system against the design requirements. The allocation of responsibilities for safety–security interfaces is also part of security management (see paras 4.147–4.153).

(b) A security operations unit that is responsible for security relating to personnel and visitors (trustworthiness and access authorization), information security, computer security, and the guards and response forces (in accordance with responsibilities assigned by the State) whose duties include access control and escorting, central alarm station operation, patrols and response to nuclear security events.

(c) A technical security unit that includes technical staff — who conduct installations and upgrades, performance testing (assisted as appropriate by security operations staff), preventive maintenance, unscheduled repairs and replacement — and provides support and input to the security management and security operations units as appropriate.

PROCESS FOR DEVELOPING AND IMPLEMENTING A PHYSICAL PROTECTION SYSTEM

4.15. This section outlines the approach for designing, developing and implementing a physical protection system for the construction of a new nuclear facility (and the construction of new installations on existing nuclear facilities), upgrading existing physical protection systems and reviewing the effectiveness of existing physical protection systems.

Approach for developing the physical protection system

4.16. The development of the physical protection system is best achieved using a systematic approach that consists of three phases. These three phases are:

(1) Identify the objectives and requirements for the physical protection system.
(2) Design the physical protection system to meet the objectives and requirements as identified in Phase 1.
(3) Analyse and evaluate the effectiveness of the physical protection system designed in Phase 2 in meeting the objectives and requirements identified during Phase 1.

The sequencing of these three phases and a broad summary of the activities under each phase are illustrated in Fig. 2.

4.17. Applying these three phases, which are discussed in more detail below and in paras 4.23–4.59, will produce a physical protection system design to protect against the threats of unauthorized removal and sabotage of nuclear material and meet any other facility specific objectives that may apply.

Physical protection system life cycle

4.18. After the physical protection system has been designed and evaluated using this development process, the next steps in the physical protection system life cycle are to implement the design; to operate, maintain and sustain the resulting physical protection system; and to plan appropriate redesign(s) of the physical protection system based on changes in the threat, the facility configuration, operations or potential targets, or based on performance monitoring. These life cycle steps are illustrated in Fig. 3.

Sustaining the physical protection system

> "3.57. *Operators*…should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:
>
> — Operating procedures (instructions).
> — Human resource management and training.

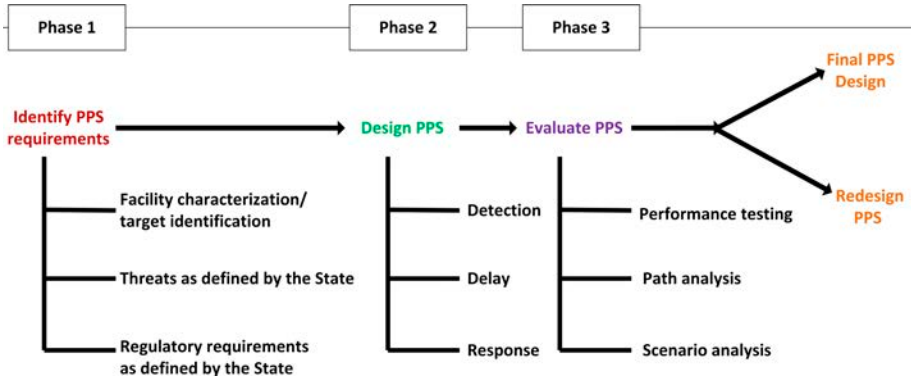


FIG. 2. Process for designing and evaluating the physical protection system. PPS — physical protection system.

— Equipment updating, maintenance, repair and calibration.
— *Performance testing* and operational monitoring.
— Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
— Resource allocation and operational cost analysis" [1].

4.19. Taking into account the State's approach to sustaining the nuclear security regime, operators should ensure that the necessary resources — trained and knowledgeable personnel, reliable equipment, associated infrastructure, quality assurance and funding — are provided to sustain their physical protection systems as part of a sustainability programme.

Meeting the State's requirements

4.20. Before beginning the three phase process shown in Fig. 2, the operator or applicant should understand the relevant aspects of the State's nuclear security regime, as covered in Section 3. Of particular relevance are several aspects that affect how the operator or applicant designs the physical protection system and applies for State approval of the design. Such aspects include:

(a) The legislative and regulatory framework of the State, including the regulatory approach selected by the State for specifying requirements to

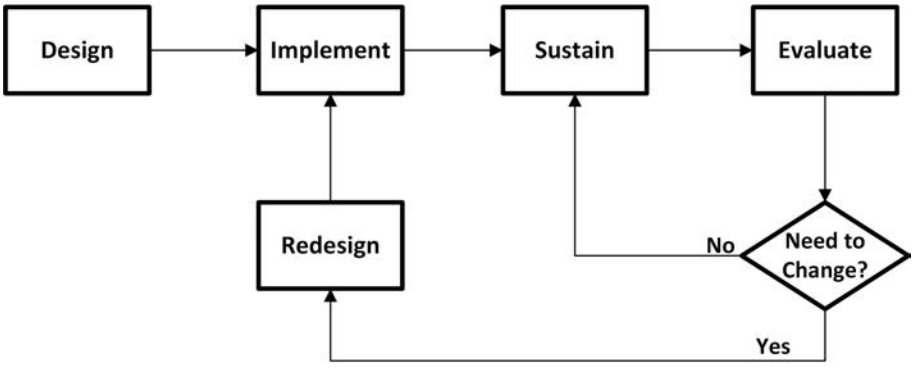


FIG. 3. Physical protection system life cycle.

address the threat as defined in paras 3.12–3.26, and the implementation of the State's trustworthiness policy;

(b) The requirements specified by the State on the basis of a graded approach, as described in paras 3.70–3.73;

(c) The licensing process for approving applications for new licences and renewals or amendments to existing licences, as described in paras 3.33–3.37.

4.21. Depending on the regulatory approach adopted by the State — the performance based approach, the prescriptive approach or the combined approach (as described in paras 3.18–3.26) — the operator's or applicant's approaches for meeting the requirements will be different.

4.22. Figure 4 shows tasks that the operator or applicant should perform, depending on the regulatory approach. For a combined approach, it will be necessary to follow both flows as appropriate. Figure 3 describes how the design is developed and evaluated; Fig. 4 depicts other activities that the operator or applicant performs and approvals that the State gives.

IDENTIFYING THE REQUIREMENTS FOR A PHYSICAL PROTECTION SYSTEM (PHASE 1)

4.23. Phase 1 in the development and evaluation of a physical protection system design by the operator or applicant is to determine how the State's requirements for physical protection apply to the specific site, nuclear facility and physical protection system. The operator or applicant needs to perform several steps in this determination:

(a) Characterization of the facility operations and conditions. This step involves describing the processes and operations within the facility; developing a thorough description of the facility, including the locations of the facility boundary and buildings, floor plans, structure elevations and access points; and, for an existing facility or design, identifying existing features or systems that may be used as elements of the physical protection system. Information about the facility can be drawn from all relevant sources, including existing documentation such as facility drawings and process descriptions, and from observations of the facility and interviews with staff. Physical protection system designers will need detailed knowledge of this information, as well as any facility specific constraints (such as safety constraints) that may be encountered during design.

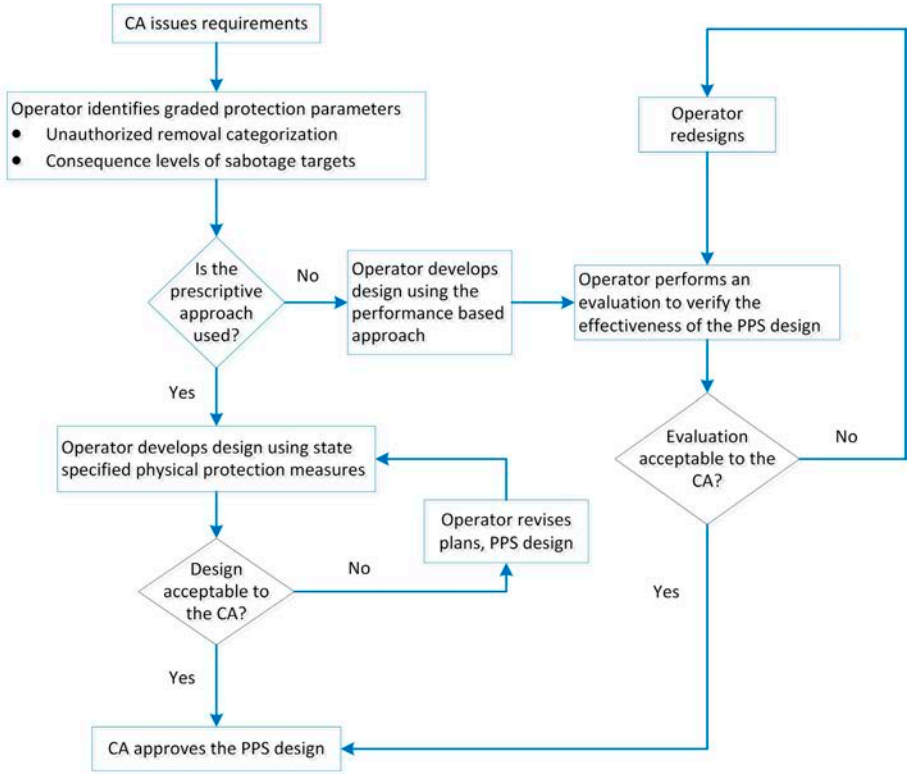


FIG. 4. Physical protection system design process. CA — competent authority; PPS — physical protection system.

(b) Interpretation of the information on the threat provided by the State to the operator or applicant to serve as the basis of the design (see paras 3.55–3.63). This step is specific to the performance based or combined approach. (In the prescriptive approach, the State usually does not provide threat information to the operator.)

(c) Identification of the targets, and their locations in the facility, that need to be protected from the adversary as defined by the State on the basis of its categorization of nuclear material and/or the potential consequences of sabotage (see paras 3.74–3.101).

4.24. Capabilities of the adversary defined by the State need to be countered by the physical protection system, and hence need to be considered by the operator or applicant. These capabilities include:

(a) Knowledge of the physical protection system;
(b) Skills that would be useful in an attack;
(c) Tools and weapons that could be used in an attack.

Target identification

4.25. Target identification determines which material and/or equipment needs to be protected from the adversary. The four steps in the process of target identification are to:

(a) Understand the physical protection objectives.
(b) Identify the types of nuclear and other radioactive material, as well as the systems important to safety (including computer based systems and information), that need to be protected from unauthorized removal and/or sabotage.
(c) Identify the appropriate categories of nuclear material and/or the potential consequences of sabotage that apply to each target.
(d) Develop a target list for the facility, including a description of each target to be protected, its category and location. The target list should be protected as sensitive information.

4.26. Recommended protection measures for each category of nuclear material are specified in paras 4.9–4.49 of Ref. [1].

4.27. For the identification of sabotage targets, the State should first determine the threshold levels of the potential radiological consequences that it considers appropriate to define as unacceptable radiological consequences and high radiological consequences (see paras 3.91–3.101).

4.28. Paragraph 5.4 of Ref. [1] states that:

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

This analysis addresses two types of sabotage that may lead to unacceptable radiological consequences, namely direct and indirect sabotage, as discussed in Ref. [14]. Direct sabotage introduces energy from an external source, such as

conventional explosives, to disperse nuclear or other radioactive material; indirect sabotage uses energy from processes within the nuclear or other radioactive material (e.g. heat from fission or radioactive decay), for example by damaging the cooling systems of a reactor core.

4.29. A conservative analysis should be performed to determine the potential radiological consequences that could arise from the complete release of the inventory of nuclear or other radioactive material in each identified sabotage target at the facility. For the indirect sabotage of nuclear material, this inventory may include fission products generated by the nuclear chain reaction.

4.30. Nuclear facilities are subject to extensive safety analysis to demonstrate that their operations are safe. The information in safety analysis reports may be useful in identifying structures, systems and components that need to be protected against sabotage. It is also important to consider other possible causes of failure due to malicious acts.

4.31. The assessed potential radiological consequences for sabotage targets are then used to determine physical protection requirements for those targets, as follows:

(a) If potential radiological consequences exceed the high radiological consequences threshold, then vital areas should be identified and protected.
(b) If potential radiological consequences fall between the unacceptable radiological consequences and high radiological consequences thresholds, then the State will specify graded protection requirements based on the level of potential consequences.
(c) If radiological consequences fall below the unacceptable radiological consequences threshold, then there may be no specific requirements for physical protection, but the operator should still secure and control access to safety related equipment and devices.

Threat definition

4.32. As part of the identification of the objectives and requirements for the physical protection system, the threat to the facility should be defined by the State through either a threat assessment or by developing a design basis threat. Relevant information should be provided to the operator, who should use this information as a basis for designing and evaluating the physical protection system.

4.33. After the objectives and requirements for the physical protection system are identified (Phase 1), the operator or applicant knows the objectives of the physical protection system: what to protect (targets), against what (threat), and how well (requirements). The next step (Phase 2) is to design the new system or redesign the existing system to provide physical protection measures for detection, delay and response sufficient to meet the objectives of the system. After the physical protection system is designed or characterized, it should be analysed and evaluated (Phase 3) to ensure that it meets the physical protection requirements. Evaluation should be based on the overall effectiveness of the system, as indicated by the effectiveness with which the different measures work together to ensure protection.

Design phase (Phase 2)

General design considerations

4.34. During this phase, the designer determines how best to combine physical protection measures such as fences, vaults, sensors, procedures, communication devices and response forces into a physical protection system that can satisfy the protection requirements. This determination takes into account safety and operational considerations so that physical protection and safety objectives are met. The overall objective is to ensure that the physical protection system fulfils the protection requirements by providing an appropriate balance between the functions of detection, delay and response.

4.35. Figure 5 illustrates the design principles and shows the timeline used to determine whether, for a defined physical protection system, the response force will be reliably notified early enough to respond before the adversary carries out all of the tasks needed to complete a specified malicious act. The top line depicts the time sequence of the adversary's attack and the opportunities along the adversary's path to the target for the physical protection system to sense the adversary's presence. The 'physical protection system response time' is portrayed on a timeline lower in the diagram: this timeline measures the time from the first successful sensing (see paras 4.62–4.67) of adversary activity at T_0 until the adversary can be interrupted at T_I. In this diagram, sensing occurs early enough to allow the adversary to be interrupted by the response force before the time T_C, when the adversary would have successfully completed the attack.

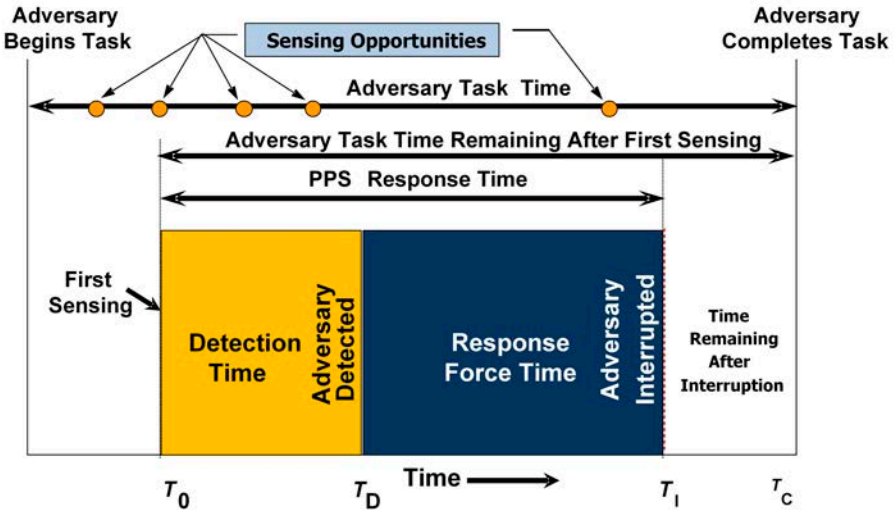


FIG. 5. Comparison of adversary and response timelines. PPS — physical protection system.

4.36. Good practice in the design of physical protection measures includes the provision of:

(a) Defence in depth, such that the adversary needs to deceive, avoid or defeat several protection measures in sequence to succeed. Defence in depth is generally implemented by placing a series of layers of protection around targets, which may include a combination of physical measures (e.g. controls on access to areas; see paras 4.86–4.89) and administrative measures (e.g. protection of sensitive information and implementation of a trustworthiness policy). This approach may involve taking advantage of the strengths of each physical protection component and using equipment in combinations that complement the strengths or compensate for the limitations of each other.

(b) Balanced protection, such that the adversary encounters comparably effective measures of the physical protection system whenever, wherever or however the malicious act is attempted.

(c) Robustness, meaning that the physical protection system will have a high probability of operating effectively during a wide range of types of adversary attack, which is typically accomplished by incorporating redundancy and diversity into the design.

4.37. The time needed for adversaries to achieve their goal is the ‘adversary task time’ (see Fig. 5). The primary role of barriers is to increase the adversary

task time by introducing impediments along any path the adversary may choose. An adversary should have to penetrate or bypass several separate barriers before gaining access to a particular target. The time involved in penetrating or bypassing each of these barriers need not necessarily be equal, but the barriers should be selected so that each necessitates a separate and distinct act as the adversary moves along the path. The effect produced on the adversary by a physical protection system that is designed to provide defence in depth will be to:

(a) Increase the adversary's uncertainty about the physical protection system;
(b) Require additional tools and more extensive preparations before attacking the physical protection system;
(c) Create additional steps that may cause the adversary to fail or to abandon the attack.

4.38. For detection and assessment systems, robustness can be achieved by a combination of multiple complementary sensors and human surveillance. To be complementary, sensors at a particular layer or barrier are chosen so that attempts to defeat one sensor are detectable by the others and different sensors do not respond to the same sources of nuisance alarms. Adding random or continuous human surveillance adds to the adversary's uncertainty about the physical protection system, making planning and executing a successful attack more difficult.

4.39. The design of the physical protection system needs to be compatible with the facility's operations systems important to safety and to allow staff to carry out their duties in a safe and secure manner. If there are physical protection measures that make it difficult for staff to complete their tasks, the staff may find ways of circumventing those measures. A thorough understanding of the operations of the nuclear facility, applied during the design of the physical protection system, will help in balancing the needs of physical protection with those of safety and operations.

4.40. The design approach described above was developed for and is applied to protection against external adversaries. Additional and/or different factors need to be considered in designing a physical protection system against insider threats.

Additional design considerations for insider threats

4.41. An insider is defined as one or more individuals with authorized access to nuclear facilities or related sensitive information who could attempt unauthorized removal or sabotage or who could aid an external adversary to do so. An insider

threat is an insider with an intention to carry out such an act. Insiders may include managers, regular employees, contractors and service providers, inspectors and some visitors. An insider may therefore be in any position at a facility and may have authorized access to any of the controlled areas or materials.

4.42. The capabilities of an insider are typically defined by three attributes:

(a) Extent of authorized access: which areas of the facility the insider may or may not enter during different facility states (e.g. normal work, non-operational periods, maintenance outages) or during a security or safety event;
(b) Level of authority over other people or over certain tasks and equipment;
(c) Knowledge of targets, facility layout, the physical protection system, and/or how to acquire and operate special tools and equipment found at the facility.

4.43. Insider threats present different problems from external adversaries because they can take advantage of these insider attributes to bypass some technical and administrative physical protection measures to commit or facilitate unauthorized removal or sabotage. Insiders can also complete their contributions to a malicious act through a series of separate actions over an extended period of time, which may reduce their chance of detection and therefore increase their likelihood of success. Insiders may also have more knowledge and/or opportunity to select the most vulnerable target and the best time to perform the malicious act.

4.44. To protect the targets against malicious acts consistent with the State's threat assessment or design basis threat, the design of the physical protection system should include features to deny access by unauthorized persons or equipment to the targets and to minimize the opportunity of insiders who have such access to commit malicious acts. For example, the presence of barriers, in combination with an effective response force, may serve to deny external adversaries access to targets, whereas locking a piece of equipment associated with the target may create a delay even for insiders who have authorized access to the area within which it is located and may be especially effective if the area is under continuous surveillance.

4.45. Reference [9] presents a systematic approach for protecting against insider threats, including preventive measures to minimize the insider's opportunity to initiate or assist a malicious act and protective measures to detect, delay, respond to and mitigate the effects of an act committed by an insider.

4.46. Protective measures to counter an insider threat attack scenario begin with detection of the attack by one or more available sources, including physical protection measures, process controls, safety alarms, alarms generated by the facility's nuclear material accounting and control system, and observation by co-workers or supervisors.

Evaluation phase (Phase 3)

> "3.29. The *operator* should develop and implement means and procedures for evaluations, including *performance testing*, and maintenance of the *physical protection system*" [1].

4.47. During Phase 3, the design of the physical protection system from Phase 2, whether for a new or an existing system, is evaluated to determine whether it meets the requirements identified in Phase 1. Reasons for evaluating the physical protection system may include:

(a) Verifying that the physical protection system as designed, or as characterized (for an existing system), satisfies the physical protection requirements;
(b) Identifying any system deficiencies in the design or implementation that need to be addressed to meet the system requirements;
(c) Analysing possible upgrades that may be necessary to address identified deficiencies and improve system performance (including such upgrades needed because of a change in the threat);
(d) Repeating the evaluation of physical protection system effectiveness on an annual or other regular basis to take into account any changes in targets or the facility.

4.48. The physical protection system provides detection, delay and response functions through structural, technical and personnel elements. The interaction of these elements with the equipment and procedures makes the evaluation of physical protection system effectiveness a challenging task.

4.49. In the evaluation phase, data are collected on the performance of physical protection system measures and used to evaluate the overall effectiveness of the physical protection system.

Physical protection evaluation and performance testing by the operator

4.50. Reference [1] emphasizes the evaluation and performance testing of the physical protection system; for example:

(a) Operators should "develop and implement means and procedures for evaluations, including *performance testing*" (para. 3.29 of Ref. [1]).
(b) For Category I and II nuclear material: "Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces* should be conducted regularly" (para. 4.35 of Ref. [1]).
(c) For Category I nuclear material: "At least annually, *performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*…" (para. 4.49 of Ref. [1]).
(d) For the sabotage of targets with the potential to result in high radiological consequences:

"Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces*, should be conducted regularly…. *Performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*…" (para. 5.41 of Ref. [1]).

4.51. These provisions suggest that the operator plans, carries out and documents the evaluation and performance testing of the physical protection system in a manner designed to satisfy the regulatory requirements. Appropriate parts of this evaluation and testing should be considered throughout the lifetime of the nuclear facility (i.e. during design, construction, licensing, operation, changes or upgrades, and decommissioning and management of radioactive waste and spent fuel).

4.52. The operator should consider using independent experts to review its system evaluation and performance testing for Category I nuclear material and for sabotage with the potential to cause high radiological consequences.

Methods for system evaluation

4.53. Several performance based approaches are available to evaluate the effectiveness of the physical protection system against insiders and external adversaries. Performance based evaluation methods include:

(a) Path analysis. This evaluation method involves building timelines, such as the one shown in Fig. 5, for different credible paths that the adversary might attempt to take to reach the target. On the basis of the timeline, the analysis determines whether there is high assurance that the attack will be

detected while there is enough of the adversary task time remaining for the response force to interrupt the adversary. Typically, the task times and the response times are measured or estimated quantitatively and the measures of the effectiveness of the detection features are probabilistic estimates based on performance tests.

(b) Simulations. This evaluation method includes computer based simulations of the physical protection system and tabletop exercises that allow consideration of the effectiveness of security and contingency plans as bases for response in the face of simulated decisions by the adversary and facility response forces. These tools are typically used to evaluate the overall performance of the physical protection system in detecting, interrupting and neutralizing simulated adversaries, taking all measures into account. Simulations may also be used to focus on specific aspects, such as the effectiveness of the response force in neutralizing the adversary (i.e. preventing the adversary from completing the act after detection and interruption).

(c) Exercises. This evaluation method ranges from limited exercises of specific elements of the physical protection system, such as response to an alarm, to force-on-force exercises that address the effectiveness of the entire physical protection system against a simulated adversary attack. Simulations may fail to reflect significant practical aspects of response and may miss important aspects of attack scenarios. Simulations therefore cannot fully replace exercises involving facility personnel and response forces on the ground.

4.54. Simulations and exercises are typically performed as part of scenario analysis, in which different postulated attacks ('scenarios') are identified, specified in detail, and then simulated or used as a basis for exercises to determine how effectively the physical protection system functions in each scenario. Scenario analysis typically builds on path analysis by considering specific methods that an adversary might use to defeat sensors, barriers and communication systems or to divert or eliminate part of the response force. Subject matter experts typically develop the scenarios, and then the exercises and/or simulations are used to qualitatively or quantitatively determine system effectiveness. Scenario analysis may use information about the path timelines created during path analysis.

4.55. Scenario analysis may include scenarios involving the collusion of insiders with external adversaries, to the extent that such scenarios fall within the scope of the design basis threat or threat assessment. Evaluations against external threats include consideration of adversary attributes, such as the numbers of attackers, their equipment (including weapons and explosives) and their skills that might

help them to defeat physical protection measures. Typically, the use of specialized tools is included in the path analysis.

4.56. System effectiveness can be measured either quantitatively or qualitatively. The State should decide which approaches should be used for different types of targets, threats and scenarios. It is suggested that the required level of overall physical protection system effectiveness be defined conservatively as the lowest level of quantitative or qualitative effectiveness of the physical protection system that still meets regulatory objectives, when all credible adversary paths and scenarios have been considered.

4.57. Two general classes of scenario address the two threats: unauthorized removal and sabotage. For unauthorized removal, the adversary needs to gain access to the location of the target material and then to remove the nuclear material to a location off-site. In the case of Category I nuclear material, an effective response strategy would be to deny access to the nuclear material or, if access is achieved, to contain the adversary before the nuclear material leaves the site. For sabotage, the adversary needs to gain access to the target material and/or vital areas and then directly sabotage the material or indirectly cause a release of radionuclides by sabotaging equipment. In this case, a response strategy would be to deny access to the material or equipment at least for the length of time that would be needed to complete the sabotage act.

Additional evaluation considerations for insider threats

4.58. Evaluations should also include analysis of the vulnerability of the physical protection system to insider threats. Guidance for performing such evaluations is provided in Ref. [9]. For analysis purposes, insider threats may be categorized by whether they are passive (e.g. the gathering of sensitive information only) or active, and if they are active by whether or not the insiders are willing to use force against a target or person. Taking into account the threat assessment or design basis threat, the evaluation may include consideration of the possibility of an insider colluding with another insider or with external adversaries.

4.59. Scenarios involving a sequence of actions by an insider threat may be used to determine the effectiveness of the facility's protection against insider threats. Adversary path timelines may be suitable only for evaluating insider threat attack scenarios involving a continuous series of actions, which can be evaluated in a similar way to external threats. The path timeline for an active insider might represent a continuous series of tasks, similar to the timeline for an external adversary (see Fig. 5), or a non-continuous series of tasks, in which

some tasks are separated by a significant interval of time and/or are carried out at different locations. An example of a scenario with a continuous timeline is abrupt theft, where the insider attempts to complete the theft of nuclear material in an uninterrupted series of actions. An example of a non-continuous insider threat attack scenario is protracted theft, where the insider attempts to acquire a significant amount of nuclear material through a series of separate thefts of small amounts over a period of several days or weeks.

KEY FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM

4.60. The physical protection system meets physical protection requirements and accomplishes physical protection objectives by deterrence and a combination of detection, delay and response. Reference [17] provides additional, more detailed guidance on these key functions of a physical protection system.

Deterrence

4.61. Deterrence is achieved if potential adversaries regard a facility as an unattractive target and decide not to attack it because they estimate the probability of success to be too low (or the potential negative consequences for themselves to be too high). To promote deterrence the operator may use observable protection measures, such as a visible presence of guards patrolling the facility, bright lighting at night, bars on windows and vehicle barriers. Deterrence may be helpful in discouraging attacks, but the effectiveness of deterrence is difficult, if not impossible, to measure. Furthermore, making physical protection measures and personnel observable may increase their vulnerability to adversary actions.

Detection

4.62. Detection is a process in a physical protection system that begins with a potentially malicious or otherwise unauthorized act or the presence of an adversary being sensed and an alarm being raised. The process is completed when the cause of the alarm has been assessed.

4.63. Figure 6 shows the sequence of events associated with detection and illustrates that detection is not a single, instantaneous event. An action by a potential adversary is only considered to have been detected when all the steps in the sequence have occurred. Information needed for the accurate assessment of alarms includes details such as who (or what) triggered the alarm, what specific activity triggered the alarm, where the activity took place, and how many

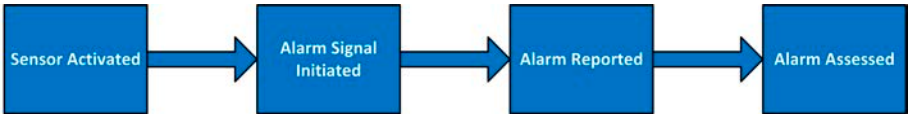


FIG. 6. Detection function in a physical protection system.

people may be involved. The first three steps in Fig. 6 — sensor activated, alarm signal initiated and alarm reported — compose 'sensing'; the final event, alarm assessed, completes the detection process.

4.64. The detection sequence starts when a sensor of some kind is activated by any cause. Activation of a sensor may mean the triggering of a hardware sensor (e.g. a radiation monitor or motion sensor) in the physical protection system or the reporting of something suspicious by an individual, such as a guard.

4.65. The effectiveness of the physical protection system in performing the detection function depends on the capabilities of the systems for sensors, alarm signal activation, alarm reporting and assessment, as well as the performance of the staff of the central alarm station and any guards or response force members who have a role in detection. Technology can increase the efficiency of all stages of the detection process. Where technology is used, the detection system should employ sensors and video systems to provide data on sensing and assessment.

4.66. The effectiveness of detection is a function of both the probability of detection and the time needed for detection to be completed. The probability of detection consists of the probabilities that the action is sensed, that the alarm is generated and reported, and that the alarm is then correctly assessed. The detection time (from T_0 to T_D; see Fig. 5) is the sum of the times for the four steps in Fig. 6 to occur. The shorter the detection time, the more likely it will be that the cause of the alarm can be assessed and the guards deployed in time to interrupt the adversary, if needed.

4.67. Detection may also be triggered by access control measures, for example in the case of the attempted unauthorized entry of persons, vehicles or prohibited items, or the attempted unauthorized removal of nuclear material.

Delay

4.68. Delay is the function of the physical protection system that seeks to slow an adversary's progress towards a target, thereby providing more time for effective

response. Delay can be accomplished simply by distances and areas that have to be crossed and by barriers that need to be defeated or bypassed, such as fences, gates, portals, doors, locks, cages and activated delay systems. Barriers may deter or defeat adversaries if they are unable to penetrate the barrier. Each type of barrier takes time for the adversary to penetrate or defeat. These delay times are factors to be considered when designing the physical protection system. Guards or response forces may provide further delay if they are appropriately positioned, armed and protected.

4.69. The primary measure of the effectiveness of a delay element in the physical protection system is the time needed by the adversary, after detection, to defeat the measure providing the delay. Any delay that the adversary encounters prior to detection is of no value to the effectiveness of the physical protection system because such a delay does not provide additional time to respond to the adversary. (External barriers may also serve other purposes, such as deterrence or mitigation of the effects of stand-off attacks.) Delay is an especially important function in cases in which the response forces are not routinely located nearby and sufficient delay needs to be provided for the response force to prevent completion of the malicious act.

Response

4.70. Response is the function of the physical protection system that seeks to interrupt and neutralize an adversary before the completion of a malicious act. Guards are assigned responsibility for controlling access, escorting individuals, monitoring and assessing alarms in the central alarm station, patrolling and/or providing the initial response on detection of a potential adversary. These guards may or may not be prepared or permitted to provide an armed response. The response force consists of persons on-site or off-site who are armed and appropriately equipped and trained to interrupt and neutralize an adversary attempting unauthorized removal or an act of sabotage.

LOCATING AND RECOVERING MISSING OR STOLEN NUCLEAR MATERIAL

4.71. The operator should, depending on the State's legal and regulatory framework, perform a number of steps in support of measures to locate and recover missing or stolen nuclear material, detailed in Ref. [1] as follows:

"4.57. The *operator* should ensure that any missing or stolen *nuclear material* is detected in a timely manner by means such as the *system for nuclear material accountancy and control* and the *physical protection system* (e.g. periodic inventories, inspections, access control searches, radiation detection screening).

"4.58. The *operator* should confirm any missing or stolen *nuclear material* by means of a rapid emergency inventory as soon as possible within the time period specified by the State. A *system for nuclear material accountancy and control* should provide accurate information about the potentially missing *nuclear material* in the facility following a *nuclear security event*.

"4.59. The *operator* should notify the *competent authority* and other relevant State organizations of missing or stolen *nuclear material* as specified by the State.

"4.60. The *operator's* measures to locate and recover missing or stolen *nuclear material* should be included in its *contingency plan* and should be regularly tested and evaluated. Appropriate joint exercises should be held with the *competent authority* and other State organizations.

"4.61. The *operator* should take all appropriate measures to locate, as soon as possible, any declared missing or stolen *nuclear material* on-site and possibly off-site (in hot pursuit) in accordance with the legal and regulatory framework and the *contingency plan*.

"4.62. As soon as possible after the missing or stolen *nuclear material* has been located and identified, the *operator* should, in accordance with the *contingency plan*, secure this material in situ and then return it to an appropriate *nuclear facility* with due authorization from the *competent authority*.

"4.63. The *operator* should provide any other necessary assistance to the State organizations to locate and recover *nuclear material* and should cooperate during subsequent investigations and prosecution."

4.72. The first step for the location and recovery of missing and/or stolen nuclear material is to detect that the nuclear material is not in its authorized location. For example:

(a) The physical protection system may detect an adversary attempting to steal nuclear material, and if the physical protection system is not successful in preventing this act, then nuclear material may be removed from the facility.
(b) The nuclear material accounting and control system may detect that nuclear material is missing during operations, inventory taking or inspection.
(c) Searches at access control points or radiation screening may detect that nuclear material is being removed in an unauthorized manner.
(d) Facility personnel may observe and detect that someone is attempting to remove nuclear material.

4.73. After it has been detected that nuclear material is not in its authorized location, the operator should take actions to confirm the amount(s) and type(s) of missing nuclear material as soon as possible. After the operator has confirmed that nuclear material is no longer in its authorized location, the relevant competent authorities within the State should be promptly notified. In accordance with the contingency plan, the operator may then continue an on-site search for the material and may also initiate an off-site search, as appropriate, in coordination with the relevant competent authorities. In some cases, these searches may require activation of emergency plans [10, 12]. The area where the missing or stolen material was previously located should be secured and treated as a possible crime scene. The continued physical protection of other nuclear material should also be verified.

4.74. All response actions should be conducted in accordance with the contingency plan and coordinated with the appropriate competent authorities. When the nuclear material is located, the operator or another appropriate party should secure it and return it to an appropriate location. Securing and returning the material will need to be done in close consultation with all relevant competent authorities, including law enforcement agencies, particularly if a criminal investigation has been or is likely to be initiated.

4.75. Arrangements for the coordination of recovery operations and protocols should be set out in detail in the contingency plans and should be coordinated, as necessary, with emergency plans. It is suggested that a follow-up review be conducted after any loss of material and that lessons learned from the response be incorporated into the modification of the contingency plans.

MITIGATING OR MINIMIZING RADIOLOGICAL CONSEQUENCES OF SABOTAGE

4.76. The response to a sabotage event may involve many competent authorities, possibly including the competent authorities responsible for response to a nuclear or radiological emergency, whether the emergency is due to an accident or an act of sabotage. To be effective, the response to a sabotage event should be appropriately integrated and coordinated with the response to any resulting emergency [10].

4.77. The operator has the following responsibilities in support of measures to mitigate or minimize the radiological consequences of sabotage, as set out in Ref. [1]:

> "5.54. The *operator* should establish a *contingency plan*.
>
> "5.55. The *operator* should prepare facility personnel to act in full coordination with *guards*, *response forces*, law enforcement agencies and safety response teams for implementing the *contingency plans*.
>
> "5.56. The *operator* should assess, on *detection* of a *malicious act*, whether this act could lead to radiological consequences.
>
> "5.57. The *operator* should notify, in a timely manner, the *competent authority*, *response forces* and other relevant State organizations of *sabotage* or attempted *sabotage* as specified in the *contingency plan*.
>
> "5.58. Immediately following an act of *sabotage*, the *operator* should take measures to prevent further damage, secure the *nuclear facility* and protect emergency equipment and personnel."

4.78. Any responders to the sabotage act need to be knowledgeable about the safety hazards (e.g. radiation exposure) that exist within the nuclear facility and how these hazards might be affected by the sabotage. The responders also need to comply with all relevant safety measures.

4.79. Contingency plans need to identify the roles and responsibilities of all relevant bodies involved in the response to an act of sabotage and include, for example, provisions that:

(a) The on-site response is promptly initiated and is managed without impairing the continuing performance of operational safety and physical protection functions.
(b) The off-site response is effectively managed and coordinated with the on-site response.
(c) The information necessary for making decisions on the allocation of resources is appraised throughout the event.

4.80. The operator should include in its contingency plan measures that focus on preventing further damage to the target and other parts of the facility, securing the nuclear facility and protecting emergency equipment and personnel.

4.81. Contingency plans should be developed and deployed to help limit the consequences of a sabotage attack. Response to the sabotage and response to a resulting emergency may involve actions in the same places and at the same time, but with different goals. Therefore, it is necessary for contingency plans and emergency plans to be complementary and jointly exercised regularly to help ensure their effectiveness and compatibility. Care needs to be taken to verify that activities of the response forces do not adversely affect safety and that physical protection is not adversely affected during the implementation of safety measures. An example of a contingency plan is contained in Appendix II.

4.82. The emergency response facility established to coordinate and direct both the on-site and off-site response to an emergency at a nuclear facility, regardless of its initiating event [10], may also be used for the command and control elements of the physical protection response functions.

PHYSICAL PROTECTION MEASURES

4.83. The physical protection system implemented at a nuclear facility should be in accordance with and described in detail in a security plan. This plan includes all aspects of the physical protection measures found in the physical protection system design. More detailed information on the implementation of physical protection measures can be found in Ref. [17].

4.84. Physical protection measures may be classified by the function(s) they perform as described in paras 4.60–4.70. Table 3 relates the recommendations in sections 4 and 5 of Ref. [1] for each type of physical protection measure to the nuclear material category for unauthorized removal and to the level of potential

consequences for sabotage. The table also lists evaluation and performance testing requirements for each protection layer.

4.85. The recommendations for physical protection measures in Ref. [1] are organized using the graded approach. The measures recommended for Category II nuclear material also include the measures for Category III, and the measures for Category I nuclear material also include the measures for Category II and Category III.

Protection areas and layers

4.86. Figure 7 provides a conceptual drawing, based on the recommendations in paras 4.14, 4.22–4.28, 4.37–4.40, 4.42–4.46 and 5.20–5.35 of Ref. [1], of the different types of area that may be found at a nuclear facility, depending on its nuclear material and sabotage targets for which defence in depth needs to be provided. These protection areas are physically separated through each having its own protection layer. Beginning with the innermost area, the requirements for each area's protection layer are discussed below in terms of the area's location, access, detection, delay and response recommendations.

Limited access area

4.87. A limited access area is a designated area, containing a nuclear facility and nuclear material, to which access is limited and controlled for physical protection purposes. Any Category III nuclear material held in this area should be protected through the implementation of the measures listed in Table 3. (A further area of land outside the boundary of the nuclear facility may also be a controlled area, in accordance with national policy.)

Protected area

4.88. Category II nuclear material should be secured within a protected area. As part of graded protection, a State may consider securing sabotage targets with potential consequences ranging from unacceptable radiological consequences to high radiological consequences within a protected area. All protected areas should be located within a limited access area and be protected through the implementation of the measures listed in Table 3. A physical barrier is specifically recommended at the perimeter of the protected area.

TABLE 3. FACILITY PHYSICAL PROTECTION MEASURES: CROSS-REFERENCES TO REF. [1] PARAGRAPHS

	Unauthorized removal of nuclear material in use and storage, by material category			Sabotage of high consequence facilities	
	Category III (limited access area)	Category II (protected area)	Category I (inner area)	Protected area	Vital area
Physical protection measure					
Detection	4.14, 4.15, 4.16	4.14, 4.15, 4.16, 4.23, 4.30, 4.31	4.14, 4.15, 4.16, 4.23, 4.30, 4.31, 4.38, 4.40, 4.46, 4.47, 4.48	5.14, 5.21, 5.22, 5.36, 5.37	5.14, 5.26, 5.29, 5.33, 5.36, 5.37
Alarm assessment	n.a.[a]	4.23, 4.30, 4.31	4.23, 4.30, 4.31, 4.47	5.21, 5.36	5.36
Access control	4.14, 4.17	4.12, 4.17, 4.24, 4.25, 4.26, 4.27, 4.28, 4.30	4.12, 4.17, 4.24, 4.25, 4.26, 4.27, 4.28, 4.30, 4.38, 4.40, 4.42, 4.44, 4.45	5.14, 5.22, 5.23, 5.24, 5.25, 5.36	5.14, 5.26, 5.28, 5.31, 5.32, 5.34, 5.35, 5.36
Detection of prohibited items	n.a.[a]	4.25	4.25, 4.43	5.14, 5.23	5.14
Central alarm station	n.a.[a]	4.30, 4.31, 4.32, 4.33	4.30, 4.31, 4.32, 4.33, 4.47	5.36, 5.37, 5.38	5.36, 5.37, 5.38
Delay	n.a.[a]	4.23	4.23, 4.38, 4.39, 4.41, 4.46	5.14, 5.21	5.14, 5.26, 5.27, 5.30
Response	4.15, 4.19, 4.20	4.15, 4.19, 4.20, 4.30, 4.32, 4.33, 4.34	4.15, 4.19, 4.20, 4.30, 4.32, 4.33, 4.34, 4.49	5.14, 5.21, 5.36, 5.38, 5.39, 5.40, 5.42	5.14, 5.36, 5.38, 5.39, 5.40, 5.42
Evaluation					
Performance testing	4.20	4.20, 4.35	4.20, 4.35, 4.49	5.15, 5.16, 5.41	5.15, 5.16, 5.34, 5.41

[a] n.a.: not applicable.

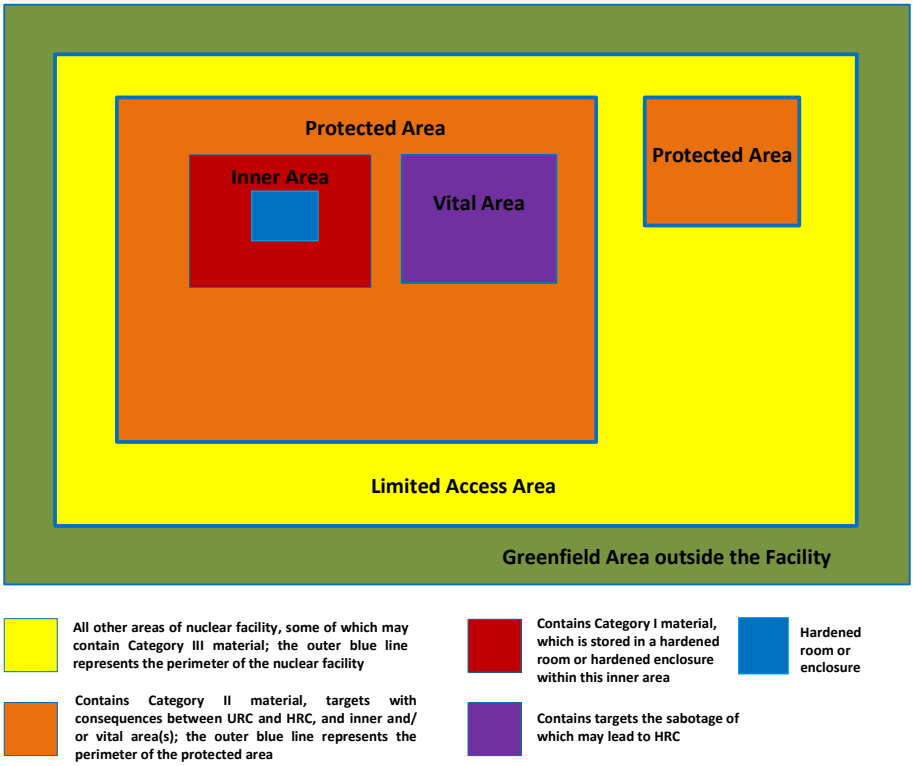


FIG. 7. Nuclear facility layout. URC — unacceptable radiological consequences; HRC — high radiological consequences.

Inner areas and vital areas

4.89. Inner areas are areas containing Category I nuclear material, and vital areas are areas containing equipment and/or radioactive material the sabotage of which could lead to high radiological consequences. An inner area may also be a vital area, in which case the measures for both unauthorized removal and sabotage should be implemented. Inside the inner area, Category I nuclear material should be stored in a hardened room or a hardened enclosure. All inner and vital areas should be located within a protected area and protected through the implementation of the measures listed in Table 3.

Central alarm station

4.90. A central alarm station is recommended for any nuclear facility holding Category I and II nuclear material and/or having sabotage targets with potential consequences above the high radiological consequences threshold.

4.91. The following recommendation is associated with the protection of Category I and II nuclear material:

> "4.30. A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a threat, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled" [1].

4.92. For sabotage targets with potential consequences above the high radiological consequences threshold, there is a recommendation in Ref. [1] that essentially combines the recommendations from paras 4.30 and 4.47 of that publication:

> "5.36. A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a threat, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station)."

4.93. An alarm communication and display system is a primary component of the central alarm station. This system facilitates the monitoring and assessment of alarms at the central alarm station. As a minimum, the functions of the system are to:

(a) Transmit alarm and video signals from the sensors and cameras to the central alarm station;
(b) Display this information to a central alarm station operator to be used as a basis for decisions and action;
(c) Assist the central alarm station operator to assess alarms.

4.94. Good practice is to design communications paths for alarms so that they are redundant (i.e. two or more separate communications systems) and diverse (e.g. the separate systems use different physical paths). Redundancy helps the communications system to be more reliable — if one communications path ceases to operate, the other(s) can take over that function — and to be more secure, as an adversary needs to defeat or compromise at least two communications paths instead of one.

4.95. The following recommendations from Ref. [1] relate to protection of Category I and II nuclear material:

> "4.31. Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper protected against unauthorized monitoring, manipulation and falsification.
>
> "4.32. Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*."

For sabotage targets with potential consequences above the threshold for high radiological consequences, there are two similar recommendations in paras 5.37 and 5.38 of Ref. [1].

4.96. Physical protection measures can be designed and operated to maintain the integrity of the alarm communications and display system (denying access to the equipment and denying and detecting access to the information) during nuclear security events. Tamper indication sensors in junction boxes and in equipment cabinets may provide an additional contribution to physical protection.

4.97. The central alarm station operator is responsible for assessing alarms and initiating the appropriate response to nuclear security events. Because of this crucial function, the central alarm station should normally be located within a

protected area. Because the central alarm station is the interface between the detection and response functions, central alarm station operators should ideally be members of the guards and/or response force, as they should have sound knowledge and understanding of the contingency plans. It is suggested that the functions of the central alarm station be regularly exercised during normal operations and tested for more infrequent operational conditions.

4.98. Further recommendations relating to Category I nuclear material with potential consequences above the threshold for high radiological consequences are contained in para. 4.47 of Ref. [1]:

> "Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. a backup alarm station)."

There is a similar provision for sabotage targets with potential consequences above the threshold for high radiological consequences in para. 5.36 of Ref. [1].

4.99. The essential functions of the central alarm station should be maintained when it is under threat, compromised or evacuated for safety reasons. A backup alarm station may provide continuity of operations for the essential central alarm station functions in such circumstances. Such a backup station needs to be located separately from the central alarm station, in a location that allows for continued operation of the central alarm station's essential functions. Physical protection systems with a backup alarm station as well as a central alarm station have the following advantages:

(a) Redundancy of equipment between the two stations provides greater hardware reliability.
(b) The central alarm station can be used as the primary system, with oversight surveillance from the backup station.
(c) The backup station can take over physical protection functions in the event of a hardware or personnel failure at the central alarm station or in case of an attack on the central alarm station.

Physical barriers

4.100. Physical barriers should be placed such that an adversary is delayed by the need to defeat or bypass them, thereby allowing the response forces sufficient time to interrupt the adversary before completion of a malicious act. A balanced

design includes balanced delays for the different adversary paths and scenarios, and physical barriers are carefully planned to fit the particular location and are positioned in the path of the adversary. The degree of delay depends on the nature of the barriers employed. Multiple layers of different types of physical barrier along all possible adversary paths, consistent with the threat assessment or the design basis threat, are suggested as ways to complicate and therefore delay the adversary's progress by requiring — in addition to increased time — the use of a variety of tools and skills. To aid in the assessment of alarms and provide opportunities for adversaries to be interrupted at predictable locations, consideration should be given to installing physical barriers and detection systems adjacent to each other so that a barrier is encountered by the adversary immediately after the attack is sensed. This arrangement delays the adversary at the point of detection and increases the probability of the detection of an attack. To detect an attack on or tampering with the physical barriers, it is suggested that barriers that are not covered by an intrusion detection system are patrolled randomly or are subject to another form of surveillance.

4.101. Vehicles can be driven to break through many types of fence or closed gates. It is recommended in Ref. [1] that vehicle barriers be installed at an appropriate distance from vital and inner areas. To minimize the probability of any secured area being breached, vehicle barriers can be designed and installed in appropriate locations on land and water. The orientation of vehicle gates and their approaches can be designed to reduce the probability of the gates being breached by vehicles being driven against them. Approach roads with series of sharp bends on each side of the gate will reduce the speed of vehicles near to the gate, thereby increasing the effectiveness of the vehicle barriers. In all cases, vehicle barriers should be designed and utilized in such a way as to be capable of stopping a vehicle described in the design basis threat or the threat assessment. To detect tampering with the vehicle barriers, it is good practice that vehicle barriers have an appropriate form of surveillance.

Access control systems

4.102. Access control systems comprise the equipment, people and procedures used to verify entry authorization and to control the movement of people and material into and out of each area. Access control systems are used to manage who is allowed to enter, when they are allowed to enter and where the access can occur, as well as to apply conditions for authorized entry. Information related to access control is sensitive, and therefore access control systems need to be suitably protected.

4.103. Access control systems can be designed to support the smooth and continual entry and exit of authorized persons, material and equipment via normal routes while detecting and delaying the movement of unauthorized persons and prohibited items. The goals of an access control system are to allow only authorized persons and vehicles to enter and exit; to detect and prevent the unauthorized movement of material, information or equipment into or out of the area; to provide information to the guard force to facilitate assessment and response; and to determine that persons are accounted for during nuclear security events and emergencies.

4.104. Access control systems need to be installed to control entry to the different areas at the nuclear facility, taking into account the number of persons who need to enter and exit at each point and when. Because the physical protection system has layers of protection, it provides detection measures of different types and of increasing rigour on the path from the limited access area to the protected area to any inner areas and/or vital areas. The number of authorized persons will be smaller at each successive entry point, and this limited access may influence the selection of access control equipment and procedures.

Guards and response forces

4.105. The operator's responsibilities for providing response differ among States, usually due to differences in national legislation relating to the legal use of force and the authority to arrest suspects. In some States the operator does not have prime responsibility for providing response forces and depends on the State to provide these capabilities, consistent with the legal and regulatory framework. In some other States, the operator provides both the guards and the response forces as part of its own staff and/or contractors. In such cases, operators retain full responsibility for ensuring that guards and on-site response forces employed by them, whether directly or under contract, fulfil their respective duties, as instructed by the operator's management and set out in the security plan.

4.106. Even when operators have their own guards and response forces, off-site response forces belonging to local or national law enforcement authorities may also respond, particularly in the case of a severe nuclear security event. In such cases, arrangements need to be documented between the operator and external organizations providing the response forces; these arrangements set out the goals, policy and concept of operations for response by all parties, to provide for a systematic, coordinated and effective response. These documented arrangements will help to ensure that the operator's contingency plan is fully consistent and coordinated with the contingency plans of the external response

forces. The coordination between guards and response forces during a nuclear security event should be regularly exercised. This coordination should be carried out with full cooperation between the operator and the response forces in the case of Category I and II nuclear material and nuclear facilities the sabotage of which could lead to high radiological consequences.

4.107. Whoever provides them, the response forces need to be able to interrupt and neutralize an adversary that has the resources and capabilities described in the threat assessment or the design basis threat. Interruption begins with communication to the response force that a potential adversary has been detected and is completed when a sufficient number of appropriately trained and equipped members of a response force arrive at the appropriate location in time to stop the adversary completing a malicious act. Neutralization is the act, following interruption, of gaining control of adversaries before their goals are accomplished or otherwise causing the adversaries to abandon the attempt. To be reliable in achieving effective neutralization, the response force needs to be superior to the adversary in terms of numbers, equipment and/or training.

4.108. Effective communication to the response force provides information about the adversary's actions and characteristics (including observed numbers and any information available about tools, equipment, weapons and vehicles) and instructions for deployment of the response force. The effectiveness of communications with the response forces can be measured by the probability of accurate communication and the time needed to accurately communicate with the response force.

4.109. The physical protection system may include a communications plan to support the coordination of response actions. It is suggested that the communication system used by the response force provide the capability for any responder to covertly send a duress signal. Communication systems should have sufficient redundancy and diversity to ensure that communications remain reliably adequate for effective response to a threat, as described in the design basis threat or the threat assessment.

4.110. A rigorous training programme is essential for an effective response. All guards, central alarm station staff and response forces need to participate in frequent training appropriate to their positions and responsibilities.

4.111. Recommendations from Ref. [1] for both guards and response forces to address a nuclear security event are as follows:

> "3.60. The coordination between the *guards* and *response forces* during a *nuclear security event* should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the *guards*, *response forces* and other response teams for implementation of the plans."

4.112. Specific recommendations from Ref. [1] on capabilities for response to unauthorized removal of Category I, II and III nuclear material are as follows:

> "4.15. Provision should be made for detecting unauthorized intrusion and for appropriate action by sufficient *guards* and/or *response forces* to address a *nuclear security event*.
>
> …….
>
> "4.20. The State should ensure that *response forces* are familiarized with the site and *nuclear material* locations and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety."

4.113. Reference [1] recommendations to counter the unauthorized removal of Category I and II nuclear material include the following:

> "4.33. A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*…. The *guards* and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations.
>
> "4.34. The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:
>
> — Deter an adversary;
> — Detect intrusion;
> — Inspect visually the physical protection components;
> — Supplement the existing *physical protection measures*;
> — Provide an initial response."

The recommendation from para. 4.34 of Ref. [1] also applies in relation to guards' functions within protected areas to protect against sabotage (see para. 5.40 of Ref. [1]).

4.114. It is good practice for patrols to cover the entire perimeter several times during each shift, but at random times, so as not to be predictable to an adversary observing the facility. During this time, the patrols may also check the integrity of fences, that lighting is functioning and that all gates and doors are appropriately secured. Other good practices are to use guards to test the operation of sensors at the perimeter of the protected area, verify the functioning of the detection system elsewhere, and provide compensatory measures when necessary, for example until a failed sensor is repaired or replaced.

4.115. Paragraphs 3.27–3.32 and 4.50–4.52 address recommendations concerning the evaluation and performance testing of response forces for the unauthorized removal of Category I and II nuclear material and against sabotage for the State and the operator, respectively.

4.116. Training for guard and response forces may include exercising contingency plans, performance testing, tabletop exercises, modelling and simulation, response force exercises and/or force-on-force exercises.

Protection measures for stand-off sabotage attacks

4.117. The operator has the responsibility to protect against the types of stand-off attack that are included in the design basis threat (see paras 3.55–3.63).

4.118. The first step for the operator in providing protection against stand-off attacks is to identify the potential vulnerability of target areas and the material, equipment and systems within those areas to stand-off attack. This process includes the development of sabotage scenarios based on the characteristics defined in the threat assessment or the design basis threat and the assessment of the impact on targets and the physical protection system in those scenarios. Close cooperation between the personnel responsible for safety and physical protection is needed in this process.

4.119. The operator is responsible for designing protection measures against stand-off attacks and, when they have been approved by the competent authority, implementing those measures. Protection measures that may protect against or mitigate the consequences of a stand-off attack include:

(a) Increasing the distance from the facility within which a stand-off attack could be attempted so as to exceed the range of weapons the adversary might use;

(b) Obscuring lines of sight to the target from areas from which stand-off attacks might be attempted;
(c) Increasing detection and deterrence through off-site patrols and surveillance;
(d) Using barriers capable of intercepting missiles or absorbing blasts or fragments;
(e) Modifying layouts of facilities to protect sensitive targets;
(f) Hardening facilities to resist such attacks.

Protection measures for airborne and water-borne attacks

4.120. The threat assessment or the design basis threat may include adversaries who use airborne and/or water-borne vehicles for transport in a theft or sabotage scenario (not to be confused with an aerial stand-off sabotage attack). In these cases, the adversaries may arrive at and/or leave the site by air or water. The operator will typically have some responsibility for protecting against these modes of attack.

4.121. Radar, acoustic and seismic sensors can all provide some detection capability for airborne attacks but need to be carefully located to provide good coverage with few nuisance alarms. Some types of aircraft may be prevented from landing at the site of a nuclear facility because of the facility's small and/or congested area. This effect may be enhanced by the strategic positioning of poles or other physical barriers.

4.122. On the basis of the design basis threat and the State's requirements, the operator may install and operate equipment and devices to detect such attacks.

Transport of nuclear material

4.123. The operator of a nuclear facility, as the shipper or receiver, has certain responsibilities for the physical protection of the nuclear material being transported into or out of the facility. These responsibilities may include providing advance notification of planned shipments, searching conveyances, protecting the confidentiality of transport information, checking the integrity of packages on arrival and notifying the shipper of such arrival, and making prior arrangements with the carrier concerning the transfer of physical protection responsibilities. Furthermore, the operator should ensure that the on-site movement of Category I and II nuclear material between two protected areas at the nuclear facility is protected in accordance with the State's requirements for the transport of such

nuclear material outside the facility. Further guidance on the security of nuclear material in transport is provided in Ref. [2].

NUCLEAR MATERIAL ACCOUNTING AND CONTROL[4] FOR NUCLEAR SECURITY

4.124. Reference [1] provides several recommendations for nuclear material accounting and control in relation to nuclear security:

> "3.26. The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority*.
>
> …….
>
> "3.36. When considering the threat, due attention should be paid to *insiders*. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The *physical protection system* should be assisted by nuclear material accountancy and control measures to deter and detect the protracted theft of *nuclear material* by an *insider*.
>
> …….
>
> "3.47. *Defence in depth* should take into account the capability of the *physical protection system* and the *system for nuclear material accountancy and control* to protect against *insiders* and external threats.
>
> …….
>
> "4.57. The *operator* should ensure that any missing or stolen *nuclear material* is detected in a timely manner by means such as the *system for nuclear material accountancy and control* and the *physical protection system* (e.g. periodic inventories, inspections, access control searches, radiation detection screening).

[4] Reference [1] uses the term 'nuclear material accountancy and control'; Ref. [17] uses the term 'nuclear material accounting and control'. Except when quoting directly from Ref. [1], the latter term is used in this publication, but the terms are considered to be interchangeable.

"4.58. The *operator* should confirm any missing or stolen *nuclear material* by means of a rapid emergency inventory as soon as possible within the time period specified by the State. A *system for nuclear material accountancy and control* should provide accurate information about the potentially missing *nuclear material* in the facility following a *nuclear security event*."

4.125. A nuclear material accounting and control system is designed to maintain knowledge of the quantity, type, location, use, movement and transformation of all nuclear material at a facility. The nuclear material accounting function provides deterrence against and detection of the unauthorized removal of nuclear material by maintaining an inventory of all nuclear material and its location. The nuclear material control function provides containment and surveillance measures, which may detect malicious activities by an insider. Either or both functions may provide a basis to initiate a response if they detect that nuclear material may have been removed without authorization or used in an unauthorized manner. An effective nuclear material accounting and control system enhances the ability of the operator to detect insider activities and to correctly assess any irregularity involving nuclear material, whether initiated by insiders or external adversaries. If nuclear material is removed from the facility, the nuclear material accounting and control system should be able to identify the quantity and characteristics of the nuclear material that has been removed.

4.126. The objectives of a nuclear material accounting and control system relevant to physical protection are to:

(a) Detect and assess unauthorized access to, or removal of, nuclear material;
(b) Provide information about the locations, characteristics and quantities of nuclear material.

4.127. Attaining these objectives will allow the operator to:

(a) Communicate to the relevant competent authorities that there has been unauthorized removal of nuclear material;
(b) Provide accurate and timely information to assist in locating any material not in its authorized location;
(c) Provide assurance, in coordination with physical protection and material control measures, that appropriate protection and controls are applied to nuclear material according to their categorization.

4.128. Material surveillance and monitoring may be used by the operator to detect the movement of nuclear material and to provide continuous information

about the status of nuclear material accounting and control equipment and nuclear material. Material surveillance and monitoring may include visual surveillance by operations personnel and visual and remote monitoring by physical protection personnel, as well as other technical means such as weight sensors, heat sensors, laser monitors, radiation monitors, radiofrequency tags and motion sensors.

4.129. For visual surveillance to be effective, the person observing needs to be capable of recognizing unauthorized activities, correctly assessing the situation and reporting the activities to appropriate response personnel in time for them to prevent unauthorized removal. If the two person rule is applied in such surveillance, the two authorized individuals will both need to have undergone appropriate training, have unobstructed views of the material and of each other, and be able to detect unauthorized or incorrect procedures.

4.130. Material containment measures and tamper indication devices can be used to help ensure the continuity of knowledge of nuclear material and to indicate any unauthorized access. The use of various levels of containment — such as cans, gloveboxes, storage cabinets and vaults — along with effective tamper indication devices and surveillance, will reduce the time needed to determine whether any nuclear material is missing, and if so what material, and whether an emergency or unscheduled inventory is necessary.

4.131. It is considered good practice that the responsibilities for the separate functions of nuclear material accounting, custody of nuclear material and physical protection are assigned to different individuals or groups.

4.132. In all cases, timely detection is important. It is suggested that the operator review all possible means of detecting that nuclear material is missing, stolen or otherwise removed in an unauthorized manner, estimating for each case the cumulative time for the various detection measures to determine whether or not it satisfies requirements set by the competent authority. Further guidance on this topic can be found in Ref. [18].

SECURITY OF SENSITIVE INFORMATION

4.133. Adversaries wishing to plan or carry out any malicious act involving nuclear material or nuclear facilities may benefit from access to sensitive information. Such information should therefore be identified, classified and secured with appropriate measures.

4.134. Sensitive information is information, in whatever form (including software), the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise nuclear security.

4.135. Paragraph 1.2 of Ref. [16] states that: “Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes.” As well as protecting the confidentiality of sensitive information, information security protects the accuracy and completeness of the information (its integrity) and the accessibility or usability of the information when it is needed (its availability).

4.136. Information security is a cross-cutting prerequisite for nuclear security and is a key element of the nuclear security regime in a State. The State, through the competent authorities, sets the information security requirements for operators and other relevant organizations, taking into account guidance and policies from the national security authorities.

4.137. Operators need to establish internal policies and procedures for protecting the confidentiality, integrity and availability of the sensitive information the operators hold or handle, in compliance with the national security policy and the relevant national laws and requirements. These procedures need to be incorporated into the security plan. The operator also needs to ensure that its contractors, whether on-site or off-site, are made aware of the sensitivity of any information passed to them by the operator and are briefed on the procedures to appropriately protect such information. The operator may be responsible for carrying out checks to ensure that contractors comply with these procedures and for ensuring that sensitive information is returned to the operator at the conclusion of the contract.

4.138. Frequent reviews and periodic audits of the information security programme may be used to determine whether it is operating as intended and to make enhancements or correct any deficiencies that have been identified. To allow for investigation and corrective actions, breaches of information security should be reported to the appropriate authorities in accordance with the State’s requirements.

4.139. Further guidance on information security, including an example classification guide to assist States and operators in identifying sensitive information, can be found in Ref. [16].

PROTECTION OF COMPUTER BASED SYSTEMS

> "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*" (paras 4.10 and 5.19 of Ref. [1]).

4.140. The State has the responsibility to provide requirements on computer security and ensure that operators provide assurance that computers and computer based systems are adequately protected against cyber attacks. Operators have responsibility for implementing a computer security programme in compliance with these requirements.

4.141. The overall goal of computer security in the physical protection of nuclear material and nuclear facilities is to protect computer systems against attacks aimed at facilitating the unauthorized removal of nuclear material or sabotage. The operator is responsible for identifying those computer based systems that need protection against compromise so as to help prevent a successful adversary attack. The operator then needs to establish a computer security policy and its implementation plan.

4.142. The threat and adversary attack vectors are multidimensional. The adversary could be:

(a) An external adversary;
(b) An insider;
(c) One or many individuals.

4.143. The attack could:

(a) Have an immediate impact, causing damage to equipment or degradation in security functions;
(b) Be ongoing, such as covert information collection;
(c) Include a delay, producing a timed or separately triggered effect;
(d) Be synchronized with other adversary activities, which may include physical attack.

4.144. Attack types might include:

(a) Denial of service or loss of function. This type of attack aims to block the operator's ability to observe and/or respond to changing system conditions by slowing the system down.
(b) Interception ('man in the middle'). By intercepting and modifying data streams between computer nodes, such an attack aims to modify information feeds or the command signals to equipment.
(c) Unobserved system monitoring and data collection. Unauthorized file access and data recording, message (information) interception and data exfiltration could provide reconnaissance in planning and executing an attack.
(d) Operator spoofing leading to incorrect action. Through the insertion of unauthorized or erroneous data streams, the attack aims to provide the operator with false system indicators, leading the operator to take incorrect action.
(e) Direct manipulation of computers and control systems. The adversary aims to assume independent control over processes and machinery.
(f) Modification to the operational characteristics of critical systems. Through the modification of system logic, equipment configuration, set points or data, the attacks aim to change the operational characteristics of the system, leading to abnormal behaviour. This modification of critical systems could be the primary purpose of the attack or could support another purpose.

4.145. Defence against such attacks needs to follow an approach based on defence in depth that uses technical, administrative and physical security controls. Computer security therefore needs to be integrated within the overall framework of the security plan.

4.146. Detailed guidance on establishing an effective computer security programme at nuclear facilities is provided in Ref. [6].

SAFETY–SECURITY INTERFACE

> "4.11. The *operator* should assess and manage the physical protection interface with safety and nuclear material accountancy and control activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive" [1].

4.147. Effectively managing the interface between safety and security is an important element of both programmes and is essential to providing the appropriate physical protection of nuclear material and nuclear facilities and protecting the health and safety of workers and the public.

4.148. The operator has primary responsibility for the safety of the nuclear facility and for physical protection measures at the facility. It is suggested that operators adopt, through their integrated management system, an integrated and coordinated approach to reviewing proposed changes before they are implemented to ensure that changes proposed for reasons related to safety or to physical protection do not result in the unintended degradation of arrangements in the other area. When possible adverse interactions are identified, the operator will need to communicate them to appropriate personnel within the organization and consider alternative measures or take compensatory and/or mitigating actions.

4.149. The operator needs to recognize safety–security interface issues and manage them appropriately during design, construction and normal operations, as well as during nuclear security events and emergencies, and during decommissioning. These interface issues may be addressed through existing management controls, such as safety or security review boards, work planning and controls, and configuration management.

4.150. Examples of such issues during nuclear security events and emergencies include:

(a) Coordinating the physical protection response to a nuclear security event with the safety response to any emergency resulting from that event.
(b) Ensuring that physical protection response forces are familiar with the nuclear facility, including the location of nuclear material and of equipment/systems important to safety, and have adequate knowledge of radiation protection requirements.
(c) Ensuring radiation protection of response forces as they move in and through contaminated areas during a sabotage attack.
(d) Protecting safety responders and facility personnel if they need to move in and through areas where the response force is operating during a nuclear security event.
(e) Ensuring that physical protection barriers satisfy physical protection objectives without compromising the ability of personnel to evacuate areas quickly in the event of a fire, a criticality or a release of radionuclides, for example through the installation of internal quick release locks on doors

and gates, coupled with alarms. Special physical protection arrangements may be necessary to allow personnel to evacuate a protected area quickly in an emergency while still ensuring that they are subject to search before leaving the nuclear facility.

(f) Requiring extensive inspections and searches prior to entry into a protected area, without adequate consideration of the potential need for off-site emergency responders and vehicles to enter quickly to assist in the event of a medical or other emergency.

4.151. Information regarding the interface between emergency plans and contingency plans is provided in paras 4.76–4.82, including the guidance that exercising both types of plan together improves coordination.

4.152. An important aspect of managing the safety–security interface is ensuring that physical protection personnel are notified of changes to the characteristics of the nuclear facility's physical layout; the configuration of facilities, structures, systems and components; and changes to the facility's operations or emergency planning. It is also helpful to have knowledgeable personnel review changes in these areas before they are implemented. Similar notification and review processes are helpful as inputs to the review of safety provisions in the light of changes related to physical protection measures. In particular, safety expertise is needed to review any new definitions of the threshold for unacceptable radiological consequences or changes to the threshold to reflect changes in operations or threats (which would then provide a basis for deciding the necessary level of physical protection to be applied to existing or new sabotage targets).

4.153. Effective management of the interface between safety and physical protection includes implementing safety and physical protection in such a way that they are mutually supportive. For example, safety procedures to prevent safety incidents or accidents may also be effective in assisting physical protection procedures against malicious acts by insiders. Structures, systems and components important to safety may be designed and located in the nuclear facility in such a way that they simplify the assignment of sabotage target protection sets and the compartmentalization of the nuclear facility for access controls. For instance, ensuring adequate physical separation of safety equipment to provide redundancy also reduces the likelihood of all of this equipment being damaged by a single act of sabotage. Reductions in inventories of nuclear material and other hazard reduction measures reduce both safety and nuclear security risks.

SECURITY PLAN

> "3.27. The *operator* should prepare a security plan as part of its application to obtain a licence. The security plan should be based on the *threat assessment* or the *design basis threat* and should include sections dealing with design, evaluation, implementation, and maintenance of the *physical protection system*, and *contingency plans*. The *competent authority* should review and approve the security plan, the implementation of which should then be part of the licence conditions. The *operator* should implement the approved security plan. The *operator* should review the security plan regularly to ensure it remains up to date with the current operating conditions and the *physical protection system*. The *operator* should submit an amendment to the security plan for prior approval by the *competent authority* before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan. The *competent authority* should verify the *operator's* compliance with the security plan" [1].

4.154. The security plan provides part of the basis for the licensing of the nuclear facility by the State, and implementation of the security plan is a condition of the licence to conduct operations at the nuclear facility. The plan should therefore describe in detail all aspects of the physical protection system at the nuclear facility. It is suggested that the security plan include a list of the targets at the facility, indicating in each case whether they are of concern for unauthorized removal and/or sabotage. It is suggested that the security plan also include the physical protection arrangements for the on-site movement of Category I and II nuclear material between two protected areas, as well as arrangements for the receipt and shipping of nuclear material to and from the nuclear facility.

4.155. The security plan describes the measures in place to meet the State's physical protection objectives and requirements. Security plans therefore need to be based on in-depth analysis and be supported by adequate information to confirm that the physical protection requirements will be met when the plan is executed. The security plan provides assurance that the physical protection system addresses the threats contained in the threat assessment or in the design basis threat.

4.156. An example of the structure and suggested content of a security plan is provided in Appendix I.

Development, review and update

4.157. The operator should keep the security plan up to date so that it reflects the existing conditions at the nuclear facility as well as the current threats. The operator therefore needs to have in place, within its integrated management system, a security management system to provide for the development, implementation and oversight of, as well as updates to, the security plan and associated procedures. Implementation procedures may document the structure of the security organization, the use of security measures such as technologies and procedures, the training and qualification of security personnel, and the contingency plan. The security plan may describe, as necessary, the schedule for implementing parts of the plan and address any activities that involve modification of the facility.

4.158. After the security plan has been approved by the competent authority, it forms part of the licensing basis for the nuclear facility. The competent authority approves changes to the security plan, and the operator is not permitted to implement proposed changes to the security plan without approval by the competent authority unless the changes do not decrease the effectiveness of the physical protection system. For minor changes that do not decrease the effectiveness of the physical protection system, the operator should notify the competent authority of the change within an agreed period of time.

4.159. The security plan should be reviewed at intervals defined by the competent authority to ensure that the plan continues to reflect the current circumstances. The security plan will also need to be reviewed before the implementation of changes in physical protection personnel, procedures, equipment or systems that could potentially adversely affect physical protection. The introduction of new quantities or types of nuclear material, changes in sabotage targets and other significant changes to the physical protection system will likely necessitate changes to the security plan. It is considered good practice that the results of such reviews, including any resulting action plan, be documented and retained.

Confidentiality of sensitive information

4.160. Some of the information in the security plan will be sensitive information, and its unauthorized release could compromise the physical protection of the nuclear facility. The operator will therefore need to protect the security plan against unauthorized disclosure. In accordance with the State's requirements, access to sensitive information should be provided only to those

whose trustworthiness has been established and who have a need to know for the performance of their duties.

4.161. The security plan may be divided into sections of different levels of sensitivity so that each section can be shared, as appropriate, with those who have a need to know and the appropriate level of trustworthiness.

Appendix I

THE SECURITY PLAN

I.1. An example of the possible structure for a security plan is set out in Box 1. After this outline, there is a brief discussion of the suggested contents of each section. The State and its competent authorities should review this proposed structure and modify it to meet their requirements and specific needs.

BOX 1: EXAMPLE STRUCTURE OF THE SECURITY PLAN

1. ADMINISTRATIVE INFORMATION
    - 1.1. Introduction and schedule for implementation
    - 1.2. Facility description (operations and layout)
        - 1.2.1. General facility description, mission and operations
        - 1.2.2. Facility layout
    - 1.3. Security policy
        - 1.3.1. Management policy
        - 1.3.2. Nuclear security culture
        - 1.3.3. Quality assurance
        - 1.3.4. Trustworthiness policy
        - 1.3.5. Sustainability programme
    - 1.4. Security organization
        - 1.4.1. Security organization structure
        - 1.4.2. Security management and allocation of responsibilities
        - 1.4.3. Qualification requirements for security personnel
        - 1.4.4. Security personnel training
        - 1.4.5. Guards/response force armament and equipment
    - 1.5. Security of nuclear information
    - 1.6. Computer security
2. DEFINING THE PHYSICAL PROTECTION SYSTEM
    - 2.1. Objectives and requirements of the physical protection system
    - 2.2. Target identification
    - 2.3. Threat definition
    - 2.4. Law enforcement liaison
3. PHYSICAL PROTECTION SYSTEM
    - 3.1. Detailed description of the physical protection system

BOX 1: EXAMPLE STRUCTURE OF THE SECURITY PLAN (cont.)

- 3.2. Insider threat mitigation programme
- 3.3. Transport of nuclear material
- 3.4. Physical protection system testing, evaluation and maintenance
  - 3.4.1. Types of testing and evaluation
  - 3.4.2. Frequency of testing and evaluation
  - 3.4.3. Maintenance
  - 3.4.4. Expansion and upgrade
- 3.5. Compensatory measures

4. RESPONSE PLANNING

- 4.1. Organization and responsibilities
- 4.2. Security forces
  - 4.2.1. Guards
  - 4.2.2. On-site response force
  - 4.2.3. Off-site response force
  - 4.2.4. Central alarm station staffing
- 4.3. Contingency plan
- 4.4. Incident communications command and control
- 4.5. Response to higher threat conditions

5. POLICIES AND OPERATIONAL PROCEDURES

- 5.1. Documented policies and operational procedures
- 5.2. Review, evaluation, audit and update of the security plan
- 5.3. Reporting of threats or incidents

REFERENCES

ABBREVIATIONS AND GLOSSARY

ADMINISTRATIVE INFORMATION

I.2. This section includes information on the complete legal name and address of the entity responsible under law for the protection of the nuclear facility. The appropriate telephone and fax numbers and email addresses of those who are applying for approval of the security plan may be contained in a covering letter.

Introduction and schedule for implementation

I.3. This section includes a short description of the facility's mission and operations, maps of the facility and other information to indicate on these maps

the locations of the major activities. The maps may depict terrain, transport routes, nearby towns or hazardous material facilities, and any other areas that could affect response activities. The maps may also indicate main and alternative routes for law enforcement or other off-site responders.

Facility description (operations and layout)

I.4. This section provides details of nuclear operations undertaken at the facility.

General facility description, mission and operations

I.5. This section gives a general description of the types of nuclear activity that take place at the facility and the nuclear and other radioactive material used or generated by these activities.

Facility layout

I.6. A map, diagram or image of the facility, with key buildings and activities identified, may be provided in this section. Block diagrams of the various operations may be useful in describing the facility's activities.

Security policy

I.7. This section contains the facility's written security policy.

Management policy

I.8. This section describes the management system that provides oversight of the facility's physical protection, the purpose of which is to develop, revise, implement and oversee physical protection procedures. This section could also address how the safety–physical protection interface is managed.

Nuclear security culture

I.9. This section describes how the operator promotes nuclear security culture as an important part of delivering the security policy to management, employees and contractors.

Quality assurance

I.10. This section describes the quality assurance aspects of the management policy and programme applicable to physical protection.

Trustworthiness policy

I.11. This section describes the trustworthiness levels and requirements applied to employees and contractors at the nuclear facility for access to specified areas within the facility (e.g. protected areas, inner areas, vital areas), to nuclear material and to sensitive information, as well as the measures taken to ensure continued trustworthiness.

Sustainability programme

I.12. This section describes the sustainability programme for the physical protection system.

Security organization

I.13. All individuals with security responsibilities may be identified with a brief description of their duties and responsibilities. This section may include the requirements for selecting, training, equipping, testing and qualifying individuals who will be responsible for protecting nuclear material and nuclear facilities. As appropriate to the operator's assigned responsibilities and capabilities, this section needs to state which parts of the security organization are provided by staff and which by external contractors. For contractors, this section may briefly describe the written agreements between the operator and contractors that describe how they will meet the requirements to protect the facility. The level of detail included in the security plan may vary depending on the facility, but this section needs to provide enough information for a reader to understand the capabilities of the security forces for the facility. The information provided seeks to confirm that the security organization is designed, staffed, trained, qualified and equipped to implement physical protection.

Security organization structure

I.14. This section describes the structure of the security organization, including management, guards and any on-site response force, technical security personnel and other persons responsible for physical protection related functions. This section may also contain a description of each supervisory and management

position, including responsibilities and how lines of authority extend up to facility and corporate management.

Security management and allocation of responsibilities

I.15. This section describes the specific physical protection responsibilities assigned to the facility's security organization.

Qualification requirements for security personnel

I.16. A description may be provided of the requirements for the initial and continued suitability of individuals who are assigned security duties and responsibilities. This section may also describe the process to ensure that these personnel continue to be qualified to provide the required services. This section also includes a description of the firearms qualification and requalification requirements for guards and on-site response force members.

Security personnel training

I.17. This section describes the training programme for guard and on-site response forces. It also describes how they demonstrate their ability to carry out their assigned duties or responsibilities. For response forces, a description of the training programme in response tactics may be included.

Guards/response force armament and equipment

I.18. This section describes the armaments assigned to members of the guards and on-site response force, by position title. A description of other equipment available to the guards and response forces to enable them to provide effective response capabilities may be provided.

Security of nuclear information

I.19. This section defines the measures that are taken to maintain the confidentiality, integrity and availability of sensitive information. Information management procedures also need to describe how the distribution of sensitive information is limited to appropriate individuals, whose trustworthiness has been appropriately determined, on a need-to-know basis. Controls applied to sensitive information may include records of its receipt, location, dispatch and destruction.

Computer security

I.20. This section describes the access control procedures, protocols and physical security arrangements in place to ensure the confidentiality, integrity and availability of sensitive information held on computers and computer based systems, as well as the integrity and availability of instrumentation and control systems.

DEFINING THE PHYSICAL PROTECTION SYSTEM

Objectives and requirements of the physical protection system

I.21. This section describes the objectives for the protection of different types of target, grouped according to their level of sensitivity.

Target identification

I.22. This section lists the potential theft or sabotage targets and their location. It also lists the computer systems important to physical protection, safety and nuclear material accounting and control the compromise of which could help facilitate a malicious act.

Threat definition

I.23. This section describes, in broad terms, the types of threat the physical protection system is designed to protect against and references the threat assessment or design basis threat defined by the State.

Law enforcement liaison

I.24. Details may be provided of how routine liaison is maintained with law enforcement agencies to help ensure early warning of potential security events.

PHYSICAL PROTECTION SYSTEM

I.25. This section is a description of the physical protection system at the facility.

Detailed description of the physical protection system

I.26. In this section, a facility map indicating the layer boundaries and protection measures, such as personnel–vehicle control points, may be provided. A description of the protection measures needs to be provided, as described below:

(a) Access control. A description of the control and search of personnel, vehicles and material at each access control point needs to be provided. This description can also include how access authorization and access control systems will accommodate the rapid entry and exit of authorized individuals and vehicles during emergencies or in situations that could lead to emergencies. Attention may be given to the control of all keys, locks, combinations, passwords and related devices used to control access to limited access areas, protected areas, inner areas, vital areas and physical protection equipment.
(b) Central alarm station. This section describes the location of the central alarm station and any backup monitoring stations. It also describes the central alarm station alarm communication and display systems, communications equipment, and access control arrangements and details how the central alarm station is protected against attack and unauthorized access.
(c) Communications. The communications capabilities for the guards and on-site response forces need to be described, as do the communications between the central alarm station and the guard and response forces. This section describes how a continuous communications capability is maintained to ensure effective command and control with on-site and off-site response forces during normal and emergency situations. If there are areas of the facility where communication is limited, these areas need to be identified.
(d) Detection and surveillance. This section describes the detection system and how alarms are communicated to the central alarm station and assessed. The section may also describe procedures to address situations in which there are indications of tampering. It describes the methods to continuously survey, observe and monitor facility areas to detect intruders and to ensure the integrity of physical barriers or other components and functions of the physical protection system.
(e) Lighting. This section describes how the operator maintains the minimum illumination levels for selected applications, such as assessment after an alarm.
(f) Physical barriers. This section describes the barriers in different security areas within the facility (e.g. buildings, topography, fences, walls, doors). It

may also contain a description of the vehicle barriers, their placement and operation, as well as associated surveillance arrangements.

(g) Security areas/layers. This section identifies the physical protection areas (or layers) that exist at the facility.

Insider threat mitigation programme

I.27. This section should describe measures to protect against insider threats.

Transport of nuclear material

I.28. This section describes the procedures for the on-site transport of different categories of nuclear material, as well as the arrangements made on-site for the receipt and dispatch of nuclear material to and from the facility.

Physical protection system testing, evaluation and maintenance

I.29. This section identifies the procedures for evaluating and testing the physical protection system.

Types of testing and evaluation

I.30. This section describes the testing and evaluation programmes that exist and how they are used to assess the effectiveness of the facility's physical protection system.

Frequency of testing and evaluation

I.31. Details need to be provided of the frequency with which the testing and evaluation programmes are implemented.

Maintenance

I.32. This section describes the maintenance and calibration programmes for all physical protection equipment.

Expansion and upgrade

I.33. This section is available to describe any schedule foreseen for implementing physical protection measures related to new construction or the significant physical modification of existing structures or the installation of equipment.

Compensatory measures

I.34. This section identifies all compensatory physical protection measures applied when physical protection barriers become degraded or equipment becomes inoperable, including during routine testing or maintenance. In particular, the provision of standby power to all types of physical protection equipment needs to be described.

RESPONSE PLANNING

Organization and responsibilities

I.35. This section provides details of the organization and responsibilities of the facility and off-site response forces to maintain an effective response strategy for the various targets at the facility.

Security forces

I.36. This section provides an overview of the response forces available to deliver a coordinated response strategy.

Guards

I.37. This section describes the number, location and duties of the guard force, including details of their weapons, equipment and transport.

On-site response force

I.38. This section describes the on-site response force capacity and capability to respond to nuclear security events in a timely manner, where such a force is employed.

Off-site response force

I.39. This section describes off-site response force capacity and capability to respond to nuclear security events, including estimated response times. The process of documenting and maintaining agreements for providing off-site response may be included.

Central alarm station staffing

I.40. This section describes the minimum number, duties, responsibilities and rotation schedule of staff employed in the central alarm station.

Contingency plan

I.41. This section describes the contingency plan for nuclear security events and for other events that may need a physical protection response. It identifies specific people and/or positions that have the responsibility and authority to carry out the contingency plan should a nuclear security event occur. It details how and when the contingency plan is reviewed and exercised.

I.42. The list below suggests examples of different types of scenario that may be considered and addressed in the contingency plan:

(a) Location and recovery of missing nuclear material (including emergency inventory taking);
(b) Minimization and mitigation of the radiological consequences of sabotage;
(c) Discovery of an insider threat;
(d) Unauthorized intrusion into a nuclear facility;
(e) External threats (e.g. bomb warning);
(f) Stand-off attack;
(g) Airborne attack;
(h) Water-borne attack;
(i) Cyber attack;
(j) Compromise of sensitive information.

I.43. As the contingency plan will contain sensitive information, it needs to be appropriately marked to indicate the level of protection required. It also needs to address arrangements for coordination with emergency plans. An example of a contingency plan is given in Appendix II.

Incident communications command and control

I.44. The security plan describes how effective command and control will be exercised in response to a nuclear security event by the agencies involved, where the on-site and off-site incident command and control centre will be located and what communications facilities will be available at these locations.

Response to higher threat conditions

I.45. A list should be provided of the planned enhancements to physical protection procedures that will be put in place in the event of any increase in the overall level of threat within the State.

POLICIES AND OPERATIONAL PROCEDURES

Documented policies and operational procedures

I.46. This section lists the documented policies and operational procedures that govern physical protection at the facility, including procedures for interfacing with systems that complement the physical protection system, such as the safety and nuclear material accounting and control systems.

Review, evaluation, audit and update of the security plan

I.47. Details need to be provided of the procedures and review processes (including their frequency) employed to ensure that the security plan remains current, together with an assurance that all necessary amendments to it will be submitted to the competent authority for approval prior to implementation.

Reporting of threats or incidents

I.48. The procedure for facility employees and contractors to report specified occurrences to the facility's security organization, and for their onward reporting to the competent authority, as appropriate, is described in this section.

Appendix II

EXAMPLE CONTINGENCY PLAN

OBJECTIVE

II.1. This section describes the objective of the particular contingency plan. The objective may be to prepare for a further response or to reduce the consequence of the adversary's actions.

INCIDENT RESPONSE PROCEDURES

Rules of engagement

II.2. This section includes the rules of engagement that define what sort of force is authorized under the law and when and where such force can be used.

Response procedures

II.3. This section describes how the response is organized and coordinated. It identifies those indicators that will be used to signal the initiation of a response under this contingency plan. The section may include:

(a) All predetermined actions, areas of responsibility and timelines for the deployment of the response force for theft and sabotage scenarios;
(b) Procedures that limit the exposure of the response personnel to possible attack;
(c) Timelines to be used when notifying the off-site response force;
(d) The minimum number of responders.

Recapture and recovery

II.4. This section states how the response is organized when the adversary has left the facility in a theft scenario. It includes the protocols used to coordinate the different response teams, the chain of command and any change in responsibilities.

Minimize and mitigate

II.5. This section states how the physical protection response is organized to help emergency responders minimize and mitigate the consequences of a sabotage attack.

Command, control and communication

II.6. This section describes the arrangements documented in protocols agreed with external response organizations. It details which agency has the operational lead and the circumstances in which this lead may be handed over to another agency. Details are provided of all the communication links to be used and the location of the incident control centres that may be used at different stages of the event, taking into account prevailing circumstances and the centres' strategic and tactical responsibilities.

EXERCISING THE CONTINGENCY PLAN

II.7. This section describes the type and frequency of exercises undertaken to test and practise implementation of the contingency plan. The information includes testing coordination between the contingency plan and the emergency plan through joint exercises in which both plans are implemented. The section also describes how lessons learned from these exercises are captured and used to further refine the contingency plan.

Appendix III

THE ADDITION OR AGGREGATION OF NUCLEAR MATERIAL

APPROACH 1

III.1. This example illustrates one way in which Table 1 may be used to categorize aggregated nuclear material. Nuclear material located in the same facility should be classified as outlined:

(a) Category I if:

$$\frac{\text{Pu} + {}^{233}\text{U}}{2000} + \frac{{}^{235}\text{U}(\geq 20\%)}{5000} \geq 1 \tag{1}$$

(b) Category II if:

$$\frac{\text{Pu} + {}^{233}\text{U}}{500} + \frac{{}^{235}\text{U}(\geq 20\%)}{1000} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%)}{10000} \geq 1 > \frac{\text{Pu} + {}^{233}\text{U}}{2000} + \frac{{}^{235}\text{U}(\geq 20\%)}{5000} \tag{2}$$

(c) Category III if:

$$\frac{\text{Pu} + {}^{233}\text{U}}{15} + \frac{{}^{235}\text{U}(\geq 20\%)}{15} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%)}{1000} + \frac{{}^{235}\text{U}(> \text{U}_{\text{nat}} \text{ and } < 10\%)}{10000} \geq 1 > \frac{\text{Pu} + {}^{233}\text{U}}{500} + \frac{{}^{235}\text{U}(\geq 20\%)}{1000} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%)}{10000} \tag{3}$$

(d) Below Category III if:

$$1 > \frac{\text{Pu} + {}^{233}\text{U}}{15} + \frac{{}^{235}\text{U}(\geq 20\%)}{15} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%)}{1000} + \frac{{}^{235}\text{U}(> \text{U}_{\text{nat}} \text{ and } < 10\%)}{10000} \tag{4}$$

or if the material consists only of natural uranium, depleted uranium or thorium,

where

Pu	is the mass in grams of all plutonium except that with isotopic composition exceeding 80% in ^{238}Pu;
^{233}U	is the mass in grams of ^{233}U;
^{235}U (≥20%)	is the mass in grams of ^{235}U present in a form enriched to 20% ^{235}U or more;
^{235}U (≥10% and <20%)	is the mass in grams of ^{235}U present in a form enriched to 10% ^{235}U or more, but less than 20% ^{235}U;
^{235}U (>U_{nat} and <10%)	is the mass in grams of ^{235}U present in a form enriched above natural but less than 10% ^{235}U;

and the denominators are masses in grams.

III.2. These formulas relate to material that is not irradiated in a reactor or to material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.

APPROACH 2

III.3. Another approach for determining the category of aggregated nuclear material uses the following formula:

$$\frac{1}{S} = \sum_i \frac{f_i}{S_i} \tag{5}$$

where

f_i (dimensionless)	is the mass fraction of material type i of the mixture (mass of each material type present divided by the total mass of material present);
S_i (kg or g)	is the mass threshold for material type i for the category being considered, as listed in Table 1;

and S (kg or g) is the mass threshold for the aggregation of material for the category being considered, as listed in Table 1.

III.4. The following are the mass thresholds for Category I:

(a) 2 kg of plutonium, all isotopes combined;
(b) 5 kg of ^{235}U present in a form enriched to 20% ^{235}U or more;
(c) 2 kg of ^{233}U.

III.5. The following are the mass thresholds for Category II:

(a) 500 g of plutonium, all isotopes combined;
(b) 1 kg of ^{235}U present in a form enriched to 20% ^{235}U or more;
(c) 10 kg ^{235}U present in a form enriched to at least 10% and less than 20% ^{235}U;
(d) 500 g of ^{233}U.

III.6. The following quantities are the mass thresholds for Category III:

(a) 15 g of plutonium, all isotopes combined;
(b) 15 g of ^{235}U present in a form enriched to 20% ^{235}U or more;
(c) 1 kg of ^{235}U present in a form enriched to at least 10% and less than 20% ^{235}U;
(d) 10 kg of ^{235}U present in a form enriched to less than 10% ^{235}U;
(e) 15 g of ^{233}U.

III.7. All plutonium is considered, except that with isotopic concentration exceeding 80% in ^{238}Pu.

III.8. These thresholds relate to material that is not irradiated in a reactor or to material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.

III.9. To determine the applicable category, first determine (step 1) whether the aggregated material is Category I. A material, or a mixture of materials, is Category I if the aggregated mass is greater than or equal to the Category I mass threshold calculated for the material or mixture. If it is not Category I, proceed to step 2.

III.10. If the aggregated material is not Category I, determine (step 2) whether it is Category II. A material, or a mixture of materials, is Category II if the aggregated mass is greater than or equal to the Category II mass threshold calculated for the material or mixture. If it is not Category II, proceed to step 3.

III.11. If the aggregated material is not Category I or II, determine (step 3) whether it is Category III. A material, or a mixture of materials, is Category III if the aggregated mass is greater than or equal to the Category III mass threshold calculated for the material or mixture.

III.12. If the mass of the material or mixture of materials falls below the Category III mass threshold, it is below Category III.

Example 1

III.13. The nuclear material consists of 4 kg of ^{235}U, contained in uranium enriched to greater than 20%, and 1 kg of plutonium, making a total of 5 kg of ^{235}U and plutonium combined. The mass fraction of uranium enriched to greater than 20% is 4/5 and for plutonium is 1/5.

Step 1: The Category I mass threshold for this material is given by:

$$\frac{1}{S} = \frac{4/5}{S_{\text{U-235}}} + \frac{1/5}{S_{\text{Pu}}} = \frac{4/5}{5\text{ kg}} + \frac{1/5}{2\text{ kg}} = 0.26$$

Therefore, S = 3.85 kg. Since the mass of the material (5 kg) is greater than S (3.85 kg), it is above the threshold for Category I for this mixture.

The material is therefore a Category I quantity.

Example 2

III.14. The nuclear material consists of 2.5 kg of ^{235}U, contained in uranium enriched to greater than 20%, and 500 g of plutonium, making a total of 3 kg of ^{235}U and plutonium combined. The mass fraction of uranium enriched to greater than 20% is 2.5/3 (or 5/6) and for plutonium is 0.5/3 (or 1/6).

Step 1: The Category I mass threshold for this material is given by:

$$\frac{1}{S} = \frac{5/6}{S_{\text{U-235}}} + \frac{1/6}{S_{\text{Pu}}} = \frac{5/6}{5\text{ kg}} + \frac{1/6}{2\text{ kg}} = 0.25$$

Therefore, S = 4 kg. The total mass is 3 kg, which is below the mass threshold for the mixture for Category I.

Step 2: The Category II mass threshold for this material is given by:

$$\frac{1}{S} = \frac{5/6}{S_{\text{U-235}}} + \frac{1/6}{S_{\text{Pu}}} = \frac{5/6}{1\text{ kg}} + \frac{1/6}{0.5\text{ kg}}$$

Therefore, $S = 0.86$ kg. The total mass is 3 kg, which is above the mass threshold for the mixture for Category II. Therefore, the mixture is Category II.

Appendix IV

CROSS-REFERENCES TO RECOMMENDATIONS

Table 4 provides cross-references between paragraphs in Ref. [1] and the related paragraphs in this publication.

TABLE 4. CROSS-REFERENCES TO RECOMMENDATIONS [1]

Paragraph(s) in Recommendations [1]	Related paragraphs in this publication
INTRODUCTION	Section 1
Background (1.1–1.8)	
Purpose (1.9–1.11)	
Scope (1.12–1.18)	
Structure (1.19–1.24)	
OBJECTIVES OF A STATE'S PHYSICAL PROTECTION REGIME (2.1–2.3)	Section 2
ELEMENTS OF A STATE'S PHYSICAL PROTECTION REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES	
State responsibility (3.1, 3.2)	3.5–3.7
International transport (3.3–3.7)	Covered in Ref. [2]
Assignment of physical protection responsibilities (3.8)	3.8–3.11
Legislative and regulatory framework	
Legislative and regulatory framework (3.9–3.17)	3.12–3.32
Competent authority (3.18–3.22)	3.39–3.48
Responsibilities of the licence holders (3.23–3.30)	3.49, 4.4–4.13, 4.154–4.161

TABLE 4. CROSS-REFERENCES TO RECOMMENDATIONS [1] (cont.)

Paragraph(s) in Recommendations [1]	Related paragraphs in this guide
International cooperation and assistance (3.31–3.33)	3.50–3.54
Identification and assessment of threats (3.34–3.40)	3.55–3.63
Risk based physical protection system and measures	
Risk management (3.41, 3.42)	3.64–3.103
Graded approach (3.43, 3.44)	3.70–3.101
Defence in depth (3.45–3.47)	3.102, 3.103
Sustaining the physical protection regime	
Security culture (3.48–3.51)	3.105, 3.106
Quality assurance (3.52)	3.107–3.110
Confidentiality (3.53–3.55)	3.111–3.115
Sustainability programme (3.56, 3.57)	3.119
Planning and preparedness for and response to nuclear security events (3.58–3.62)	3.120–3.126
REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE	4.4–4.14, 4.23–4.59, 4.71–4.75, 4.124–4.139
General	
Basis for concern (4.1–4.4)	
Categorization (4.5–4.8)	3.74–3.90
Requirements for physical protection against unauthorized removal in use and storage	
General (4.9–4.12)	4.83–4.123, 4.133–4.146

TABLE 4. CROSS-REFERENCES TO RECOMMENDATIONS [1] (cont.)

Paragraph(s) in Recommendations [1]	Related paragraphs in this guide
Requirements for Categories I, II and III nuclear material (4.13–4.20)	4.33–4.59, 4.83–4.123
Requirements for Categories I and II nuclear material (4.21–4.35)	4.33–4.59, 4.83–4.123
Requirements for Category I nuclear material (4.36–4.49)	4.33–4.59, 4.83–4.123
Requirements for measures to locate and recover missing or stolen nuclear material	4.71–4.75
Requirements for the State (4.50–4.56)	
Requirements for the operator (4.57–4.63)	
REQUIREMENTS FOR MEASURES AGAINST SABOTAGE OF NUCLEAR FACILITIES AND NUCLEAR MATERIAL IN USE AND STORAGE	4.4–4.14, 4.23–4.59, 4.76–4.82, 4.133–4.146
General (5.1–5.3)	
Basis for a graded approach for physical protection against sabotage (5.4–5.8)	3.91–3.101
Requirements for the process to design a physical protection system against sabotage (5.9–5.19)	4.140–4.153
Requirements for physical protection against sabotage at nuclear facilities	4.33–4.59, 4.83–4.123
Requirements for high consequence facilities including nuclear power plants (5.20–5.42)	4.33–4.59, 4.83–4.123
Requirements for other nuclear facilities and nuclear material (5.43)	5.20–5.42

TABLE 4. CROSS-REFERENCES TO RECOMMENDATIONS [1] (cont.)

Paragraph(s) in Recommendations [1]	Related paragraphs in this guide
Requirements for associated measures to mitigate or minimize the radiological consequences of sabotage	4.76–4.82
Scope and boundary (5.44)	
Requirements for the State (5.45–5.53)	
Requirements for the operator (5.54–5.58)	

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[7] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[10] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).
[12] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Physical Protection of Nuclear Materials and Facilities, IAEA-TECDOC-1276, IAEA, Vienna (2002).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

IAEA
International Atomic Energy Agency

No. 25

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

CANADA

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.
Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

FRANCE

Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: www.libreriaaeiou.eu

JAPAN

Maruzen-Yushodo Co., Ltd
10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302 or +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT
IAEA Nuclear Security Series No. 10
STI/PUB/1386 (30 pp.; 2009)
ISBN 978-92-0-102509-8 Price: €18.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8
STI/PUB/1359 (25 pp.; 2008)
ISBN 978-92-0-109908-2 Price: €20.00

NUCLEAR SECURITY CULTURE
IAEA Nuclear Security Series No. 7
STI/PUB/1347 (37 pp.; 2008)
ISBN 978-92-0-107808-7 Price: €30.00

IDENTIFICATION OF VITAL AREAS AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 16
STI/PUB/1505 (37 pp.; 2013)
ISBN 978-92-0-114410-2 Price: €22.00

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

This publication is the lead Implementing Guide in a suite of guidance on the implementation of IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).

The guide focuses on the physical protection of nuclear material against unauthorised removal and of nuclear material and nuclear facilities against sabotage. It provides guidance to States and their competent authorities on how to establish, strengthen and sustain their national physical protection regime and how to implement the associated systems and measures, including operators' physical protection systems.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–111516–4
ISSN 1816–9317