IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

No. 49-T

Evaluation of Physical Protection Systems at Nuclear Facilities

TECHNICAL GUIDANCE

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.

EVALUATION OF PHYSICAL PROTECTION SYSTEMS AT NUCLEAR FACILITIES

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS, THE
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CABO VERDE
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COOK ISLANDS
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
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GAMBIA, THE
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUINEA
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, KINGDOM OF THE
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT KITTS AND NEVIS
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOMALIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TONGA
TRINIDAD AND TOBAGO
TUNISIA
TÜRKİYE
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. 49-T

EVALUATION OF PHYSICAL PROTECTION SYSTEMS AT NUCLEAR FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2025

COPYRIGHT NOTICE

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
tel.: +43 1 2600 22529 or 22530
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
July 2025
STI/PUB/2104
https://doi.org/10.61092/iaea.pckz-it39

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Evaluation of physical protection systems at nuclear facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2025. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 49-T | Includes bibliographical references.
Identifiers: IAEAL 25-01762 | ISBN 978-92-0-137124-9 (paperback : alk. paper) | ISBN 978-92-0-137224-6 (pdf) | ISBN 978-92-0-137324-3 (epub)
Subjects: LCSH: Nuclear facilities — Safety regulations. | Nuclear facilities — Security systems. | Radioactive substances — Law and legislation. | Nuclear nonproliferation.
Classification: UDC 341.67 | STI/PUB/2104

FOREWORD

by Rafael Mariano Grossi
Director General

The IAEA Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The IAEA establishes and maintains this guidance as part of its central role in providing nuclear security related international support and coordination.

The IAEA Nuclear Security Series was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States. As Director General, I am committed to ensuring that the IAEA maintains and improves upon this integrated, comprehensive and consistent set of up to date, user friendly and fit for purpose security guidance publications of high quality. The proper application of this guidance in the use of nuclear science and technology should offer a high level of nuclear security and provide the confidence necessary to allow for the ongoing use of nuclear technology for the benefit of all.

Nuclear security is a national responsibility. The IAEA Nuclear Security Series complements international legal instruments on nuclear security and serves as a global reference to help parties meet their obligations. While the security guidance is not legally binding on Member States, it is widely applied. It has become an indispensable reference point and a common denominator for the vast majority of Member States that have adopted this guidance for use in national regulations to enhance nuclear security in nuclear power generation, research reactors and fuel cycle facilities as well as in nuclear applications in medicine, industry, agriculture and research.

The guidance provided in the IAEA Nuclear Security Series is based on the practical experience of its Member States and produced through international consensus. The involvement of the members of the Nuclear Security Guidance Committee and others is particularly important, and I am grateful to all those who contribute their knowledge and expertise to this endeavour.

The IAEA also uses the guidance in the IAEA Nuclear Security Series when it assists Member States through its review missions and advisory services. This helps Member States in the application of this guidance and enables valuable experience and insight to be shared. Feedback from these missions and services, and lessons identified from events and experience in the use and application of security guidance, are taken into account during their periodic revision.

I believe the guidance provided in the IAEA Nuclear Security Series and its application make an invaluable contribution to ensuring a high level of nuclear security in the use of nuclear technology. I encourage all Member States to promote and apply this guidance, and to work with the IAEA to uphold its quality now and in the future.

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.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The physical protection of nuclear material and nuclear facilities is an essential component of the nuclear security regimes of 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], provides States with recommendations on developing (or enhancing), implementing and sustaining effective physical protection and emphasizes in particular the importance of evaluating physical protection systems (PPSs), including through performance testing. IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [2], offers guidance on how to implement those recommendations.

1.2. The Convention on the Physical Protection of Nuclear Material [3] establishes legal obligations for States Parties to the Convention regarding physical protection during international transport of nuclear material used for peaceful purposes. The 2005 Amendment to the Convention on the Physical Protection of Nuclear Material [4] entered into force on 8 May 2016 and extends the scope of the Convention to cover nuclear material and nuclear facilities used for peaceful purposes in domestic use, storage and transport, and the sabotage of such material or facilities. Reference [1] provides guidance to States Parties to the Convention and its Amendment on meeting their obligations.

1.3. Ensuring that the PPS at a nuclear facility is operating as designed is crucial for the security of the nuclear material and the nuclear facility itself. Evaluating the individual components of the PPS, as well as the system as a whole, provides a measure of the effectiveness of the facility's PPS. This publication provides guidance on the methods that can be used to conduct such evaluations.

OBJECTIVE

1.4. This publication provides technical guidance for States, competent authorities and operators on evaluating the effectiveness of PPSs in order to protect (a) nuclear material in use and in storage against unauthorized removal and (b) nuclear material and facilities against sabotage.

SCOPE

1.5. This publication covers methods for evaluating the effectiveness of a PPS and methods for evaluating nuclear material accounting and control procedures and systems for nuclear material and nuclear facilities. This guidance may also be applied to the evaluation of security measures for other radioactive material and associated facilities and activities.

1.6. This publication does not include the assessment of computer security for the protection of nuclear facilities, although some aspects of blended attacks (i.e. combined cyber-attacks and physical attacks) are considered in the context of evaluating a PPS. Information on the assessment of computer security can be found in IAEA Nuclear Security Series Nos 42-G, Computer Security for Nuclear Security [5]; 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities [6]; and 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [7].

1.7. Although this publication does not explicitly address evaluation of the effectiveness of measures protecting against aircraft or stand-off attacks, it presents general methods for doing so that may be used to protect against such attacks based on national threat statements.

1.8. The following topics are outside the scope of this publication:

(a) The security of nuclear material in transport (see Ref. [1] and IAEA Nuclear Security Series No. 26-G, Security of Nuclear Material in Transport [8] for further guidance);
(b) Response to a nuclear or radiological emergency that could result from a nuclear security event (see IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [9]);
(c) Mitigation or minimization of the radiological consequences of sabotage at nuclear facilities (see GSR Part 7 [9]);
(d) Location and recovery of nuclear material out of regulatory control (see IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [10] for further guidance);
(e) Physical protection considerations in the siting of nuclear facilities (see IAEA Nuclear Security Series No. 35-G, Security During the Lifetime of a Nuclear Facility [11] for further guidance).

STRUCTURE

1.9. Section 2 of this publication provides an overview of the evaluation of a PPS. A detailed description of evaluation processes and methods to verify that protection requirements are met is given in Section 3. Section 4 provides guidance on the considerations to be taken into account when developing a performance based evaluation programme for a PPS. The Appendix describes considerations relating to the establishment of a process for the evaluation of the effectiveness of a PPS. Annexes I–XIV outline examples of test plans for different protection elements, and Annex XV gives examples of root causes that can lead to deficiencies in a PPS. Methods for evaluating nuclear material accounting and control elements to evaluate the effectiveness of a PPS are presented in Annex XVI. Annex XVII provides examples of the use of insider analysis to evaluate the effectiveness of the PPS against the abrupt or protracted theft of nuclear material.

2. OVERVIEW OF THE EVALUATION OF PHYSICAL PROTECTION SYSTEMS

2.1. Paragraph 3.12 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [12], states:

> "A *nuclear security regime* ensures that each *competent authority* and *authorized person* and other organizations with nuclear security responsibilities contribute to the sustainability of the *regime* by:
>
> …….
>
> (e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the *nuclear security systems*;
>
> …….
>
> (h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times."

METHODOLOGICAL FRAMEWORK FOR THE EVALUATION OF THE EFFECTIVENESS OF A PHYSICAL PROTECTION SYSTEM

2.2. The primary purpose of effectiveness evaluation and testing is to determine if the applicable security requirements for the facility or the activity are met. These requirements can be based on prescriptive requirements, performance requirements, or a combination of the two, as defined by the relevant competent authority or the State. In addition, the evaluation provides insights into the strengths and weaknesses of the PPS. Effectiveness evaluations that repeatedly and consistently reveal the same or similar weaknesses in a security system suggest that the problems are generalized and are best addressed at a strategic level. If weaknesses are identified, appropriate remedial actions should be taken to rectify the issues, after which the facility can be re-evaluated.

2.3. The operator is responsible and accountable for the physical protection of the facility and the associated material. As such, the operator ensures that security measures are appropriate and effective and comply with regulations. Even if a particular security measure is not a regulatory requirement, it is in the operator's interests to conduct periodic performance based effectiveness evaluations to provide continued assurance of the measure's effectiveness and to strengthen the confidence of stakeholders in the security measures.

2.4. In addition to evaluating the compliance of the PPS with regulatory requirements, the competent authority may wish to initiate evaluations to ensure that existing physical protection measures are effective. The operator needs to consider both the efficiency and the effectiveness of these PPS elements, taking into account the costs associated with the measures [13].

2.5. Figure 1 illustrates the methodological framework presented in Ref. [13] and used in this publication for the evaluation of the effectiveness of a PPS. The first step is planning the evaluation process. The second and third steps consist of collecting the relevant information and conducting the evaluation. The fourth step is to assess the security measures against the security requirements. Following this, it is necessary to determine if the overall level of security meets the security requirements. If the overall level of security does not meet the security requirements, then security upgrades or modifications should be identified and the PPS should be re-evaluated for its effectiveness. If the overall level of security meets the security requirements, then the evaluation process is complete.

2.6. Specific background information is needed for many of the steps described in paras 2.7–2.12. Evaluations of background information may, for example,

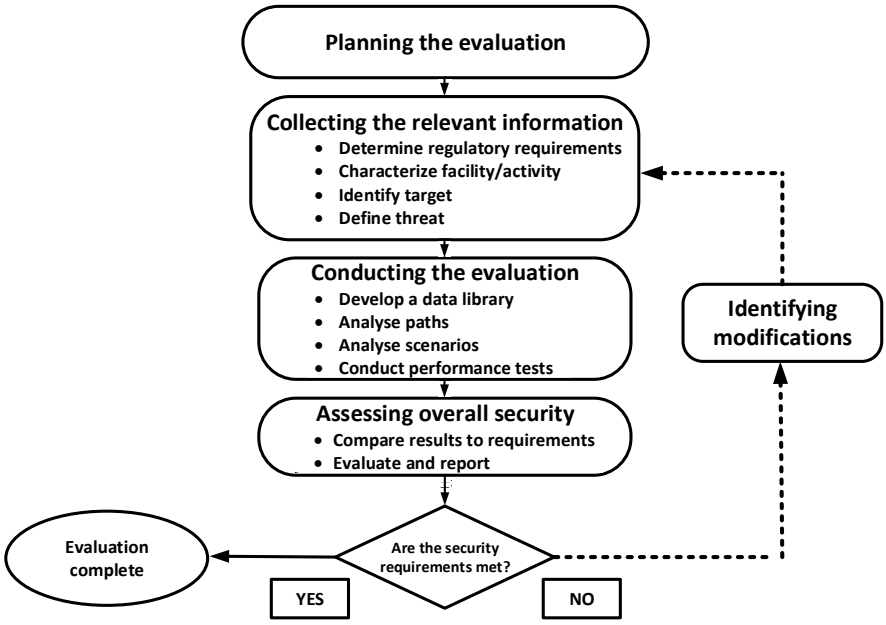


FIG. 1. The methodological framework for the evaluation of the effectiveness of a physical protection system (adapted from Ref. [13]).

reveal security shortcomings that need to be addressed before conducting an effectiveness evaluation.

Planning the evaluation

2.7. Activities that are undertaken during the evaluation planning step may involve external organizations. This step should result in a project plan or other planning document.

2.8. Deciding on the purpose of the evaluation should include determining the objectives of the nuclear security system, the proposed design or characterization of an existing nuclear security system, the evaluation of the design, and possible PPS redesign or refinements. (See the Appendix for more details.)

Collecting the relevant information

2.9. When planning the evaluation of the effectiveness of a PPS, the following information should be collected:

(a) Relevant regulatory requirements and reports. The starting point of the methodology is collecting information on the existing national regulatory framework, policies and guidance on which the PPS is based. Information of interest may include inspection reports, corrective actions and recommendations from previous evaluations of the PPS.
(b) Information on the facility configuration and activities. This includes information on the operations and activities at the facility, a comprehensive description of the facility itself, the operating conditions, the physical protection requirements, as well as the regulatory requirements. This information should be well documented by the facility and made available to the competent authority.
(c) Information on targets in the facility or in the associated activity. This information includes descriptions of the nuclear material in the facility and of the vital areas in the facility, based on the information collected during the characterization of the facility. The necessary level of protection of these targets against theft or sabotage is determined mainly on the basis of the type of material and the risk (i.e. the potential radiological consequences associated with the target). Objectives can thus be identified for the PPS (e.g. what to protect, against whom, at what level) on the basis of the information collected.
(d) Information on the design basis threat or the representative threat statement. This information is based on the national security policy defined by the State and on other considerations, such as the type of facility or activity, the local conditions at the facility or activity, and the adversary profile (e.g. possible intent, motivation, types, capabilities, range of tactics).

Conducting the evaluation

2.10. Evaluating the effectiveness of a PPS typically includes the following activities:

(a) Developing a data library. Data libraries are collections of data from performance testing of the PPS that can be used as a basis to estimate the probability of detection, the probability of accurate assessment, or the delay times that are used in modelling and simulation activities. Such data libraries can be developed and maintained as part of an evaluation programme or

process, including during verification of the compliance of the PPS with regulatory requirements and during enforcement activities. The data should be collected in the initial stages of the evaluation process and should be used for the characterization of the facility, providing documented evidence of the results of the effectiveness evaluation of the facility.

(b) Conducting a path analysis. A path analysis is an evaluation method to determine whether the PPS is effective across all paths that an adversary might take to attempt the unauthorized removal of nuclear material or sabotage at the facility. Guidance on conducting path analyses is given in paras 3.42–3.44.

(c) Conducting a scenario analysis. Scenarios are hypothetical sets of conditions and sequences of events constructed for the purpose of PPS evaluations. A scenario analysis is the process of using paper models, tabletop exercises, two dimensional and three dimensional computer simulations, and other evaluation methods to evaluate these scenarios. Guidance on conducting a scenario analysis is given in paras 3.47–3.61.

(d) Conducting performance testing. Performance testing is used to validate the ability of a PPS to meet performance requirements, but it may also be necessary when a prescribed measure has to meet a technical criterion or specification (see IAEA Nuclear Security Series No. 40-T, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities [14]). Guidance on conducting performance tests is given in paras 3.66–3.116.

Assessing overall security

2.11. This step entails comparing the results of the evaluation of the effectiveness of the PPS with the PPS objectives defined in regulatory requirements. The results should indicate whether the PPS as designed — or (for an existing system) as characterized — satisfies the physical protection requirements and should identify any system deficiencies and vulnerabilities in the design or implementation of the PPS that should be addressed to meet the PPS requirements.

2.12. An assessment report should be prepared to document the results and findings of the evaluation, and it should identify any corrective actions needed. This report should be submitted to the competent authority, as appropriate, or as required by the regulations.

ROLE OF RISK MANAGEMENT IN THE EVALUATION OF EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEMS

2.13. Paragraph 3.41 of Ref. [1] states that "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."

2.14. Paragraph 3.65 of Ref. [2] states:

> "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."

2.15. Risk management can thus be used to identify whether additional measures are required to reduce risks. In a risk management approach, either the State or the competent authority identifies an acceptable level of risk, above which additional protection measures are required. Risk management decisions are derived from evaluations of the effectiveness of the PPS and from performance testing. More detailed guidance on risk management can be found in Ref. [2].

PERFORMANCE METRICS FOR A PHYSICAL PROTECTION SYSTEM

2.16. The performance metrics for a PPS can be developed by the competent authority in consultation with relevant stakeholders using a graded approach or a risk-informed approach. These metrics can then be used to evaluate the functions of the PPS, more specifically the functions of detection, delay and response. The individual performance of each PPS element is taken as input to determine the effectiveness of the PPS qualitatively and quantitatively.

2.17. Detection is a process in a PPS, which begins with the sensing of a potentially criminal or intentional unauthorized act and concludes with the assessment of the cause of the alarm. The associated performance metric is the probability of detection, which is a product of the probability of sensing and the probability of assessment.

2.18. Delay is the function of a PPS designed to increase adversary penetration time for entry into and/or exit from the nuclear facility, thereby providing more time for effective response. The associated performance metric is the delay time necessary to ensure an effective PPS.

2.19. Response is the function of a PPS that seeks to interrupt and neutralize an adversary before the completion of a criminal or intentional unauthorized act. Two performance metrics are associated with response: the probability of interruption and the probability of neutralization. The probability of interruption is the probability that the response will reach adversaries before the criminal or intentional unauthorized act is accomplished. The probability of neutralization is the probability that the response can stop adversaries before their goal is accomplished or can cause the adversaries to abandon their attempt to remove material or sabotage a facility.

CHARACTERIZATION OF THE PERFORMANCE METRICS FOR A PHYSICAL PROTECTION SYSTEM

2.20. Methods for characterizing the performance metrics for the components of a PPS include the use of models and simulations, statistical data derived from testing, and expert judgement.

2.21. Models and simulations should be used to characterize performance metrics when direct testing cannot be performed, which often occurs because of safety concerns relating to testing, when destructive testing is needed or when the level of testing needed to collect the desired data is cost prohibitive. Models and simulations range from semi-quantitative tools that assess security at facilities with predominantly prescriptive requirements to complex tools that assess security at facilities governed by performance based requirements. Modelling and simulation methods include manual or computer based mathematical models, computer simulations and tabletop exercises.

2.22. Statistical data from the performance tests and the simulations are used to characterize performance metrics. These data are gathered through statistical sampling and testing. Statistical data may also be derived from other sources, such as national testing organizations, civil or military agencies, vendors, national or international publications, or security event databases.

2.23. Expert judgement can also be used during the characterization of performance metrics, particularly in the absence of data or in the absence of an efficient means

of conducting tests to correctly collect the data. In such cases, the evaluation depends on values elicited from subject matter experts, based on their experience.

2.24. Owing to the strengths and limitations inherent in each evaluation method, multiple methods may be needed to obtain a comprehensive understanding of the effectiveness of the PPS. If multiple methods are used, a means of comparing the results of the different methods (e.g. a scale to compare qualitative results with quantitative results) should be available. All these methods should be implemented with the support of subject matter experts with practical experience and knowledge of the threats included in the design basis threat or the representative threat statement as well as the capability to understand the merits and limits of these methods in relation to the threats.

INTERFACE OF THE NUCLEAR MATERIAL ACCOUNTING AND CONTROL SYSTEM WITH THE PHYSICAL PROTECTION SYSTEM

2.25. Nuclear material accounting and control measures are an important element in protection against an adversary who might attempt the unauthorized removal of nuclear material. Measures against this threat are presented in detail in IAEA Nuclear Security Series Nos 8-G (Rev. 1), Preventive and Protective Measures Against Insider Threats [15], and 32-T, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility During Use, Storage and Movement [16].

2.26. To determine the effectiveness of a PPS to protect against potential adversaries defined in the design basis threat or the representative threat statement, a comprehensive analysis should be performed that includes addressing potential insider threats. These could involve either an insider adversary acting alone or in collusion with another insider adversary, or an insider acting with external adversaries.

2.27. The system for nuclear material accounting and control operates in coordination with the PPS to control access to areas where nuclear material is stored or used and to provide measures for controlling the nuclear material. Many of these measures are also used as, or complement, physical protection measures (e.g. access control, video surveillance systems, the two-person rule, daily checks, radiation detection alarms). Information from the system for nuclear material accounting and control can be used to determine the type, quantity and isotopic composition of nuclear material; its categorization; and its location, use and movement within the facility. This information, in turn, can be used to support

the selection of the appropriate protective measures. As part of the programme for nuclear material accounting and control, non-destructive analysis tools and methods can be used to detect unauthorized changes in the nuclear material. A comprehensive evaluation of the PPS should therefore include an evaluation of the system for nuclear material accounting and control, particularly in the case of an interface between physical protection measures and nuclear material accounting and control measures.

2.28. Records should be kept concerning all nuclear material on the site. Protecting the nuclear material at a facility includes maintaining control over the material. The nuclear material accounting and control system of the facility keeps records on the nuclear material and on administrative and technical control measures. Accounting records, data and associated systems should all be protected and secured from unauthorized access, data removal and/or data alteration.

2.29. Examples of the use of nuclear material accounting and control elements in an evaluation of the PPS are provided in Annex XVI. More information on nuclear material accounting and control can be found in IAEA Nuclear Security Series No. 25-G, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities [17].

ROLE OF COMPETENT AUTHORITY PERSONNEL IN THE CONDUCT OF EVALUATIONS

2.30. The method used by the competent authority personnel to conduct PPS evaluations and regulatory oversight thereof depends on the regulatory approach used (i.e. performance based, prescriptive, or combined) and the types and numbers of nuclear facilities and activities within the State.

2.31. A performance based regulatory approach for PPS evaluation usually includes a combination of analyses and performance testing. This approach often necessitates that the operator conduct the analyses and testing, which are then reviewed by the competent authority. This type of review takes time and involves sufficient knowledge on the part of the competent authority personnel to verify that the analyses and testing have been performed correctly and that the conclusions are accurate. An approach that includes analyses and testing conducted independently by the competent authority usually takes more time and involves significant knowledge, skills and experience on the part of the competent authority personnel in analysis and performance testing methods.

2.32. Assessments conducted under a prescriptive regulatory approach are generally not as resource intensive as those conducted under a performance based approach. Sufficient time should nevertheless be allotted to ensure that all the prescriptive requirements are met. Moreover, the personnel conducting the assessment should have sufficient knowledge, skills and experience to determine whether the PPS measures in place adequately meet the prescriptive requirements.

2.33. Facilities that store or use Category I or II nuclear material and facilities that are classified as potentially having unacceptable or very high radiological consequences, need to be evaluated more frequently and in more depth than facilities classified as having lower potential radiological consequences. A performance based or combined regulatory approach should be applied to facilities classified as having higher potential radiological consequences. Consequently, for the evaluation of these facilities, the competent authority needs significantly more resources than for the evaluation of other types of facility.

2.34. Given the critical nature of the facilities being assessed, the workload of the assessment personnel should be managed to prevent impacts on assessment performance. A realistic evaluation should be made regarding the time, effort and skill set needed to perform an assessment of each type of facility falling under the purview of the competent authority; this evaluation should be based on the regulatory approach and the potential risk associated with the facility. This evaluation, combined with a calculation of the number of facilities to be evaluated, should be factored into determining the optimum staffing levels for the competent authority and the necessary qualifications and experience of the personnel conducting the assessments.

3. PROCESS FOR THE EVALUATION OF THE EFFECTIVENESS OF A PHYSICAL PROTECTION SYSTEM

3.1. This section describes in detail the process for the evaluation of the effectiveness of a PPS, as outlined in Fig. 1.

METHODS FOR THE EVALUATION OF A PHYSICAL PROTECTION SYSTEM

3.2. The methods used to evaluate the effectiveness of a PPS can be based on different approaches that have been defined by the competent authority and are either prescriptive or performance based or a combination of both. In accordance with a graded approach, the PPS for lower consequence targets is typically evaluated using a prescriptive approach and the PPS for higher consequence targets is typically evaluated using a performance based or combined approach.

3.3. When using a prescriptive approach, the methods for evaluating the effectiveness of a PPS should include a review of the following: operational plans and procedures, records and logs, personnel training, specific PPS features, and interviews and observations on the operation of the PPS. Such methods use a checklist approach, verifying if each applicable prescriptive requirement is met or not.

3.4. When using a performance based approach, the methods for evaluating the effectiveness of a PPS should include performance testing, simulations and use of analysis tools. These methods demand a higher level of involvement by the operator and therefore need more time, data and resources than the prescriptive methods. Performance based evaluations determine if the PPS design is effective against the adversary capabilities defined in the design basis threat or the representative threat statement.

3.5. A combined approach uses methods from both the prescriptive approach and the performance based approach. All three approaches are presented in more detail in paras 3.8–3.31, and additional guidance can be found in Refs [1, 2].

3.6. The methods used for the evaluation of the effectiveness of the PPS may range from simple to complex, they may involve response tests and manual evaluation methods or complex computer simulations, they may be prescriptive or performance based, and they may involve limited scope performance tests or full scope performance tests. Combinations of these methods can also be used. As each type of evaluation method has its own strengths and weaknesses, multiple evaluation methods should be used in a complementary fashion to take advantage of the strengths and offset the weaknesses of each individual method.

3.7. Table 1 lists different methods for the evaluation of the effectiveness of a PPS and provides a short description and an example for each method [13].

TABLE 1. METHODS FOR THE EVALUATION OF THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEMS [13]

Method	Description
Manual	
Checklist for evaluation against prescriptive requirements	A qualitative tool to determine the presence or absence of required features or the adequacy or inadequacy of a required capability. Checklists examine how a system meets requirements from a high level perspective, allowing the user to identify areas that need more extensive evaluation. The checklist may also record adjectival scores assigned by an expert, such as the 'high', 'medium' or 'low' effectiveness of some equipment or a security procedure against the threat (the design basis threat or the representative threat statement), based on an inspection of equipment or analysis of the procedure.
Observation	A method that consists of observing a process or procedure to provide insight on how well the process or the procedure is performed. This method is often used for cases in which the evaluator does not want to disrupt the process or procedure using more intrusive methods. An example of observation is when an evaluator is present in an alarm station to observe whether the alarm station operators are assessing alarms in accordance with the existing procedure.
Random sampling	A method to determine a subset of items to be examined and then deduce conclusions about the overall set of items. Sampling can be used to determine which items to inspect (i.e. to review or examine for certain required features) or to test the performance of a feature. For example, the evaluator may select from a set of material transfer forms, see whether they are completed correctly, and then determine how well the site personnel are adhering to procedures for completing the forms. As another example, if the site has a number of sensors, sampling might be used to determine which sensors to test during an audit.
Tabletop	
Map exercise	An exercise using small models of guards, response forces and adversaries placed on one or more maps.
Scale model (sand table) exercise	An exercise using small models of combatants on a scale model of a facility or area that includes terrain features, vegetation, roads and buildings. (It is called a sand table exercise because it was historically performed on a table where the terrain was modelled in sand.)

TABLE 1. METHODS FOR THE EVALUATION OF THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEMS [13] (cont.)

Method	Description
Computer based exercise	An exercise that involves moving icons of guards, response forces and adversaries on a computer display of a facility.
Computer simulation	
Human in the loop	Evaluators control activities performed by computer generated adversaries and defenders within an environment modelled on a computer.
Human out of the loop (constructive simulation or automated behaviour)	Software routines (not evaluators) control activities performed by computer generated adversaries and defenders within an environment modelled on a computer.
Single path	A method that calculates the probability of interruption for a single adversary path.
Performance testing	
Barrier testing at a State or competent authority laboratory	A method for testing access delay systems involving either active or passive delay. Experts develop delay times against the design basis threat or the representative threat statement to be used in evaluations and may provide guidance for facilities on making upgrades.
Testing for response force equipment at a State or competent authority laboratory	A method for testing response force equipment, such as weapons, protective gear and fighting positions. Experts provide guidance on what response force equipment to use at facilities and on the training needed for operating such equipment. Experts may also support force-on-force exercises.
Facility level testing (includes component testing and subsystem testing)	Facility testing, which could include functional or operability tests to ensure that individual components are working; standardized maintenance performance tests to ensure that such components meet performance requirements; simulated adversarial attack tests by skilled testers; and physical protection subsystem tests (e.g. to determine if an alarm generated on the perimeter is acknowledged and assessed in accordance with procedures by the personnel of the alarm station).

TABLE 1. METHODS FOR THE EVALUATION OF THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEMS [13] (cont.)

Method	Description
Resistance testing	Experiments to evaluate the resistance of structures and physical protection measures against explosives, weapons, vehicles, etc.
Response test	
Alarm response test	Performance test to assess the readiness of the response force and of the response to an alarm by a group of responders that move to a specific location.
Limited scope performance test	Test to determine the performance level of an individual in performing security force or guard force responsibilities. Examples include the effectiveness of searches, the assessment of alarms by the personnel of the central alarm station, and procedures for the use of force when engaging with the adversary.
Force-on-force exercises	A performance test of the physical protection system that uses designated personnel in the role of an adversary force to simulate an attack consistent with the design basis threat or the representative threat statement. This is typically a full scale field simulation of an attack on the site, involving all on-site guards and response forces.

Prescriptive approach for the evaluation of a physical protection system

3.8. Paragraph 3.22 of Ref. [2] states:

> "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."

3.9. The evaluation of a PPS against prescriptive requirements should consist of understanding the requirements, collecting information and then comparing the information against the requirements to confirm compliance. The prescriptive approach should result in an objective assessment of the compliance of the PPS with each prescriptive requirement.

3.10. In the prescriptive approach, requirements for the evaluation of the PPS should be established by the competent authority prior to conducting an evaluation. These requirements should establish the baseline for the regulatory prescriptive evaluation to determine the scope and criteria against which the PPS requirements are to be evaluated. The competent authority can choose to develop a simple checklist outlining the requirements for evaluation to guide the evaluation and document the results.

3.11. Compliance with prescriptive requirements can usually be evaluated by the competent authority through observations made at the nuclear facility (e.g. during regulatory inspections). Such evaluations should include the following:

(a) Review of security plans, procedures, processes and records, including records of personnel training (see paras 3.13–3.18);
(b) Interviews with personnel and knowledge testing (see para. 3.19);
(c) Reviews of specific PPS features, including specialized security equipment (see para. 3.20);
(d) Direct observation of the deployment of security personnel in accordance with security plans.

3.12. The use of the prescriptive approach in the evaluation of a PPS is effective in determining the compliance of the PPS with the regulatory requirements, but the approach is limited in determining the effectiveness of the PPS.

Review of security plans

3.13. The evaluation should verify that the physical protection measures described in the approved security plan comply with regulatory requirements and applicable licence conditions. The evaluation can be performed through a direct prescriptive comparison between the details of the approved security plan and the plan's implementation. Detailed guidance on security plans and the suggested contents can be found in Ref. [2].

3.14. The following are examples of questions that can be used for the direct prescriptive comparison:

(a) Do the security organizational structure at the facility and personnel responsibilities comply with the approved security plan requirements?
(b) Have security operational plans been developed and kept up to date, as required?

(c) Are memorandums of understanding for external response in place and up to date?
(d) Does the security plan document the facility management and organizational structure, as well as the role of the responders from external organizations who do not belong to the facility's security organization but have physical protection responsibilities?
(e) Are security procedures available and implemented as described in the security plan?

Review of procedures and processes

3.15. A prescriptive evaluation should include a review of the approved procedures and processes described in the approved facility security plan. This review should determine if the procedures are being implemented, maintained and periodically revised as approved by the competent authority. Information related to both the evaluation and the security plan should be protected and secured from unauthorized access or data removal.

3.16. The following are examples of questions that can be used in the review of procedures and processes:

(a) Are the locks on doors and gates kept locked and monitored in accordance with the procedure?
(b) Are logs of personnel entering and leaving certain areas maintained and accurately recorded?
(c) Are guard personnel posted at all times in accordance with the security plan?
(d) Are all the primary components of the emergency communication process in place and operable? Are the responsible personnel aware of the communication process?
(e) Are evacuation procedures clearly identified, communicated to all personnel and practised?

Review of records

3.17. A prescriptive evaluation should include a review of the facility records and operational records, along with the personnel training records, to assess compliance with the regulatory requirements. Recognized inspection sampling techniques should be used to verify that records have been consistently developed and are up to date, accurately completed and effectively managed.

3.18. The evaluation of security training should include examination of training plans and course material, observation of training, and conduct of interviews with personnel to verify their capability to perform the procedures or activities covered in the training programmes.

Interviews with personnel and knowledge testing

3.19. A prescriptive evaluation should include interviews and discussions with facility personnel to determine the extent of their knowledge of current facility policies, plans and procedures. The interviews should cover procedures for normal and contingency (emergency) operation, including security response procedures. This evaluation process can be useful in determining the effectiveness of the training programme for nuclear facility personnel. Reference [18] provides additional information on interview techniques and good practices for regulatory inspectors of nuclear power plants.

Reviews of specific physical protection system features

3.20. A prescriptive evaluation should ensure that requirements for specific PPS features are met. These could be either State requirements or the requirements contained in the approved security plan and might include prescribed fence heights and provisions for redundant power sources, uninterruptible power supplies, maximum detection zone lengths, wall and barrier thicknesses, and door types. A review of procurement data should also be carried out to certify that the barrier doors meet the design specifications as well as the minimum delay values used in the effectiveness evaluation. Facility walkdowns should be conducted to ensure that physical protection measures on building elements (e.g. doors, windows, vents) are in place and performing as required. Facility walkdowns are an effective method for assessing facility conditions (e.g. access controls, guard duties, lighting conditions) and should be used to provide initial insights into physical protection operations at the facility and to determine if a more detailed evaluation is needed.

Performance based approach for the evaluation of a physical protection system

3.21. Paragraph 3.18 of Ref. [2] states:

> "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."

3.22. To determine if physical protection measures are effective, the facility design should be analysed using simulations and performance testing. Simulations and performance testing can validate the PPS against performance requirements. They may also be needed where a prescribed measure is expected to meet a technical criterion or specification. Performance based requirements should be established by the State and should specify the acceptable level of performance of a PPS against unauthorized removal or sabotage, based on the threats defined in the design basis threat or the representative threat statement. Performance requirements for unauthorized removal should be based on the highest category of nuclear material protected by the PPS. Performance requirements for sabotage should be based on the State's defined thresholds for unacceptable radiological consequences and high radiological consequences.

3.23. The performance based approach can be highly effective in evaluating the effectiveness of a PPS because it simulates real situations and the actions and performance of equipment and personnel in different scenarios. However, conducting performance based evaluations necessitates detailed planning and the extensive involvement of personnel. It can also present scheduling challenges and involve significant costs. Guidance on a performance based approach for the evaluation of the effectiveness of a PPS is provided in Section 4.

3.24. The performance based approach for the evaluation of the effectiveness of a PPS may include the following:

(a) Modelling and simulations (see paras 3.25–3.27);
(b) Performance tests (see para. 3.28);
(c) Direct comparative reviews of other test data (see paras 3.29 and 3.30).

Modelling and simulations

3.25. Modelling and simulations can be used to evaluate the effectiveness of the PPS in meeting performance based requirements. Modelling and simulation tools range from manual, semi-quantitative tools that assess physical protection against predominantly prescriptive requirements to complex computerized tools that assess physical protection at facilities that follow performance based requirements. Modelling and simulation tools can consist of simple path analysis,

paper or tabletop models, two dimensional and three dimensional computer simulations, and virtual reality simulations.

3.26. Simulations may be conducted at existing facilities in the following cases:

(a) To collect statistical data over multiple simulation runs to evaluate the effectiveness of the PPS in a quantitative manner;
(b) To investigate PPS elements that are not practicable to assess through performance testing;
(c) To circumvent having to allow limited or restricted access to the operational environment of a nuclear facility for evaluators or response forces;
(d) To ensure an evaluation of the effectiveness of the PPS when resource restrictions and/or safety concerns render other testing impracticable.

3.27. Direct performance testing of certain physical protection measures is not possible when a nuclear facility is still in the design stage. In such cases, evaluations may be composed of modelling and simulations to determine the effectiveness of the PPS in terms of detection, delay and response. Additional information on modelling and simulations can be found in Ref. [13].

Performance tests

3.28. Performance tests can include limited scope exercises (e.g. testing of a single PPS element) and full scope exercises (e.g. force-on-force exercises) and are designed to determine if the security personnel, procedures and equipment are effective in protecting against criminal or intentional unauthorized acts.

Direct comparative reviews with other test data

3.29. When performance testing or modelling of specific physical protection measures is not possible, statistical test data for physical protection measures may be available for comparison. These may include, for example, the data resulting from testing performed by national testing organizations, civil or military agencies, or qualified vendors. Relevant data can also be found in national or international publications or in documentation on the testing of similar PPS measures (e.g. delay values of similar barriers).

3.30. Other sources of data include results that are collected as part of testing or validation activities within the facility's quality assurance programme and results from safety evaluations, safeguards validation or maintenance testing. When test

data are not available for a specific physical protection measure, expert judgement can be used to estimate the input for an effectiveness evaluation.

Combined approach for the evaluation of a physical protection system

3.31. The combined approach includes elements from both the prescriptive approach and the performance based approach. It uses the strengths of both approaches, and thus allows for greater flexibility. The evaluation against prescriptive requirements should be performed before other performance based or combined evaluations can proceed. At a minimum, the deficiencies identified through the verification of prescriptive requirements should be corrected prior to performing more extensive performance based or combined evaluations in order to ensure reliable results. More information on the combined approach can be found in Ref. [2].

IDENTIFYING AND MANAGING DEFICIENCIES OF THE PHYSICAL PROTECTION SYSTEM

3.32. The effectiveness of a PPS can be influenced by many factors, including equipment malfunction or failure; deficiencies in policies, procedures or training; the security culture; and poor system design. Prescriptive, performance based or combined approaches can be used to detect potential deficiencies of the PPS.

3.33. Once these deficiencies are identified, corrective actions should be applied or compensatory measures should be implemented until corrective actions can be completed. The impact and potential consequences of deficiencies should be the basis for determining the need for compensatory measures until the appropriate corrective actions can be taken. A graded approach may be applied based on the severity of the deficiency and the urgency of implementing the corrective actions. The severity of identified PPS deficiencies ranges from minor impacts (e.g. procedures not being revised in the specified time frame) to significant impacts (e.g. physical protection measures not functioning).

3.34. After a deficiency has been identified and its impact has been determined, a corrective action plan should be implemented. The corrective action plan should include how the deficiency is to be resolved, the timeline needed to implement the identified solution, and any compensatory measures that should be put in place. The corrective action plan should be updated with the results of the reassessment once the corrective actions are complete.

3.35. The process for corrective actions should include the following steps:

(a) Identify the immediate causes associated with the deficiency.
(b) Identify the root causes associated with the deficiency.
(c) Develop corrective action plans for deficiencies by addressing the root causes to prevent the reoccurrence of these deficiencies in the future.
(d) Prioritize the deficiencies to be corrected, starting with the deficiencies that have the most severe impact rather than the deficiencies identified most recently.
(e) Establish a corrective action plan with appropriate milestones.
(f) Assign responsibility to specific organizations and individuals for completion of the corrective actions.
(g) Continually update the plan if new milestones are needed to resolve the deficiency.
(h) Ensure that adequate resources are assigned to correct the deficiencies in a timely manner.
(i) Maintain a system to track the implementation of the corrective actions.

Examples of root causes of PPS deficiencies are provided in Annex XV.

EVALUATING PHYSICAL PROTECTION SYSTEM DESIGN OPTIONS AND THEIR EFFICIENCY

3.36. An evaluation of design options for a PPS can be undertaken for multiple reasons, including a new facility design, changes to existing facilities, the correction of identified deficiencies, or changes to the design basis threat or the representative threat statement. Design options for the PPS should be evaluated prior to their implementation to ensure that the most cost effective and efficient physical protection measures are selected.

3.37. Evaluations of proposed PPS design options differ from evaluations of an existing PPS or PPS element in that actual performance testing is often not possible for design options, and thus simulations and/or analytical methods should be used. However, the scope of the evaluations should be the same. The evaluation of proposed designs should address both prescriptive and performance based requirements to identify the advantages and limitations of the designs and enable a comparison between alternative design solutions.

3.38. The design of a PPS should incorporate lifetime sustainability considerations, including implementation costs, as well as maintenance and testing activities. The

design should also incorporate efficiencies in maintenance and testing activities. For example, the placement of sensors, closed circuit television (CCTV) cameras and lighting should take into account ease of access for facility maintenance personnel during routine testing, component failure, preventive maintenance and/or calibration activities.

EVALUATION OF THE PHYSICAL PROTECTION SYSTEM AGAINST BLENDED ATTACKS

3.39. A blended attack is a malicious act involving the coordinated use of both cyber-attack and physical attack [19]. For example, the PPS or a physical protection subsystem could be compromised by a cyber-attack as a precursor to a physical attack or even after a physical attack. A precursor cyber-attack could occur immediately before, or much earlier than, the physical attack. It is also important to consider cases in which cyber-attacks occur after physical attacks.

3.40. A comprehensive evaluation of the effectiveness of a PPS should therefore include an analysis of blended attacks. An evaluation of the PPS computer network should be conducted separately to identify any potential deficiencies in computer security. Further evaluations should then be conducted for scenarios that include the computer network being compromised as part of an overt attack, a criminal or intentional unauthorized act by an insider, or other type of security event. Such evaluations could include simulations and performance testing, which could simulate, for example, compromised alarm communications or CCTV signals remaining undetected, in which case false data would be sent to the central alarm station. In such evaluations, the impact of blended attacks on the overall effectiveness of the PPS should be determined. If any deficiencies are identified, the operator should ensure that physical protection measures and procedures are implemented to provide defence in depth (see paras 3.32–3.35). More information on computer security is provided in Refs [5–7].

EVALUATION THROUGH MODELLING AND SIMULATION

3.41. The modelling and simulation methods used to evaluate the effectiveness of a PPS should be systematic, structured, comprehensive and appropriately transparent.

Path analysis

3.42. A path is a time ordered series of adversary tasks or actions, with descriptions of where those tasks or actions are performed within a nuclear facility. Path analysis produces simplified estimates of the probability of interruption for each credible path that an adversary could take to reach a defined target, assessing for each path how likely it is that an adversary would be detected early enough to be interrupted before an act of unauthorized removal of material or sabotage can be completed.

3.43. This method should be used to identify adversary paths that have the lowest probability of interruption, which would be the most vulnerable paths. The effectiveness of the PPS design in providing interruption is measured as the probability of interruption for the most vulnerable path. If the probability of interruption is too low for the most vulnerable path, then the PPS design should be considered inadequate and improvements should be implemented.

3.44. Path analysis is useful primarily because it provides insight into the performance of a PPS across many possible paths simultaneously; it also serves to efficiently determine which paths have the lowest associated performance against the design basis threat or the representative threat statement. Additional information on path analysis can be found in Ref. [13].

Neutralization analysis

3.45. Neutralization analysis is a method for determining the probability of neutralization. The probability of neutralization is the probability that response forces can stop an adversary before a criminal or intentional unauthorized act is accomplished or that response forces can cause an adversary to abandon an attempt at unauthorized removal of material or sabotage. Neutralization analyses should factor in legal and regulatory requirements, as well as the effectiveness of response forces.

3.46. Several methods can be used to assist in determining the probability of neutralization. These methods can range from modelling methods (e.g. qualitative, quantitative, tabletop) and simulation methods to limited scope and full scope performance tests. Each method has advantages and disadvantages in terms of the time and cost of the analysis and its accuracy. Multiple analytical methods should therefore be used to determine the probability of neutralization.

Scenario analysis

3.47. Scenario analysis is a method for evaluating the effectiveness of a PPS against specific attack scenarios. Using this method, adversary attack scenarios are postulated and the probability of PPS effectiveness can be determined directly, avoiding the need for two separate tools to calculate the probability of interruption and the probability of neutralization. The process involves identifying PPS elements that might be susceptible to defeat and developing scenarios to exploit these PPS elements. The scenarios could include defeat methods for sensors, barriers and communication systems and the possible diversion or elimination of portions of the response forces. Scenario analyses can also be used to evaluate more advanced adversary tactics, such as diversionary attacks and split team attacks, as well as the potential role of insiders in collusion with an external adversary.

3.48. Scenario analysis may use modelling and simulation tools and other evaluation methods, as reflected in Fig. 2. These analysis methods can be performed by subject matter experts, computer simulations, or a combination of both through a human–computer interface. Scenario analysis consists of the following four steps [13]:

(1) Identify scenario sets to be analysed.
(2) Develop detailed scenarios.
(3) Review and select final scenarios to be evaluated.
(4) Determine effectiveness against final scenarios.

Identify scenario sets to be analysed

3.49. As a first step, the set of scenario classes to be analysed should be determined. A scenario class can be defined in terms of unique combinations of scenario attributes, where each class conceptually includes all individual scenarios that have the corresponding scenario attributes [13].

3.50. The scenario classes to be analysed should be identified prior to the development of scenarios. While not all scenario classes can be covered in the scenario analysis, the competent authority or the operator might request that specific scenario classes be included.

3.51. In Fig. 2, the ‘start’ node represents the start of the analysis process. The ‘path identification tools’ node is followed if a software tool or evaluation method that employs a path analysis approach is used to generate paths (e.g. path 1,

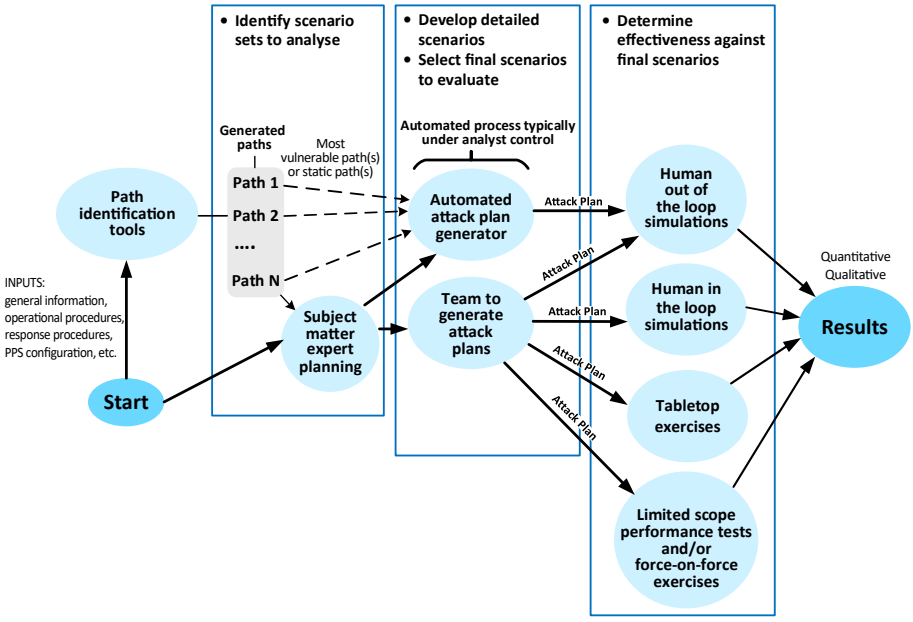


FIG. 2. How scenario analysis steps correspond to the process for using software tools and evaluation methods (adapted from Ref. [13], courtesy of M. Snell, Sandia National Laboratories).

path 2). These generated paths become inputs for a subject matter expert or a software program to generate an attack plan.

3.52. If path identification tool outputs are available, subject matter experts should review, and modify as needed, the paths generated by path identification tools. The approved or modified paths are then used as input to the scenario development step. Subject matter experts can also develop paths based on their knowledge of the PPS elements independent of path identification tool output if specific PPS elements need review.

Develop detailed scenarios

3.53. The attack scenarios developed should be those that present the maximum practicable challenges to the security and operations of the facility. These scenarios should still be within the scope of the design basis threat or the representative threat statement and the relevant scenario class. Within a scenario class, the scenarios under which the facility or activity is most vulnerable should be selected. As shown in Fig. 2, scenarios can be developed on the basis of the most vulnerable

path (which can be either generated by path analysis software or developed by a team of subject matter experts).

3.54. Attack plans developed by subject matter expert teams can be used in human in the loop simulations (e.g. humans control activities performed by computer generated adversaries and defenders within an environment modelled on a computer), tabletop exercises and force-on-force exercises, or they can be used as part of limited scope performance tests.

3.55. It is not necessary to develop detailed scenarios for every scenario class in the scenario set. The time and resources needed to evaluate all the scenario classes should also be taken into consideration.

Review and select final scenarios to be evaluated

3.56. The scenarios should be reviewed to decide which ones will be evaluated; this review and selection can take place either during the scenario development process or after its completion. Stakeholders (e.g. facility management, personnel of the competent authority) may be involved in this review and selection. Documentation of assumptions (e.g. assumptions beyond those found in design basis threat documentation about how the threat will employ a particular capability during a scenario, or restrictions to bound scenario analysis parameters), including which scenarios and assessment methods are to be analysed, may be approved by stakeholders.

3.57. Part of this review considers whether all objectives for the current assessment have been covered by the set of scenarios selected. Another consideration is whether all selected scenarios appear to be credible and within the capabilities specified in the design basis threat or the representative threat statement. If there are issues with either of these concerns, then it may be necessary for the assessment team to revise some of the existing scenarios or develop new ones [13].

Determine effectiveness against final scenarios

3.58. The four methods shown in Fig. 2 (i.e. human out of the loop simulations, human in the loop simulations, tabletop exercises, limited scope performance tests and/or force-on-force exercises) can be used either individually or in combination for the evaluation of scenarios. Many considerations, including the nature and size of the facility and the type of assessment and its objectives, should be taken into account when selecting the combination that will be used. For example, in some cases, a tabletop exercise could be sufficient to perform the evaluation.

3.59. A simple path analysis approach based on scenario timelines can be used to assess detection and delay. This approach assesses the detection and delay elements of the scenario to determine whether the response forces can interdict the adversary force. (A simple calculation may show that the response forces cannot arrive in time, making further detailed scenario simulation or exercises unnecessary.)

3.60. A simple vulnerability approach can also be used to assess detection and response. Instead of building out an entire adversary timeline, only potential vulnerabilities are analysed, which may lead to revealing circumstances that are vulnerable. This approach assesses the detection and response elements of scenarios where the adversary actions and resulting consequences occur without building a timeline [13].

3.61. The final step is to document the analysis results. In many instances, owing to the need to combine outputs from different modelling or simulation data inputs and approaches, the results are a combination of quantitative and qualitative analyses. Obtaining a meaningful number of test samples is difficult in many cases owing to budget limitations (e.g. only a limited number of explosives tests and/or force-on-force exercises are possible).

Insider adversary analysis

3.62. An insider is defined in Ref. [19] as:

> "An individual with authorized access to *associated facilities* or *associated activities* or to *sensitive information* or *sensitive information assets*, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities* or *associated activities* or other acts determined by the State to have an adverse impact on nuclear security."

Authorized access to facilities, materials and sensitive information provides the insider adversary with an enhanced opportunity to commit a criminal or intentional unauthorized act.

3.63. Given the complex nature of acts involving insider adversaries, the insider adversary analysis should include a combination of path analysis and scenario analysis. Annex XVII provides an example of an insider analysis method, which can also be applied — either alone or in combination with other evaluation tools — to scenarios involving collusion between an external adversary and an insider. For example, if it is possible that an insider could relocate nuclear material

outside its authorized location, a scenario involving an external adversary taking the relocated material from the new target location could be analysed. Additional information on insider analysis can be found in Annex XVII.

Nuclear material accounting and control analysis

3.64. An effective nuclear material accounting and control system ensures the security of nuclear material, in particular against an insider adversary who has the intent to commit theft of nuclear material. The facility operator manages the PPS and the nuclear material accounting and control system in such a manner that these two systems are mutually supportive [1].

3.65. The nuclear material accounting and control system relies on the PPS to limit access to the nuclear material and to protect it. The PPS relies on nuclear material accounting and control for information about nuclear material. Analysing the effectiveness of the facility PPS should include evaluating elements of the nuclear material accounting and control system, especially at the interface of the PPS and nuclear material accounting and control measures. Annex XVI provides examples for the use of nuclear material accounting and control elements — including records, physical inventories, nuclear material measurements, nuclear material controls and nuclear material movements — in an evaluation of the overall effectiveness of the protection of nuclear material and nuclear facilities.

EVALUATION THROUGH PERFORMANCE TESTING

3.66. Performance testing is conducted during or following the initial modelling and simulation process. It is used to evaluate the performance of personnel, procedures, equipment, technology and hardware and should be conducted as part of the evaluation process to validate the PPS against performance requirements. Performance testing should be used where a prescribed measure has to meet a technical criterion or specification. Performance testing methods and results should be well documented, particularly when used to justify assigned values for use in the evaluation of the effectiveness of a PPS. Test methodologies should be well structured to ensure the most efficient and accurate use of individual test trials and observations. Performance tests should be repeatable and impartial. To be considered valid, testing by different experts using the same test plan should yield comparable results.

Considerations for performance testing

Development of test plans

3.67. Developing effective test plans ensures the efficient use of resources and contributes to producing useful and accurate results (see paras 4.32–4.63 for a detailed description of a test plan and Annexes I–XIV for examples of performance test plans).

3.68. Test plans should be designed to ensure the following:

(a) Valid data are collected to characterize the PPS effectively.
(b) Achievable test objectives are established.
(c) Assumptions and results are documented.
(d) Proper approvals are obtained and testing activities are coordinated.
(e) Any identified deficiencies are managed.

Frequency of testing

3.69. The frequency of testing for specific PPS measures should be commensurate with the overall importance of the measures for ensuring effective detection, delay and response. Other factors that should be considered when determining the frequency of testing include the history of PPS element failure rates and the resources needed for large scale performance tests (e.g. force-on-force exercises). Additional guidance on the frequency of testing is given in para. 4.15.

Test criteria

3.70. Test criteria should specify the information to be gathered from the evaluation of the PPS and which performance metrics should be used. The test criteria should identify how the evaluation will be deemed successful or unsuccessful. An evaluation of response times, for example, could be measured against the time specified in the security plan, and the result could be a simple pass or fail, depending on whether the responders are in position within the specified amount of time.

Independent testing and reviews

3.71. Paragraph 3.32 of Ref. [2] states that "The competent authority may consider using an independent third party with appropriate expertise to conduct performance testing." For example, the operator could involve experts with

specialized skills in breaching techniques to perform delay tests of sample barriers or could use a team from the military or national police to act as an adversary in force-on-force performance tests. The military or police might be able to better simulate the knowledge and motivation of an external adversary than could guards and responders who are assigned to the facility. The use of the same national adversary team to conduct performance tests at different nuclear facilities could also help harmonize the test results between those facilities.

Documenting test results

3.72. Test results should be documented to ensure an effective evaluation and performance testing programme. Proper documentation also enables corrective actions to be determined. Performance testing data should be maintained in a data library, which can then be used to justify assumptions about the probabilities of detection and assessment and the delay and response times used in the evaluation of the PPS. If the information is considered sensitive, it should be protected in a manner consistent with the applicable regulatory requirements. Detailed guidance on documenting test results is provided in Section 4.

Integration of test data

3.73. The integration of test data is the process of collecting individual test results and characterizing a PPS element or multiple PPS elements that operate in coordination. For example, to determine the total time it would take for an adversary to breach a facility perimeter, several smaller individual tests of the different adversary tasks involved in the overall breach may be necessary. In this case, the total perimeter delay time would be determined by combining the individual test results for each postulated adversary task.

Selection of physical protection system elements to be tested

3.74. The competent authority should define testing as a regulatory requirement. The requirement should either prescribe a testing frequency for specific PPS elements or require a documented and approved testing schedule.

3.75. Analysis of the PPS should be used to identify and prioritize PPS elements that should be tested in accordance with the significance of the physical protection measure. Elements that are deemed crucial to the overall effectiveness of the PPS and elements with unknown, uncertain or unconfirmed performance should also be considered in the analysis.

3.76. Following initial modelling, the evaluation should produce a list of PPS elements for which more data might be needed to assess their effectiveness. Determining which PPS elements to analyse or test can be based on identification of the component as an important PPS element, on historic performance testing results or on the competent authority's guidelines. In addition, specific PPS elements might need to be tested more frequently, on the basis of lessons that may have been identified, results of previous analyses and testing, inspections, security incidents, or other information suggesting a potential weakness in the PPS.

3.77. The most important elements for the operation of the PPS should be considered when determining what is to be tested and when. In addition, consideration should be given to elements with high failure rates. Decisive factors for selecting elements to test include the skills needed by personnel (e.g. the ability to operate equipment, the ability to comply with procedures and physical protection requirements). If any changes (i.e. upgrades or modifications) are made to equipment and/or policies and procedures, those changes should be reviewed to confirm that they are effective as designed; it should also be confirmed that personnel are familiar with the modifications and adequately trained to conduct operations after the changes have been implemented.

3.78. Performance tests for guards and response forces range in complexity from simple demonstrations of a single individual skill to major integrated tests involving an entire response force operating with other PPS elements. A graded approach should be used when a performance testing programme is established, to ensure that the testing of PPS elements is commensurate with the national threat statement and the consequences of a criminal or intentional unauthorized act.

Facility operations

3.79. Facility operations, policies and procedures and environmental conditions should be considered when planning performance testing in the nuclear facility. During testing, the interface between safety and security should be effectively managed so that nuclear material remains appropriately protected and the safety of workers and the public is maintained.

3.80. Planning should take into consideration the type of nuclear material and its location and use; radiation levels; the potential impact of testing on operations; any difficulties in accessing testing locations during operations; proper coordination with, and necessary approvals by, all facility organizations; the frequency of testing; and the types of PPS elements or procedures to be tested.

Determining the testing schedule of a physical protection system element

3.81. The testing schedule of PPS elements should take into account the following:

(a) Regulatory requirements;
(b) International and national standards;
(c) For equipment, the applicable recommendations by the manufacturer;
(d) Facility specific conditions (e.g. day versus night shift, material movements) and activities necessary for the operation of the facility (e.g. maintenance, refuelling);
(e) Weather conditions;
(f) Maintenance programme;
(g) Past performance of equipment or procedures, including any failures;
(h) Outcomes of any corrective actions;
(i) Past performance of the personnel in performing security functions;
(j) Facility procedures;
(k) Any changes in the design basis threat or the representative threat statement.

3.82. A graded approach should be applied when developing the performance testing schedule for a facility. The testing frequency for individual elements may vary according to the PPS element. Schedules may consist of monthly, quarterly, semi-annual and/or annual testing. All PPS equipment should be tested at least annually to ensure effective operation.

Lessons from previous tests and operational experience

3.83. At the facility level, a continuous improvement methodology should be implemented for performance testing, incorporating lessons learned from previous tests and maintenance activities. Where possible, the facility should engage with other nuclear facilities to exchange information and to share best practices and lessons learned from testing, maintenance and operational experience.

3.84. Data from previous test results and operational experience could point to a need to retest physical protection measures on a more frequent basis. Such data are of particular importance for PPSs and physical protection measures that are associated with crucial detection points.

Security events

3.85. Data collected by the competent authority or by the facility relating to previous security events, violations and other malicious acts relevant to nuclear

security should be considered when determining the testing of PPS elements and physical protection measures.

On-site testing

3.86. On-site testing involves close coordination with facility management to minimize disruption of operations. Testing can be conducted at a limited scale or at full scale. It can be performed to demonstrate to the competent authority compliance with the regulatory requirements, or it can be performed at the behest of the management of the facility.

3.87. On-site testing provides the opportunity to evaluate the security design and procedures used to protect the current equipment and facilities. It should be ensured that physical protection measures are operating as intended during testing, with oversight and coordination by site security personnel. If a deficiency is identified through testing, or if a PPS element is defeated as part of a test (e.g. a fence is cut), corrective actions should be initiated as soon as testing is complete. If corrective actions cannot be initiated immediately, compensatory measures should be implemented that should remain in place until the corrective actions have been completed.

3.88. An effective communication plan is integral to testing and should be included in the test design. Pre-established communication procedures are necessary to ensure the efficiency of performance testing. Personnel involved in the test should be equipped with appropriate knowledge and resources to perform required tasks. The personnel involved in the test should have a clear understanding of the information they are expected to communicate, and of when and how they are expected to communicate this information.

3.89. Knowledge of communication procedures should not be limited to the personnel who are conducting the test; other facility and/or site personnel who might be affected by the conduct of the test should also be aware of the procedures. Off-site notifications may be necessary to ensure that test objectives are met and that the personnel conducting the test are protected.

Use of dedicated test beds

3.90. Performance testing on dedicated test beds located at the facility or at another location should be considered to test the effectiveness of PPS elements under a wide range of conditions and using a wide range of tactics. A dedicated test bed enables testing under realistic conditions without affecting facility

operations or security. The test bed could include equipment to test the interior and exterior systems related to physical protection and the infrastructure to support sensor testing, data gathering and data recording. In addition, access control systems, delay systems, prohibited item detection sensors, lighting, assessment or surveillance systems, power distribution systems, as well as alarm communications, display, monitoring and recording systems might be included in the test bed. Computer security concerns for any equipment that is shared between the facility and the test bed should be addressed. More information on dedicated test beds is given in Ref. [14].

Safety aspects

3.91. Personnel safety should be ensured during performance tests. The type and scope of the test can introduce a variety of non-routine safety risks, which can be mitigated through a comprehensive safety plan. The safety plan should describe all the resources involved in the test, including the equipment to be used, emergency medical procedures that may be necessary, and the arrangements and procedures for notification of the relevant authorities, as needed.

3.92. All test participants (e.g. the personnel conducting the test, the personnel being tested, anyone observing the test) should be adequately briefed on potential safety issues that might arise during the test — which could relate to the environment, radiation protection, health, the use of simulated weapons, rules of engagement, or boundaries and out-of-play areas — as well as the procedures to follow in such cases. For unannounced, limited scope performance tests, strict controls should be implemented to avoid any escalation of unplanned or unsafe actions outside the scope of the approved test plan.

3.93. The potential conflict between conducting a test in a safe manner and maintaining the necessary level of security should also be addressed when conducting the tests. Qualified facility safety management personnel and security management personnel should be involved in the planning process, with the objectives of the test being reviewed to ensure that both safety and security are maintained.

Other considerations

3.94. Information gathered from other States, including information on best practices, should also be considered. Training exercises pertaining to nuclear and other radioactive material, and the results of such exercises, should be taken into account when determining a path forward and enhancing evaluation

processes. Any information or intelligence on actual criminal or intentional unauthorized events, or potential planned events (including resources being used for those events), should be taken into consideration when determining evaluation objectives. Continual monitoring for pertinent information that could assist in enhancing the PPS and the evaluation of the PPS should be considered as well.

Performance metrics

3.95. The performance and the overall effectiveness of the PPS should be defined by metrics, where appropriate, such as probabilities of detection, delay times and response times. However, qualitative evaluation may be required to assess the performance of some elements, such as the efficiency of the tactical armed response. The requirements for the evaluation of these metrics should be defined by the State; for example, evaluations could be based on specific standards (particularly for the prescriptive approach) or on capabilities described in the design basis threat or the representative threat statement. To take into account every factor that could influence the overall effectiveness of the PPS, performance testing should include all potential defeat methods and tactics outlined in the design basis threat or the representative threat statement and should encompass different environmental conditions at different times of the day and the night. The personnel tested should not have prior knowledge of the particular scenario; if response forces are being evaluated, the responder team should be assembled from regularly scheduled responders.

3.96. Performance metrics can be determined statistically using the results of multiple tests. Statistical confidence is the likelihood that the derived performance metric is accurate. Some examples of performance metrics include delay time (i.e. time needed for an intruder to defeat a barrier), response time (i.e. time needed for the responders to arrive), the probability that the operator at a central alarm station will properly assess an alarm, and the probability that an alarm will be triggered when someone enters the area that the alarm is monitoring. Where such data exist, statistical techniques can be used, such as estimations of maximum likelihood, confidence intervals and hypothesis tests.

3.97. Statistical confidence is determined by the number of tests conducted (i.e. the more tests conducted, the higher the level of confidence in the results). When a numerical performance metric is specified (e.g. probability of detection), it should be accompanied by the desired confidence level. For example, if a test plan involves testing the detection sensor to ensure that it provides a minimum 85% probability of detection, at a 95% confidence level, then the pass/fail criteria would be that at least 85% of the tests confirm the sensor’s detection capacity and

that the total number of tests is large enough to provide a 95% confidence level that the probability of detection is at least 85%.

3.98. A testing strategy should include the selection of an acceptable and achievable confidence level. The higher the desired confidence level, the more testing and resources are needed to arrive at statistical probabilities of detection that approach the measured detection rates.

Probabilities of detection

3.99. The probability of detection should be used as a performance metric when evaluating the performance of PPS sensors. The probability of detection is an indication of the expected performance of a sensor. The probability of detection can be stated as a percentage and should be determined statistically through multiple tests. If a sensor is purported to have a probability of detection of 90%, this would indicate a 90% chance that the sensor will successfully detect an intrusion attempt. More details on probabilities of detection are provided in paras 4.16–4.19 and in Ref. [13].

Delay times

3.100. The delay time is a key performance metric for physical barriers. Delay can be accomplished by increasing the distances and areas that have to be crossed by the adversary and/or by introducing barriers such as fences, gates, portals, doors, locks, cages and activated delay systems, which would need to be defeated or bypassed by the adversary before reaching the target location. Physical barriers should be tested against specific delay time standards. An effective PPS should have sufficient delay times for responders to interrupt and neutralize an adversary attack before the adversary's goal can be achieved. Paragraph 6.30 of Ref. [1] states that "The objective should be the arrival of the *response forces* in time to prevent *unauthorized removal*."

3.101. The delay time in relation to individual components of the PPS can be defined as the time needed to defeat the individual component using a specific tool set. The delay time for a specific component should be tested by installing the component in a realistic setting and then calculating the time needed to defeat that component. Average delay times should be determined statistically through multiple tests. The tool set should be consistent with the capabilities of the adversary described in the design basis threat or the representative threat statement and should be established or validated by the competent authority, particularly for the prescriptive approach.

Response times

3.102. Another key performance metric is the amount of time it takes for the response force to respond to different events. Response forces may consist of persons on the site or off the site who are armed and appropriately equipped and trained to counter an attempted unauthorized removal of nuclear material or an act of sabotage. The response time should include the time needed to assess an alarm, to communicate the results of the alarm assessment to the response commander, to dispatch the responders and to travel to the appropriate response location. Response times should be determined statistically through multiple tests. These tests should include multiple attack scenarios and tactics in accordance with the design basis threat or the representative threat statement.

Ability to neutralize an adversary

3.103. The ability of the response forces to effectively neutralize an adversary attack can also be a key performance indicator. Factors to consider are timeliness, communications, command and control, and equipment and training, as well as compliance with laws, policies and procedures. The response forces should be capable of being in position in time to interrupt the adversary, have a sufficient number of personnel, be able to avoid attrition (e.g. ambushes, snipers, traps), have sufficient equipment to counter the threats outlined in the design basis threat or the representative threat statement, have the necessary training to use that equipment in an effective manner, and have appropriate policies and procedures in place to enable them to effectively neutralize the adversary.

Determination of defeat methods

3.104. Performance based evaluations should factor in the different methods that an adversary might use to try to defeat the PPS. A library of defeat methods, using different threat capabilities that include blended attacks, should be created to assist in the timely and realistic assessment of the PPS. This assessment should include a facility specific evaluation of how adversaries would attempt to defeat the PPS by attacking PPS computers and networks as a precursor to a physical attack. In addition, consideration should be given to the potential vulnerabilities of PPS elements, such as CCTV blind spots, sensor detection dead zones or communication dead zones. The methods available to defeat adversaries depend on the security measures that are in place. The determination of these methods of defeat should be a continual process that should be revised to reflect any changes of equipment. It should also take into account changes in the design basis threat or the representative threat statement.

Limited scope performance testing

3.105. A limited scope performance test is typically small in scale and is designed to test a part of the overall PPS. Specific pass/fail criteria should be defined, and the expected results should be identified, to ensure that the methods for data collection and analysis are useful and cost effective for the overall evaluation of the PPS.

3.106. Limited scope performance tests can be used to evaluate many PPS measures without disrupting facility operations and without using extensive resources and personnel. Limited scope performance tests can provide an indication of the performance of a specific physical protection capability; a series of limited scope performance tests for different actions can provide increased assurance of the overall capability of the PPS.

Testing individual physical protection system elements

3.107. Limited scope performance testing of an individual PPS element should be used to verify whether the specific element is functioning as designed and whether the relevant procedure is being followed correctly by personnel. Limited scope tests may involve an evaluation of the personnel's broad understanding of procedures or their ability to operate physical protection equipment.

Benefits and drawbacks of testing individual physical protection system elements

3.108. The benefits of testing individual PPS elements include the following:

(a) Easy to define pass/fail criteria;
(b) High reliability of test results;
(c) High repeatability of test results;
(d) Low impact on facility operations;
(e) Less planning and coordination needed than for more complex tests;
(f) Lower overall cost than for testing combinations of PPS elements.

3.109. The drawbacks of testing individual PPS elements include the following:

(a) The amount of data collected is limited.
(b) The interdependencies and interfaces of PPS elements are not tested.

Testing combinations of physical protection system elements

3.110. Limited scope testing of combinations of PPS elements should be used to determine if interdependent PPS elements are operating effectively. For example, this might include determining whether a sensor meets the detection sensitivity criteria as defined in the requirements, or whether the central alarm station operator accurately assesses the alarm triggered by the sensor and notifies the response forces.

Benefits and drawbacks of testing combinations of physical protection system elements

3.111. The benefits of testing combinations of PPS elements include the following:

(a) Ability to determine whether the interdependencies and interfaces of the selected PPS elements are effective;
(b) Collection of more test data than during testing of an individual element;
(c) Reliability of test results;
(d) Repeatability of test data;
(e) Lower impact on facility operations than during more complex tests;
(f) Less planning and coordination needed than for more complex tests;
(g) Lower overall cost than for full performance testing.

3.112. The drawbacks of testing combinations of PPS elements include the following:

(a) More complex planning is needed than for testing of individual elements.
(b) More complex testing criteria and an understanding of interdependencies and interfaces is necessary.

Full scope performance testing of a physical protection system

3.113. Full scope performance testing of a PPS focuses on the evaluation of the overall performance of all the elements of a PPS functioning as a whole. Testing the whole system should ensure that individual elements operate in a coordinated manner to provide effective detection, delay and response. The effectiveness of each PPS element along the adversary path that is being tested should be evaluated, and the effectiveness of the overall PPS performance should also be evaluated. Depending on the testing criteria and facility limitations, some PPS elements (e.g. detection, barrier delay) can be simulated during the test, while

other elements (e.g. adversary travel times, alarm assessment times, response times, interruption, neutralization) should be tested in practice. Force-on-force exercises can also be conducted as limited scope performance tests to evaluate a specific element or elements of the PPS, but they can also be conducted as full scope performance tests and include all the elements of the PPS.

3.114. The full scope performance test of a PPS is a large and complex test, involving a significant number of personnel and multiple organizations. The planning for such a test may also be more elaborate than the planning for a limited scope test. The following items should be considered during the planning for a full scope performance test of a PPS:

(a) Establishing clear test objectives. The objectives of the performance test should be clearly established, they should contain specific criteria for evaluation and they should be fully understood by all stakeholders. These objectives may include the following:
    (i) Validating the input data, assumptions, activities, results and conclusions of the vulnerability analysis;
    (ii) Demonstrating the physical protection capabilities;
    (iii) Ensuring that the performance of physical protection measures is effective.
(b) Coordinating with the personnel and the organizations involved in, or impacted by, the test. Planning the performance test in coordination with the stakeholders involved is crucial for ensuring that the test objectives are met, sufficient resources are allocated for the test and the tests are conducted safely.
(c) Selecting the attack scenario. Attack scenarios can be identified through various methods, such as modelling, simulations and tabletop exercises. When a range of scenarios has been developed, one scenario or several scenarios should be selected for testing. Considerations when selecting attack scenarios include identifying a 'worst case' scenario or bounding scenarios (i.e. scenarios that would represent difficult tests for the PPS and can thereby determine the effectiveness in less demanding scenarios); identifying a scenario suitable for testing a specific feature of a PPS element; and identifying a range of scenarios that can be tested over time. When selecting the attack scenarios, different types of cyber-attack on computer based systems that compromise the functions of those systems should be considered. The scenarios selected should enable the test objectives to be met.
(d) Using simulations. Various simulation techniques are available and can be useful tools for the development and implementation of performance tests. Simulations provide good insights into the effectiveness of the PPS, including

in relation to contingency plans; command, control and communication; and the training level of the response forces. Many types of computer simulation have been developed to perform analyses similar to force-on-force tests. These simulations range from those with relatively low fidelity that may have simulating factors such as engagement, weapons effects, personnel movement and two dimensional terrains, to those with relatively high fidelity that may have three dimensional terrains and algorithms that calculate the ability to see, hear, move and engage opposing forces using various weapons systems. Despite many limitations, simulations have the ability to gauge the performance of PPS elements that are not well modelled by path analysis or other mathematical models.

(e) Defining the adversaries and their capabilities. Adversaries and their capabilities, as described in the design basis threat or the representative threat statement, are used as input in effectiveness evaluation processes. Performance testing evaluates the effectiveness of the PPS against the threat described in the design basis threat or the representative threat statement to ensure the effective physical protection of nuclear facilities.

(f) Establishing compensatory measures. During a performance test, compensatory measures should be implemented to ensure the continued protection of nuclear material and of the nuclear facility. Performance testing of alarm and assessment activities may include opening perimeter barriers and the doors of buildings, which can reduce the effectiveness of the PPS if an actual attack occurs during the test. Additionally, testing that includes access to computer based components of the PPS could create computer security concerns. Compensatory measures that address the reduced effectiveness of the PPS during the test should be documented and should be approved in the plan for the performance test. Appropriate measures should also be taken to ensure full regulatory compliance (both for safety and security) during performance testing.

(g) Examining safety aspects and controls. Owing to the safety requirements necessary to operate a nuclear facility and to conduct non-routine response force actions during a full scope performance test (e.g. force-on-force), safety controls should be established during test activities. The primary functions of these controls are to ensure the safe conduct of the test and to control the activities of the scenario. Moreover, to ensure that the tests are conducted safely, one or more trained test controllers could be used (see also paras 4.53–4.56).

(h) Ensuring communication. A communication plan should be developed that establishes how and when facility and/or site personnel, as well as off-site personnel, will be informed that a performance test will occur. In the development of this plan, the performance test should be evaluated to

determine the potential safety risks associated with the scope of the test and the communication measures that will be necessary to reduce those risks. For example, if a full scope performance test (i.e. force-on-force) is to be conducted, then a communication plan should be implemented to reduce the potential for an unintended, real world response by the facility and/or site personnel or by off-site personnel.

3.115. The benefits of conducting full scope performance testing of a PPS include the following:

(a) Most interdependencies and interfaces of the PPS are tested.
(b) Personnel performance and the effectiveness of responses, tactics, procedures and specialized security equipment systems and vehicles are evaluated comprehensively.

3.116. The drawbacks of conducting full scope performance testing of a PPS include the following:

(a) The tests are resource intensive, in terms of both financial and human resources.
(b) The tests are time consuming to plan, conduct and evaluate.
(c) There is increased potential for the disruption of operations at the facility.
(d) There is increased potential for the injury or radiation exposure of personnel.
(e) Elaborate and challenging coordination efforts need to be undertaken with all the different stakeholders impacted by the testing.

4. PERFORMANCE BASED EVALUATION OF THE PHYSICAL PROTECTION SYSTEM

4.1. An evaluation programme should be established by the competent authority to verify and ensure consistent and effective oversight of nuclear security within the State. Additionally, a programme for the evaluation of the PPS should be established by the operator of the facility; the programme should provide an in depth, comprehensive examination of the PPS and should demonstrate the effectiveness of the PPS and its compliance with regulatory requirements. The competent authority should evaluate the operator's PPS evaluation programme to determine compliance with regulatory requirements; it may also conduct an independent evaluation of the PPS. The PPS evaluation programme can help identify whether

any upgrades or changes are needed to the PPS. A graded approach should be used by the operator when establishing the performance testing programme so that the testing of PPS measures is commensurate with the national threat statement and the consequences of a criminal or intentional unauthorized act. The competent authority also should develop regulatory requirements, using a graded approach, that are informed by the national threat statement and the consequences of a criminal or intentional unauthorized act.

DEVELOPMENT OF A PERFORMANCE BASED EVALUATION PROGRAMME

4.2. An effective performance based evaluation programme should be developed through detailed planning. Programme planning should address management systems, resource needs, funding, training and qualifications of personnel, data management, communication with internal and external stakeholders and processes for resolving issues. The management system details the methods, processes and tools that should be used by management at the nuclear facility to create a safe and secure framework for conducting all activities, including evaluations and performance testing. The programme should cover all stages in the lifetime of the facility.

Coordination and communication between organizations

4.3. Owing to the complexity of operations in a nuclear facility, the potential risks for the safety of personnel and the potential impacts on security of conducting performance testing, effective coordination that integrates all relevant stakeholders should be ensured when planning and conducting performance testing. For example, if response forces intend to conduct a test in an area where nuclear or other radioactive material is stored or used, coordination should take place with (a) safety personnel, to ensure compliance with safety rules and policies; (b) operating personnel, to ensure that the impact on normal operations is minimal; and (c) maintenance personnel, in case any equipment needs to be immediately repaired or restored after the conduct of the test.

4.4. Depending on the scope of performance testing, the number of entities involved may vary and should include the following:

(a) The competent authorities;
(b) Different departments of the facility, such as the departments responsible for security, operations, training, safety and response;

(c) Law enforcement, security and military agencies, and emergency and medical services.

4.5. Effective communication should be ensured during the planning and implementation of performance testing. This communication should include the personnel conducting the test and other facility and/or site personnel who might be affected by the test. Notifications to off-site personnel may be necessary to ensure that test objectives are met while safety controls are maintained. For example, in the case of a security incident, a number of organizations should be involved in effectively responding to and mitigating the incident. The planning and conduct phase of an evaluation should include representatives from each of these organizations to enable them to become familiar with one another's duties and responsibilities. Regulatory oversight of the performance based evaluation programme by the competent authority is an effective approach to avoid potential conflicts of interest between the organizations involved in the evaluation.

Programme planning

4.6. Programme planning should be undertaken for the effective conduct of an evaluation, and the level of planning should be determined by the type and complexity of the evaluation programme. A graded approach should be applied that takes into account the risk management approaches described in paras 2.13–2.15, the regulatory requirements, the number of protection elements to be tested, the frequency of testing, the available resources, the items to be protected, and the design basis threat or the representative threat statement. For example, a nuclear power plant with a limited access area, central alarm station, protected area and multiple vital areas, having hundreds of alarms, needs a rigorous testing programme, and large amounts of resources are needed to implement the programme. A testing programme for a Category III nuclear material storage area with a limited access area and fewer alarms normally needs much less testing and fewer resources to meet regulatory requirements.

4.7. A nuclear facility should implement performance testing programmes that make use of ongoing testing conducted by facility maintenance personnel, in addition to dedicated PPS testing, so as to ensure that the available data are used efficiently.

4.8. Considerations such as the following should be factored into the planning of the testing programme to ensure that tests are meaningful, realistic and cost effective:

(a) National laws and regulations;
(b) The design basis threat or the representative threat statement;
(c) Results from effectiveness evaluations that identify crucial systems;
(d) Specific PPS elements and subsystems to be tested;
(e) Objectives of the test;
(f) Evaluation criteria, including the specific pass/fail criteria to be applied;
(g) Personnel and equipment needed;
(h) Impact on the facility and/or site operations;
(i) Compensatory measures needed;
(j) Length of time needed to conduct the test;
(k) Lessons identified from previous tests;
(l) Costs of conducting the tests;
(m) Specific and general safety considerations;
(n) Current facility and/or site plans and procedures;
(o) Current level of training of personnel.

4.9. Inspections that are part of the competent authority's evaluation programme are often conducted on an annual or semi-annual basis. As a result, the planning process may be formal and rigorous to ensure that the inspections are conducted and completed within a strict time frame.

4.10. The planning process for performance testing should be included in the integrated management system of the facility. The advantage of such an approach is that planning and coordination processes are well defined and managed for all phases of performance testing.

4.11. The evaluation plan should clearly specify the test methodology, the test objectives, the roles and responsibilities of personnel involved in the tests, approval authorities, and processes for coordination with the facility personnel. The evaluation plan should also define the evaluation criteria, methodology and frequency; the approach for implementing corrective actions; and the integration with other organizations, as appropriate and necessary.

4.12. The evaluation plan should include the evaluation and testing of all the essential components and subsystems of the PPS. The system effectiveness evaluation process identifies crucial elements (components or subcomponents) of

a PPS that directly affect the system's effectiveness. Critical elements may consist of equipment, procedures and/or personnel.

Briefings and meetings

4.13. Depending on the components, scope and scale of the tests to be conducted, the planning process should include meetings and briefings to ensure that the purpose and objectives of the test are both pertinent and proportionate. These meetings and briefings should also ensure coordination with all of the relevant stakeholders.

4.14. Final approval should be obtained from stakeholders once the final test plan has been developed. Such stakeholders may include:

(a) Facility management;
(b) Facility security management;
(c) Facility safety representatives;
(d) The competent authority, if necessary.

Frequency of testing

4.15. As part of the planning process for performance testing, a testing schedule for the physical protection measures should be established. The following criteria should be considered when determining the testing frequency:

(a) The applicable recommendations from the equipment manufacturer, relevant standards, facility and/or site specific conditions and operational needs, and other factors that are intended to ensure system effectiveness;
(b) The results of the evaluation of the effectiveness of the PPS;
(c) The category of the nuclear material;
(d) The radiological consequences of sabotage;
(e) The strategy for physical protection of the facility;
(f) Any changes in the site operations and/or the facility;
(g) Any major modifications to the PPS;
(h) Any changes in the security mission at the facility and/or site;
(i) Any changes in the design basis threat or the representative threat statement;
(j) The results of previous tests;
(k) The reliability of physical protection equipment.

Statistical confidence

4.16. The evaluation plan should specify the required statistical confidence level to be achieved when determining performance metrics, which should include the selection of an acceptable and achievable confidence level.

4.17. When specifying a numerical performance metric as a test criterion, the confidence level should be provided; for example, a test plan for a sensor could specify that the criterion for the sensor is to demonstrate a 90% probability of detection at an 85% confidence level.

4.18. The confidence level is the probability range that contains the true value. The more trials that are conducted as part of the test, the higher the confidence in the results.

4.19. Table 2 indicates the number of trials needed for three different probabilities of detection and three different confidence levels. This table is based on a pass/fail criterion of zero failures (i.e. missed detections). If there is one missed detection, then the sensor fails the test. As shown in Table 2, to demonstrate a 90% probability of detection at an 85% confidence level, 18 trials have to be conducted without any failures. Increasing the level of confidence would involve an increase in the number of trials. For example, to demonstrate a 90% probability of detection with a 90% confidence level, the number of trials would need to increase to 22, without any failures. This method is considered practical if the actual probability of detection is expected to be close to 100%.

TABLE 2. NUMBER OF CONSECUTIVE SUCCESSFUL TRIALS WITH ZERO FAILURES FOR DIFFERENT CONFIDENCE LEVELS AND PROBABILITIES OF DETECTION

Confidence level	Probability of detection		
	0.95	0.90	0.85
0.95	59	29	19
0.90	45	22	14
0.85	37	18	12

Interpreting and applying test data

4.20. The methodology to be used to interpret and analyse or assess data against performance metrics should also be established (e.g. conducting statistical analyses, applying a basic pass/fail criterion).

Feedback and improvement

4.21. The evaluation programme should include a process for obtaining feedback from the performance testing activities. This feedback should be used to adjust and improve the evaluation programme on a periodic basis and should include the following:

(a) Effectiveness of the test plan in addressing the test goals and objectives;
(b) Suggested adjustments to the testing schedule;
(c) Suggested improvements to the test plan;
(d) Safety concerns during the test;
(e) Security concerns during the test;
(f) Level of training needed for the personnel conducting specific tests.

Performance testing

4.22. Performance tests are conducted once planning is complete. The test should not begin, however, until all pre-test activities noted in the test plan have been completed and have been verified to be complete. Pre-test activities should include all the necessary coordination activities and briefings (e.g. safety briefings for test participants).

4.23. The performance test should be conducted by qualified personnel who are sufficiently trained in conducting such tests and have sufficient knowledge of the test subject to understand the test results. The test should follow the test plan precisely to ensure the integrity of the results. If a deviation from the test plan is necessary, the changes should be documented and factored into the analysis of the test results.

Management of performance test data

4.24. Data management is necessary for the collection, organization, analysis and retrieval of data for validation activities relating to the effectiveness of a PPS, both historically and in the future. The stored data can also be used to justify the probability of detection, assessments, delay times and response times used

in modelling and simulation activities and in physical protection evaluations. Effective data management should be implemented to ensure the integrity of any evaluation programme that includes performance testing.

Data collection

4.25. The test plan should specify the data to be collected from the test. Personnel conducting the test should clearly record all relevant data, including the name of the data recorder and the date that the data were obtained. The circumstances explaining why data could not be obtained should also be recorded.

4.26. When testing response functions, the collective observations from each of the controllers and/or evaluators are often the most accurate information source for test results. The evaluation forms used by the controllers and/or evaluators to record their observations should be carefully developed. The topics outlined on the evaluation forms should reflect the goals and objectives of the test.

4.27. If, during the analysis of the performance test data, deficiencies in security equipment are identified that are outside the scope of the original test, a determination should be made of how significant the deficiency is to the security design and operation of the facility, and whether it is a maintenance or operator issue. An analysis should also be conducted to determine adequate compensatory measures.

Data integration with other testing

4.28. Multiple data sources or tests might need to be integrated to determine the effectiveness of individual physical protection measures or of the overall PPS. In such cases, the integration of test data with data from other sources should be undertaken to increase the confidence level of the results and to demonstrate that similar configurations of PPS elements provide comparable detection, assessment and delay values for similar facilities.

Maintenance of data

4.29. Test results should be maintained for the purpose of analysing and validating the PPS. Data from performance testing should be maintained in a data library.

Data confidentiality

4.30. Protecting the confidentiality of the data that are produced or recorded, both in digital and hard copy format, is an important element of the overall management of the evaluation data. The confidentiality of the results should be determined during the planning phase of the evaluation, with sensitive information appropriately managed from the beginning of the process [14]. More information on sensitive information can be found in IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [20].

Periodic testing of equipment and software

4.31. Testing of security equipment and software should be conducted periodically, in accordance with national regulations and the applicable recommendations of the equipment manufacturer. Periodic testing of equipment should include identification of potential computer security vulnerabilities. Further guidance on periodic equipment testing is provided in Refs [6, 14].

DEVELOPING TEST PLANS

4.32. A test plan provides a structured approach to the development and implementation of the performance test. Once a determination is made on the type of performance test to be conducted, the development of the test plan can commence.

4.33. The planning actions that should be conducted during the test plan preparation process include a review of the facility security plan, facility procedures and protective force coordination.

4.34. The test plan should include the following elements:

(a) Goals, objectives and scope of the test;
(b) Test location;
(c) Test scenario;
(d) Compensatory measures;
(e) Test methodology and evaluation criteria;
(f) Test procedures;
(g) Test controls;
(h) Human resource needs;
(i) Role of controllers;

(j) Role of evaluators;
(k) Test coordination;
(l) Operational impact;
(m) Test references.

Goals, objectives and scope of the test

4.35. Clear goals, objectives and performance standards should be developed as part of the test plan for performance testing. The goals should describe the expected results of the performance test and identify the specific protection elements to be tested. The goals should also state the reasons for the conduct of performance testing, including:

(a) To satisfy regulatory requirements;
(b) To identify PPS deficiencies;
(c) To test and evaluate PPS elements and subsystems and/or to evaluate the effectiveness of the overall PPS;
(d) To identify training needs and areas that need improvements or upgrades;
(e) To validate the implementation of changes or upgrades.

4.36. The objectives should include the specific tasks to be tested and observed in the performance test. These objectives should be based on performance standards against which the performance test will be evaluated.

4.37. Depending on the type of test to be conducted, the scope of the test can range from simple to complex. The scope should identify the following:

(a) The PPS elements that will be tested;
(b) The PPS elements that will be excluded from the test;
(c) The locations and times of the test;
(d) The duration of the test.

Test location

4.38. All test locations should be clearly identified in the test plan to ensure effective coordination between the organizations participating in the test and to obtain facility approvals prior to testing.

Test scenario

4.39. Scenario development is the process used to outline the details of the test. It should include consideration of measures designed to prevent and respond to criminal or intentional unauthorized acts, such as the sabotage of the facility. The scenario should be credible and should be based on the capabilities and timelines of both the adversaries and the response forces.

4.40. Depending on the type and scope of the performance test, the scenario can range from very simple to very complex. The scenario for the performance test should be discussed and agreed with relevant stakeholders to ensure that it meets the test objectives. Regardless of the test type, the scenario should be designed to take into account the PPS elements and subsystems, including the response forces.

4.41. For large scale tests, scenario development should consider the following:

(a) The design basis threat or the representative threat statement;
(b) The defeat methods for different PPS elements involved in the test or exercise;
(c) The adversary capabilities, in accordance with the design basis threat or the representative threat statement.

Compensatory measures

4.42. During the planning for the test, the safety equipment needed for the conduct of the test should be identified, as well as all safety related information that needs to be communicated to the personnel conducting the test.

4.43. If any degradation of safety and security readiness is expected while conducting performance tests, compensatory measures should be identified and implemented. Compensatory measures should also be implemented if a test identifies a major failure of an essential element for safety or security. The root cause of such a major failure should be identified, and measures should be taken to prevent a future reoccurrence.

Test methodology and evaluation criteria

4.44. The test methodology should describe how the test will be conducted and who will be involved. The methodology should include the following:

(a) A random selection of PPS elements to be tested, as appropriate;

(b) A list of the steps for conducting the test;
(c) The number of tests to be performed for each scenario, based on statistical confidence, as appropriate;
(d) The criteria for assessing the test results (e.g. pass/fail criteria);
(e) A checklist for each objective to be tested;
(f) The methods for data analysis.

4.45. Evaluation criteria should specify the information to be collected from the evaluation and the performance metrics to be used. These criteria should also identify how the evaluation will be deemed successful or unsuccessful.

Test procedures

4.46. During operability and functional testing, only the operation of PPS elements and subsystems is confirmed, with no attempt at defeat or determination of effectiveness (see Ref. [14] for additional guidance).

4.47. Effectiveness testing is used to determine if the protection measure is operating as designed, including meeting technical specifications and regulatory requirements. An example of this determination is whether a sensor provides proper coverage of a specific location (e.g. door, window, storage location, room volume).

4.48. Scenario testing is the process of defining scenarios by which adversaries could carry out theft or sabotage and then testing the PPS elements against these defined scenarios.

Test controls

4.49. Test controls should be imposed to maintain the integrity of the test and minimize safety risks and security risks. These controls may be applied to people, procedures and equipment. An example of a test control could be limiting the number of personnel who have knowledge of a scenario on a need-to-know basis. Other examples of controls may include providing minimum notice in advance of tests, controlling lighting levels, or testing equipment under specific environmental conditions.

4.50. Safety controls should be employed, for example when using vehicles or when live or simulated weapons are incorporated in the scenario. These controls can include procedures and personnel to control potentially unsafe actions during the conduct of the test. Plans should also be in place in case an actual security event occurs during the conduct of the test.

Human resource needs

4.51. For performance tests of response measures, in addition to the personnel being evaluated, other personnel who are involved in planning and conducting the tests and evaluating results are essential for the tests to be effective. The personnel involved could include the following:

(a) Security managers;
(b) Material control specialists;
(c) PPS equipment specialists;
(d) Response force managers;
(e) Off-site response managers;
(f) Safety managers;
(g) Radiation protection specialists;
(h) Facility managers;
(i) Crisis/emergency managers;
(j) Analysts responsible for conducting assessments of the effectiveness of the PPS;
(k) Computer security and software specialists.

4.52. Test participants should be subject matter experts in relevant areas and hold positions that qualify them for participation in the performance test.

Role of controllers

4.53. Controllers should be used when conducting performance tests on response measures, particularly if the performance test includes simulated engagements. The controllers should be responsible for ensuring that safety and security are maintained during performance tests, for introducing simulations, for monitoring the general progression of the scenario and for communicating scenario prompts (also known as 'injects').

4.54. All personnel should, at a minimum, attend an orientation briefing and should receive handout materials that cover the objectives and procedures of the test plan. Additional training should be provided to controllers for large scale tests. This training should emphasize the roles and responsibilities of the controllers and the evaluators, as well as the functional interactions between them. Controllers need to understand, and receive training on, how they are to interact with the personnel being tested.

4.55. The training should also demonstrate how to maintain safety and security during the test while fulfilling the objectives of the test and without interfering in the integrity of the exercise. Other elements of the training should include how to start the test, how to deliver test injects, what to do if the test deviates from the test plan and how to end the test.

4.56. In a large scale test, there should be a lead or senior controller, assistant controllers for the different elements being tested and a controller in charge of the exercise players acting as the adversaries. The lead or senior controller should report to an exercise director, who is responsible for the approval of the exercise scenario and maintains overall accountability throughout the exercise. All the controllers should be fully informed of the test plan and the timing of the sequence of steps so as to ensure that the test objectives are met.

Role of evaluators

4.57. When conducting performance tests for response measures, evaluators should be used to collect data. The evaluators should have knowledge of the appropriate actions to be followed by the test personnel, of the operation of the equipment that is to be used in the test, and of the security response plans. This knowledge is needed to understand how operations are conducted and to have an accurate performance standard against which to evaluate the performance test. When applicable, it might be acceptable for controllers to also perform evaluator duties.

4.58. At a minimum, all evaluators should receive an orientation briefing and handout materials on security plans, procedures and the responsibilities of the exercise players. Evaluators could also receive additional training on emergency centre operations, incident command and control, and response actions.

4.59. Evaluators should be familiar with the following [13]:

(a) Facility specific measures for security management and contingency response plans;
(b) Facility specific safety measures;
(c) The purpose and objectives of the test;
(d) The PPS elements being evaluated;
(e) Scenario events and timelines;
(f) Evaluator roles and responsibilities;
(g) Evaluation techniques;
(h) Procedures for monitoring and tracking player actions;

(i) Procedures for recording player actions and feedback;
(j) Procedures for reacting to player questions;
(k) Procedures for communicating test problems or deviations from the test plan;
(l) Specialized security equipment, including the use of various weapons systems;
(m) Regulatory requirements;
(n) The site or facility specific threat and risk assessment.

4.60. In most cases, all the evaluators can act as controllers (depending on the scope of the test), but not all the controllers can act as evaluators, since they may lack the specific knowledge or training needed to evaluate performance during the test.

Test coordination

4.61. Coordination with all the stakeholders involved in the planning, approval and conduct of the test is essential to ensure a successful, safe test with minimal operational impact on the stakeholders. The more complex the testing, the more coordination and planning is necessary.

Operational impact

4.62. Testing activities that take place at a nuclear facility can all have a potential impact on ongoing operations. The test plan should describe any operational impacts that might result from performance testing (e.g. operations, security, overtime) and identify measures to mitigate such impacts.

Test references

4.63. References should be listed in the test plan to determine a baseline for test requirements and criteria. These references should reflect the requirements relating to the security plan, the performance based requirements for the evaluation of the effectiveness of the PPS, and the regulatory requirements, as well as any potential weaknesses identified in previous test results.

Appendix

PLANNING AND MANAGEMENT OF AN EVALUATION OF THE EFFECTIVENESS OF A PHYSICAL PROTECTION SYSTEM

A.1. The process for evaluating the effectiveness of the PPS can be applied to the evaluations of physical protection measures designed to prevent the unauthorized removal of nuclear material and/or the sabotage of a nuclear facility. This process is intended for use with fixed site facilities that handle, store, manage and/or transport nuclear material and high activity radioactive sources. The process can also be adapted for low activity radioactive sources and associated facilities and activities.

DEFINING THE PURPOSE OF THE EFFECTIVENESS EVALUATION

A.2. The evaluation of a PPS is conducted by the operator in order to maintain the effectiveness of the PPS and to determine if the applicable physical protection requirements established by the State for the nuclear facility are met. The State defines the reference framework by which the evaluation should be conducted. The State may also conduct effectiveness evaluations to ensure that the PPS meets the regulatory requirements. When applicable, the PPS should be consistent with the capabilities described in the design basis threat or the representative threat statement.

A.3. Effectiveness evaluations should address the targets that have the highest potential radiological consequences or are the most vulnerable. The principal purpose of the effectiveness evaluation should also be clearly defined. For example, the intention might be to evaluate the PPS that an adversary might have to overcome or to simply evaluate the response to adversary actions. The purpose of the effectiveness evaluation should therefore determine what the evaluators will assess and which methods will be used.

ESTABLISHMENT OF REQUIREMENTS FOR AN EFFECTIVENESS EVALUATION

A.4. There is extensive documentation on the need for, and methods of achieving, the physical protection of nuclear material and activities that need to be protected from external threats. This documentation ranges from publications outlining obligations under international conventions to recommendations and guidance based on expert experience. The regulations, policies and guidelines

applicable to a particular facility determine the nuclear security objectives to be met and the type of effectiveness evaluation to be performed.

A.5. An effectiveness evaluation takes place within the national regulatory framework, and there is likely to be a significant amount of pre-existing information of direct relevance to the evaluation.

A.6. An effectiveness evaluation, whether initiated by the competent authority or by the operator, should have a clear purpose and should identify the targets to be assessed. The purpose and the identified targets determine the regulatory basis for the effectiveness evaluation and allow the evaluation team to focus on the following [17]:

(a) Appropriate nuclear security requirements and plans;
(b) Previous nuclear security inspection reports;
(c) Relevant safety and risk mitigation measures;
(d) Previous operator effectiveness evaluations and facility records.

A.7. This information also allows the evaluation team to focus on any particular issues that need investigation or reinvestigation and on the adversary scenarios that could be the most informative. This process could be iterative, with the purpose and target of the effectiveness evaluation changing depending on the information acquired and the methods and tools chosen.

A.8. The type of information to be considered, specific to the effectiveness evaluation being conducted, may also draw on policies and regulations from other States. Examples of the information to be considered include the following:

(a) Provisions to prevent proliferation;
(b) Nuclear security laws and regulations;
(c) The design basis threat or the representative threat statement;
(d) The responsibilities and legal authority of the respective competent authorities to fulfil their assigned roles;
(e) PPS requirements;
(f) Requirements for the nuclear material accounting and control system;
(g) Transport security requirements for nuclear or other radioactive material;
(h) Requirements for the protection of the confidentiality of sensitive information and of sensitive information assets;
(i) Requirements for trustworthiness of personnel;
(j) Responsibilities of operators.

MANAGEMENT OF AN EFFECTIVENESS EVALUATION

A.9. An effectiveness evaluation can be a major and costly project with potentially significant consequences for the operator and the competent authority, particularly if it includes a full scope performance test. The effectiveness evaluation should be approved and overseen by the appropriate level of management, which is responsible for implementing actions based on the outcomes of the effectiveness evaluation.

A.10. This subsection presents a project management approach for the conduct of large scale effectiveness evaluations, providing a hierarchy of oversight and control. Limited scale effectiveness evaluations can be given the same logical approach but might not need such formalized structures.

A.11. An effectiveness evaluation is performed by an evaluation team, consisting of one or more levels of security management and, for large scale evaluations, possibly including the facility security manager. This team might report to internal stakeholders (e.g. a board of directors, the facility manager) and might interact with external stakeholders (e.g. the competent authority). An effectiveness evaluation involving performance testing at the facility should be coordinated with the performance testing organization of the facility, which has the responsibility and authority to perform these tests. It is the responsibility of the project manager to ensure that the evaluation is performed safely and does not adversely affect safety in the facility.

A.12. It might not be possible for all evaluation team members involved in an effectiveness evaluation to have complete knowledge of all the relevant requirements. Therefore, a core team will typically perform the evaluation. This core team will have access to one or more subject matter experts, either in relevant nuclear security domains or in supporting areas such as intelligence or facility safety. In a performance based evaluation, the core team will interact with a performance testing team responsible for planning, conducting and documenting the appropriate limited scope performance test to collect information such as task times and probabilities of detection. If necessary, the evaluation may involve a force-on-force exercise, which is typically performed by a specialized organization [13].

A.13. Clarifying the roles of the different entities involved in an effectiveness evaluation is an essential element of the evaluation because individuals may be exercising different levels of authority than under normal circumstances. The size and composition of the core team should be commensurate with the facility

size, the complexity of the systems being assessed and the topics to be addressed. For example, nuclear material accounting and control specialists and computer security experts might be members of the core team or subject matter experts.

A.14. The effectiveness evaluation team may include the following [13]:

(a) Core team members:
    (i) Team leader (physical protection specialist);
    (ii) Site or facility liaison;
    (iii) PPS engineer;
    (iv) Assessment analyst;
    (v) Operations representative;
    (vi) Response expert;
    (vii) Access delay or explosives expert;
    (viii) Alarm communication and display engineer.
(b) Subject matter experts:
    (i) Locksmith;
    (ii) Nuclear material accounting and control specialist;
    (iii) Assessment software specialist;
    (iv) Threat specialist;
    (v) Safety representative;
    (vi) Site or regional nuclear security officer;
    (vii) Physical protection technician;
    (viii) Security force personnel;
    (ix) Fire protection specialist;
    (x) Construction or structural engineer;
    (xi) Information technology administrator.

Planning documents

A.15. To support the effectiveness evaluation, the following planning documents and presentations may be developed:

(a) An approved work agreement describing the goals of the effectiveness evaluation, an evaluation security plan, the scope of the systems to be assessed, the project management structure, the schedule, and the budget and resources needed;
(b) An initial briefing for members of the effectiveness evaluation team describing the information in the work agreement, as well as a briefing by the team leader on the assumptions regarding the scenario testing conditions for the PPS being evaluated (e.g. daytime or night-time operating conditions);

(c) A guide for the effectiveness evaluation team, which provides guidance and details the processes and procedures for the conduct of all the phases of the evaluation.

Effectiveness evaluation of the security plan

A.16. The existing security plan for the facility or activity should be evaluated to determine if it supports planned evaluation activities or if further elements are needed. An important element to consider is the plan to protect sensitive and confidential information in compliance with security regulations and standards. Information security measures should also be considered to prevent unauthorized personnel from gaining knowledge about performance tests and exercises, so as to reduce the probability that an adversary will use the performance test to conceal or enhance a criminal or intentional unauthorized act. Furthermore, when performance tests and exercises are being conducted at the facility, they are inherently an attempt to circumvent the facility's security system. However, the effectiveness of the security at the facility should be maintained throughout the conduct of the test or exercise, which usually means using supplementary measures. Special consideration should be given to maintaining an effective security response and to ensuring that effective security measures are maintained throughout the effectiveness evaluation.

Defining the effectiveness evaluation

A.17. An effectiveness evaluation may be evaluating the security of an entire facility. However, such an evaluation could be too disruptive operationally or could introduce vulnerabilities if conducted in certain parts of the facility. In the interests of efficiency, economy and safety, the specific boundaries and the scope of the effectiveness evaluation should be precisely defined.

A.18. The boundaries of the effectiveness evaluation do not necessarily need to correspond to a specific location but could be a discrete part of the security system (e.g. personnel screening, access control) or the entire system. For example, the effectiveness evaluation could examine how the system responds to a mistake made in granting security clearance, or it could include or exclude information security aspects of personnel screening. Similarly, if the effectiveness evaluation needs to evaluate effectiveness up to, but not including, a particular vital area, the boundary of the evaluation stops at the perimeter of that vital area. However, it may be necessary to decide whether to include parts of distributed systems, such as alarm or access control systems, that are located within that vital area [13].

Resources

A.19. An effective evaluation involves adequate funding, time and expertise. For the period during which the effectiveness evaluation is taking place, the normal activities of the facility could be disrupted. Managers may allocate resources and make provisions for any disruptions caused by the effectiveness evaluation.

Effectiveness evaluation team guides

A.20. The effectiveness evaluation team should develop a specific guide that covers details such as the following:

(a) The skills, knowledge and attributes needed for members of the effectiveness evaluation team and the factors that determine the selection of the team members;
(b) A description of the processes and time frames for obtaining sensitive site information and accessing the site;
(c) Essential information needed for the evaluation;
(d) Management structure of the effectiveness evaluation team.

Management structure of the effectiveness evaluation team

A.21. An effectiveness evaluation team leader should be assigned and should have the responsibility and authority to perform the evaluation. Given that most evaluations take place at a facility, it is the responsibility of the team leader to ensure that the evaluation activities are coordinated with the site management to ensure that safety is maintained at all times.

A.22. The planning of the effectiveness evaluation determines how unplanned external inputs are managed. For example, it might be difficult to determine whether the arrival of fire and rescue services was triggered from within the exercise, by someone outside the exercise who is unaware that an exercise is taking place, or by a real event outside of the exercise.

Effectiveness evaluation documentation

A.23. All the information arising from the effectiveness evaluation, as well as any uncertainties and assumptions taken into account during scenario development, should be thoroughly documented, since an effectiveness evaluation is a complex, iterative and detailed process involving many areas of a facility and many people and decisions.

Effectiveness evaluation training

A.24. The evaluation team involved in planning and performing an effectiveness evaluation should be trained on how to conduct the evaluation in accordance with documents pertinent to the specific evaluation and the facility. Training is also needed for others who are involved in the evaluation, such as the subject matter experts and stakeholders, so that they understand the purpose of the evaluation and their roles in it. All those involved should understand that a performance based evaluation depends on their cooperation and their openness to uncovering and discussing the strengths and potential vulnerabilities of the PPS being evaluated.

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), https://doi.org/10.61092/iaea.ko2c-dc4q

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[3] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980).

[4] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1 (Corrected), IAEA, Vienna (2021).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

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

[9] 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), https://doi.org/10.61092/iaea.3dbe-055p

[10] 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).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013), https://doi.org/10.61092/iaea.ajrj-ymul
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA-TECDOC-1868, IAEA, Vienna (2019).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility During Use, Storage and Movement, IAEA Nuclear Security Series No. 32-T, IAEA, Vienna (2019).
[17] 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).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook for Regulatory Inspectors of Nuclear Power Plants, IAEA-TECDOC-1867, IAEA, Vienna (2019).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, 2022 (Interim) Edition, IAEA, Vienna (2022), https://doi.org/10.61092/iaea.rrxi-t56z
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015). (A revision of this publication is in preparation.)

Annex I

SAMPLE FORMAT FOR A PERFORMANCE TEST PLAN

I–1. Performance test plans include all the elements of a test that are to be performed to evaluate the performance of a physical protection system (PPS). Relevant stakeholders can review the plan to have a clear understanding of what the test involves and of how and where it is to be conducted. The structure of the performance test plan indicates all the resources to be used and the criteria that determine how the test is to be analysed. A sample format for a performance test plan is given in Fig. I–1. Annexes II–XIV provide examples of plans for different elements of the PPS.

SAMPLE TEST PLAN

Test Plan [XX]
Protection Measure [X]
Date of latest revision:

Approval signatures		
Performance Testing Approval:	_____ Signature	_____ Date
Physical Security Approval:	_____ Signature	_____ Date
Security Systems Approval:	_____ Signature	_____ Date
Risk Management Approval:	_____ Signature	_____ Date

Performance test goal
(brief summary)

Test preparation	Safety equipment requirements
• Review previous performance test results • Review the facility security plan • Review any effectiveness evaluation documentation • Review immediate actions book in central alarm station • Create test plan for area being tested • Coordinate and schedule test • Notify guards and response forces of test prior to start	☐ Safety glasses ☐ Respirator ☐ Elbow pads ☐ Knee pads ☐ Gloves ☐ Helmet ☐ Crash pad (recommended, not required) ☐ Padded vest (recommended, not required)

Performance test personnel will continually monitor the area as well as their tactics for safety issues while conducting the test. All performed tasks required to complete the performance test will be accomplished using appropriate safety gear. If any safety hazards are identified by the system tester during the test, the test will be placed on hold until the safety issue is resolved.

NOTE

The completion of a performance test may require actions that exceed standard safety practices.
In these situations, all necessary safety precautions will be taken.

Classification Level 1

FIG. I–1(a). Sample format for a performance test plan — page 1.

I. Test goals

Expected results of the tests.

II. Test objectives

Specific tasks to be tested and observed.

III. Test scope

Identify the PPS elements being tested, what PPS elements are excluded from the test if any, the locations of the test, the times of the test and the duration of the test.

IV. Test location

All test locations should be clearly identified and approvals from facility owners documented or referenced.

V. Test scenario

Threat description and equipment, procedure, personnel being evaluated.

VI. Compensatory measures

In the event of a system failure, notification will be made to the appropriate authorities.

VII. Test methodology and evaluation criteria

Test results

- Test results recorded on worksheet.
- Determination of test results vs. criteria.

Sample criteria

- Performs effectively: The system and its individual components functioned properly and there is no credible or exploitable pathway.
- Needs improvement: One or more system components are not functioning and/or might not be compliant with the approved requirements. The system did not function properly but there were no credible or exploitable pathways.
- Significant weakness: The system has a credible and exploitable pathway to gain access or remove security interests without detection.

VIII. Test procedures

Define test procedures used (e.g. operability/functional testing, effectiveness testing, scenario testing).

IX. Test controls

Describe test and safety controls being employed.

X. Human resource needs

Define the personnel involved in the test and their responsibility as needed.

XI. Role of controllers

Responsible for ensuring safety and security are maintained during performance tests on response.

XII. Role of evaluators

Responsible for collecting data during performance tests on response.

XIII. Test coordination

Identify coordination activities with operations and support elements (e.g. operations, quality assurance, radiation control).

XIV. Operational impact

Describe any operational impacts that may result during testing (e.g. operations, security, overtime).

XV. Test references

A. Facility security plan
B. Special requirements for effectiveness evaluation
C. Regulatory requirements
D. Previous test reports

Classification Level 2

FIG. I–1(b). Sample format for a performance test plan — page 2.

Annex II

EXAMPLE OF A PERFORMANCE TEST PLAN FOR INTERIOR MOTION SENSORS

II–1. Performance tests for interior motion sensors (e.g. microwave sensors, passive infrared sensors) are conducted using any combination of walk tests, crawl tests and/or run tests. A performance test focuses on whether an adversary is detected prior to reaching a specified location; for defence in depth, the adversary is expected to be detected by more than one sensor. An example of a performance test plan for interior motion sensors is provided below.

PERFORMANCE TEST PLAN FOR INTERIOR MOTION SENSORS

Performance test goal

The performance test is designed to determine the effectiveness of interior motion sensor coverage in the nuclear material storage room of the facility.

Objectives

The performance test establishes the effectiveness of interior motion sensor coverage. The adversary tactics (i.e. modes of attack) used in the performance test include both walking and crawling.

Location

The nuclear material storage room of the facility is used for the performance test.

Physical protection measures to be tested

The physical protection measures to be tested are the interior motion sensors in the nuclear material storage room.

Compensatory measures

A guard is positioned outside the door of the testing location to perform visual alarm detection and assessment during the test. The guard maintains

communication with the central alarm station during the test and reports any criminal or intentional unauthorized acts to the central alarm station. The guard remains in place until the test is complete and the physical protection system has returned to normal operation.

Scenario description

The performance of interior motion sensors in the nuclear material storage room of the facility is tested against the design basis threat or the representative threat statement. The adversary tactics include both walking and crawling to avoid being detected by the sensors, with the ultimate goal of unauthorized removal of nuclear material. The test is performed during normal operating hours.

Test methodology and evaluation criteria

A total of six walk and crawl tests are performed. The tests will include the simulation of an adversary path from the door of the nuclear material storage room to the nuclear material storage rack, where the adversary attempts to touch the nuclear material rack without being detected. The exact path from the storage room door to the nuclear material storage rack is determined prior to testing.

Evaluation criteria

The motion sensors are considered to have passed the test if the system tester acting as the adversary is detected by at least two sensors prior to reaching the nuclear material rack, during both the walk and the crawl tests.

Procedure

The test consists of the following steps:

(1) The system tester is positioned inside the storage room within 0.3 m of the storage room door. The system tester limits movements for at least 20 s before walking.
(2) Any test observers remain outside the storage room door (or in the central alarm station) so that they do not affect the test results.
(3) Using one of the paths drawn in Fig. II–1, the system tester walks at a speed of approximately 0.3 m/s from the door towards the storage rack.
(4) If an alarm occurs:
    (i) The operator at the central alarm station announces the alarm and the sensor label via radio.

(ii) On the worksheet shown in Fig. II–2, the test observers note the sensor(s) that sounded the alarm.

(5) Using the same path, the system tester crawls at a speed of approximately 0.3 m/s from the door towards the storage rack.

(6) If an alarm occurs:

(i) The operator at the central alarm station announces the alarm and the sensor label via radio.

(ii) On the worksheet shown in Fig. II–2, the test observers note the sensor(s) that sounded the alarm.

(7) Steps 1–6 are repeated for each path indicated in Fig. II–1.

(8) The total number of alarms is recorded on the worksheet shown in Fig. II–2.

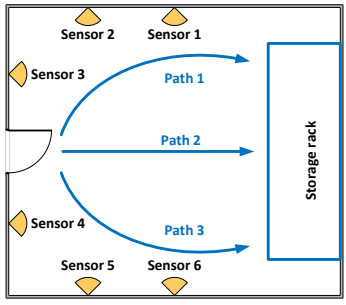


FIG. II–1. Example of the paths to be followed during an interior motion sensor performance test.

Test no.	Motion sensor alarm (yes/no)						Total no. of alarms
	1	2	3	4	5	6	
Path 1 walk							
Path 1 crawl							
Path 2 walk							
Path 2 crawl							
Path 3 walk							
Path 3 crawl							
Total alarms out of 6							

FIG. II–2. Example of a worksheet for an interior motion sensor performance test.

Annex III

EXAMPLE OF A PERFORMANCE TEST PLAN FOR EXTERIOR BISTATIC MICROWAVE SENSORS

III–1. Exterior bistatic microwave sensors are often installed in perimeter zones to detect someone attempting to walk, run or crawl across the perimeter. In this type of application, crawl tests are conducted to verify the detector alignment and sensitivity and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while minimizing the radar cross-section. Tests are often conducted with an object that simulates a person crawling, such as a metal sphere. An example of a performance test plan for exterior bistatic microwave sensors is provided below.

PERFORMANCE TEST PLAN FOR EXTERIOR BISTATIC MICROWAVE SENSORS

Performance test goal

The performance test is designed to determine the probability of detection by an exterior bistatic microwave sensor as part of the perimeter intrusion detection and assessment system.

Objectives

The performance test establishes the probability of detection by an exterior bistatic microwave sensor. The performance test uses a metal sphere to simulate a crawling intruder.

Location

The performance test is conducted in the perimeter intrusion detection and assessment system.

Protection elements to be tested

The physical protection system element to be tested is an exterior bistatic microwave sensor.

Compensatory measures

A guard is positioned close enough to the testing location to perform visual alarm detection and assessment during the test. The guard maintains communication with the central alarm station during the test and reports any criminal or intentional unauthorized act to the central alarm station. The guard remains in place until the test is complete and the physical protection system has returned to normal operation.

Scenario description

The performance of an exterior bistatic microwave sensor is tested against the design basis threat or the representative threat statement. The test is conducted in the perimeter intrusion detection and assessment system of the facility. The adversary tactic being tested is an attempt to avoid detection by crawling under microwave coverage, presenting a minimum cross-sectional area to the sensor. The test takes place during daylight hours.

Test methodology and evaluation criteria

The test includes the simulation of a crawling adversary, by moving a metal sphere across the detection zone.

Equipment

One hollow aluminium sphere, 30 cm in diameter, with a cord attached that is long enough to allow testers to pull the sphere across the detection zone, is used in the test.

Evaluation criteria

The sensor is considered to have passed the test if the probability of detection is determined to be 88% or higher at an 85% confidence level.

Procedure

The test consists of the following steps:

(1) The system tester records the starting position (e.g. at the crossover point near the transmitter) and the distance from the centre line of the sensor's detection volume.

(2) The aluminium sphere is set outside of the detection zone, approximately 4.5 m from the centre line of the sensor's detection volume.
(3) One tester is positioned on either side of the centre line of the sensor's detection volume, each holding a string attached to the aluminium sphere.
(4) The tester at the outer fence begins pulling the aluminium sphere at a rate of 0.3 m/s. The sphere is pulled across the detection volume of the microwave sensor from the outside of the detection zone to the inside of the detection zone.
(5) The system tester verifies whether an alarm occurs.
(6) The system tester documents the results.
(7) Steps 1–6 are repeated. At step 4, the sphere is pulled from the inside of the detection zone to the outside of the detection zone.
(8) Steps 1–7 are repeated for the remaining tests needed to determine probability of detection and confidence levels.
(9) When all the tests have been completed, the worksheet in Fig. III–1 is filled out to determine the probability of detection.

Total detected alarms for all the test locations	[No. of alarms] out of [No. of tests]
No. of failures	[No. of failures]
Probability of detection	[Probability of detection] at confidence level of [goal confidence level]
Record whether the element met, or failed to meet, the goal	
Goal probability of detection	88% at a confidence level of 85%
Did the test meet or fail to meet the performance level?	[Meet or fail]

FIG. III–1. Example of a worksheet for an exterior bistatic microwave sensor performance test to determine probability of detection. In this performance test plan, the goal probability of detection is 88% at a goal confidence level of 85%.

Annex IV

EXAMPLE OF A PERFORMANCE TEST PLAN FOR AN EXTERIOR CAMERA

IV–1. Exterior cameras are often installed in combination with perimeter sensors as a means of assessment. An example of a performance test plan for an exterior camera installed on a perimeter is provided below.

PERFORMANCE TEST PLAN FOR AN EXTERIOR CAMERA

Performance test goal

The performance test is designed to determine the capability of an exterior camera to cover an entire assessment zone on the video monitor in the central alarm station and to determine whether the video assessment system can effectively provide the three levels of assessment resolution (i.e. assessment, classification and identification).

Objectives

The performance test establishes the capability of an exterior camera to cover an entire assessment zone on the video monitor in the central alarm station. This performance test determines the effectiveness of the exterior camera for the near field of view and for the far field resolution of an assessment zone. The test is to be conducted during daylight hours.

Location

The performance test is conducted within the perimeter detection zone of the facility.

Protection elements to be tested

The physical protection system elements to be tested are the exterior camera of the protected area of the facility and the alarm communication and display system of the central alarm station.

Compensatory measures

A guard is positioned in view of the testing location to perform visual alarm detection and assessment during the testing. The guard maintains communication with the central alarm station during the test and reports any criminal or intentional unauthorized act to the central alarm station. The guard remains in place until the test is complete and the physical protection system has returned to normal operation.

Scenario description

The performance of the alarm assessment system in the protected area is tested to determine the ability of the system to display an entire assessment zone on the video monitor of the central alarm station and to determine whether the alarm assessment system can effectively provide the three levels of assessment resolution (i.e. assessment, classification and identification). The results of the test establish the ability of the system to effectively detect an adversary crossing through the entire assessment zone, either overtly or covertly, during the day. The test is to be conducted in the assessment zone of the protected area during normal operations.

Test methodology and evaluation criteria

The test determines if the exterior camera meets the requirement of covering the entire alarm assessment zone and whether the alarm assessment system has sufficient resolution to classify an object in the detection zone.

To conduct the test, two teams are needed: a field team that is positioned on the perimeter and a monitor observation team that is located in the central alarm station. The field team consists of a team leader to direct the test, one person responsible for communicating by radio to the central alarm station, one person responsible for taking notes, and three persons to act as testers and hold up the targets for identification (these roles may be combined, as needed). The monitor observation team consists of the central alarm station operator and an optional person responsible for taking notes.

Equipment

The following equipment is used to conduct the test:

(a) Handheld radios;
(b) Three geometric shapes (e.g. a triangle, a circle, a square) that are 30 cm in size and white on one side and black on the other;

(c) Four markers (e.g. orange cones) that are highly visible to the central alarm station operator.

Evaluation criteria

The camera is considered to have passed the test if it is able to cover the entire assessment zone including the near field of view, the far field of view and both the inner and outer fence lines, and it can obtain sufficient resolution to classify a 30 cm target in the far field (i.e. at the far end of the assessment zone).

Procedure

The test consists of the following steps:

(1) The field team places the markers at the four corners of the assessment zone.
(2) The monitor observation team verifies that the perimeter assessment system displays the entire assessment zone, including near and far fields of view and both the inner and outer fence lines (see Fig. IV–1). The monitor observation team records the results from the central alarm station.
(3) The testers take the triangle, circle and square shapes to the end of each sector (see Fig. IV–2). The purpose is to check the ability of each camera to identify a 30 cm target at the far end of the assessment zone. The field team verifies the identification of the shapes and the results recorded with the monitor observation team.
(4) With the black side of the three geometric shapes facing the camera, the testers hold the shapes in front of and above their heads or, at the perimeter, at ground level. The shapes can be oriented in any order and varied. For example, the triangle can be turned upside down or the square rotated 45 degrees to make a diamond. The shapes and the order are changed for each test. When in position, the designated field team member communicates the start of the test using the radio, and the monitor observation team records the order of the geometric shapes viewed on the monitor and the results. If the observed order was correct, the evaluation criteria have been met.
(5) If the evaluation criteria have not been met, the exterior camera is adjusted and retested.

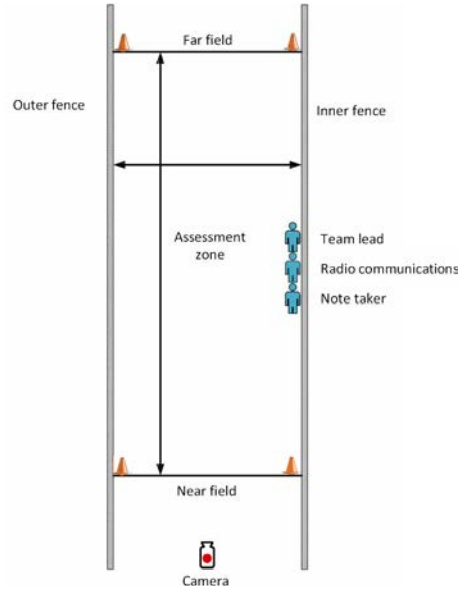


FIG. IV–1. Test configuration for an exterior camera.

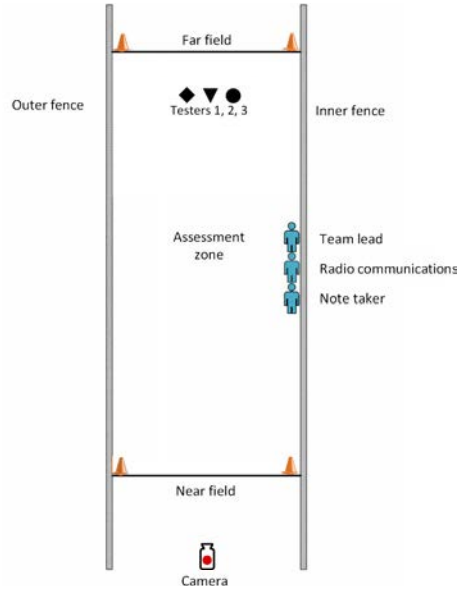


FIG. IV–2. Configuration to test the far field resolution of an exterior camera.

Annex V

EXAMPLE OF A PERFORMANCE TEST PLAN FOR A HAND GEOMETRY UNIT

V–1. Hand geometry units are a form of biometric access control system that verify the identity of an enrolled person by measuring the dimensions of their hand. An example of a performance test plan for a hand geometry unit is provided below.

PERFORMANCE TEST PLAN FOR A HAND GEOMETRY UNIT

Performance test goal

The performance test is designed to evaluate the effectiveness of a hand geometry unit of an access control system in detecting an unauthorized person attempting to pass through an entryway.

Objectives

The test establishes whether the hand geometry unit meets the minimum requirements for the probability of detecting attempted access by an unauthorized person. In the test, an unauthorized person attempts to gain access using the hand geometry unit.

Location

The performance test is conducted at the door of the facility's nuclear material storage room.

Protection elements to be tested

The physical protection system element to be tested is the hand geometry unit. The test assesses the following:

(a) Access control measures for individuals with authorized access, including through the use of a personal identification number (PIN);
(b) The biometric database of persons with authorized access;
(c) The ability of the hand geometry unit to control access.

Compensatory measures

A guard is positioned at the door being tested to perform manual access control for access into the room and to conduct visual alarm detection and assessment during the testing. The guard maintains communication with the central alarm station during the test and reports any criminal or intentional unauthorized act to the central alarm station. The guard remains in place until the test is complete and the hand geometry unit has returned to normal operation.

Scenario description

The performance of a hand geometry unit at the storage room door is tested to determine the probability of detecting unauthorized access. The adversary tactic is to obtain the PIN of an authorized person and attempt to gain access using the hand geometry unit. The test establishes the probability that the hand geometry unit will reject access for the unauthorized person. The test is performed during normal operating hours.

Test methodology and evaluation criteria

Evaluation criteria

The hand geometry unit is considered to have passed the test if the probability of detection is determined to be 88% or greater, at an 85% confidence level.

Procedure

The test consists of the following steps:

(1) One person with authorized access tests the hand geometry unit to ensure proper operation.
(2) Once it has been established that the hand geometry unit operates as designed, the person with authorized access inputs their PIN and a second person places their own hand on the hand geometry unit in an attempt to gain unauthorized access.
(3) Fifteen attempts per test are performed and recorded. Based on the predetermined statistical confidence, if any of the 15 attempts results in provision of unauthorized access, the system fails the test.

Annex VI

EXAMPLE OF A PERFORMANCE TEST PLAN FOR A SEARCH PROCEDURE USING A HANDHELD RADIATION DETECTOR

VI–1. Handheld radiation detectors can be used to search personnel, packages and vehicles for hidden nuclear or other radioactive material; however, their effectiveness is affected significantly by the search procedure followed and by the skills of the person conducting the search. An example of a test plan for a limited scope performance test of the search procedure using a handheld radiation detector is provided below.

PERFORMANCE TEST PLAN FOR A SEARCH PROCEDURE USING A HANDHELD RADIATION DETECTOR

Performance test goal

This limited scope performance test is designed to test the procedures used by a guard who operates a handheld radiation detector.

Objectives

The performance test evaluates the ability of a guard to effectively search for, and detect, a radioactive source at the exit of the facility.

Location

The performance test is conducted at the access control point at the exit of the facility.

Protection elements to be tested

The physical protection system element to be tested is the capability of the guard at the access control point to follow the approved search procedure and detect a radioactive source using a handheld radiation detector.

Compensatory measures

A second guard is positioned at the testing location to perform the routine access control search function during the test. The second guard maintains communication with the central alarm station during the test and reports any criminal or intentional unauthorized acts to the central alarm station. The second guard remains in place until the test is complete and routine access control searches are resumed.

Scenario description

The radiation portal detector at the access control point of the facility is assumed to be out of operation and an alternative search method is therefore being used. The guard at the access control point uses an approved procedure to search personnel exiting the facility with a handheld radiation detector to detect nuclear or other radioactive material that might have been removed from the facility. The purpose of the procedure is to detect an insider who might be attempting to steal nuclear or other radioactive material. The guard's ability to follow the approved procedure is tested using a test radioactive source that simulates nuclear material. The test is conducted during normal operating hours.

Test methodology and evaluation criteria

Equipment

A test source is used to test and calibrate the handheld radiation detector.

Evaluation criteria

The criteria for the evaluation are the following:

(a) Whether the guard correctly follows the approved procedure for conducting the search;
(b) Whether the guard is able to locate and identify the test source.

Test controls

The supervisor of the guard and the person responsible for evaluating the test (i.e. the evaluator) is present to observe the guard and ensure the safety of all participants. When the test source is recognized, the supervisor of the guard intervenes and prevents the guard from taking further action.

Procedure

The test consists of the following steps:

(1) A test radioactive source simulating nuclear material is hidden on the body of a trusted person before that person exits the building through the access control point.
(2) The supervisor of the guard and the evaluator position themselves to observe the search.
(3) The test is concluded when either the guard locates the test source or when the search is completed without locating the source.
(4) The evaluator then questions the guard on what actions should be taken if radioactive material were to be found on the person. The following questions are used to evaluate the search process:
    (i) Did the guard ensure the handheld detector was operating properly?
    (ii) Did the guard follow the approved procedure when scanning the person exiting the facility? For example, did the guard begin the search at the person's feet and scan up to the person's waist, arms, shoulders and head area? Did the guard instruct the person to turn around and did the guard repeat the scan process? Did the guard scan all hand carried items?
    (iii) Did the guard understand their responsibility to detain the person if radioactive material had been discovered and to notify the appropriate organization identified in the approved search procedure?

Annex VII

EXAMPLE OF A PERFORMANCE TEST PLAN FOR A METAL PORTAL DETECTOR

VII–1. Metal portal detectors are used to detect the introduction of prohibited metal items to a facility or the removal of nuclear material using shielding. An example of a performance test plan for a metal portal detector is provided below.

PERFORMANCE TEST PLAN FOR A METAL PORTAL DETECTOR

Performance test goal

The performance test is designed to determine whether the facility's metal portal detector meets the State's requirements for the prevention of the introduction of prohibited metal items or the removal of nuclear material using shielding.

Objectives

The performance test determines whether the probability of detection of prohibited metal items, such as weapons and radiation shielding, meets the State's recommended threshold.

Location

The performance test is conducted at the access control point of the facility.

Protection elements to be tested

The physical protection measure to be tested is the metal portal detector at the access control point of the facility.

Compensatory measures

While the testing of the metal portal detector is being performed by one guard, a second guard is positioned at the testing location to perform compensatory metal detection searches of personnel using a handheld metal detector. The second guard maintains communication with the central alarm

station during the test and reports any criminal or intentional unauthorized acts to the central alarm station. The second guard remains in place until the test is complete and the metal portal detector has returned to normal operation.

Scenario description

The adversary tactic is to attempt to carry prohibited metal items into or out of the facility. The metal portal detector is tested to determine if it can detect an attempt by a person to introduce prohibited items, such as a weapon, or to remove nuclear material using shielding.

The test standard approved by the facility (i.e. a simulated weapon and/or shielding item) is used for the test. The performance of the detector is tested against the design basis threat or the representative threat statement. The test is performed during normal operating hours.

Test methodology and evaluation criteria

Equipment

The following equipment is used for the conduct of the test:

(a) Metal test standard for weapons;
(b) Metal test standard for shielding.

Evaluation criteria

The detector is considered to have passed the test if the probability of detection is determined to be 88% or greater, at an 85% confidence level.

Procedure

The test consists of the following steps:

(1) The test standard is carried by a tester through the metal portal detector at either the head, waist or ankle level and at either a slow, moderate or fast speed, for a total of 15 passes.
(2) Each result is recorded in the worksheet shown in Fig. VII–1.
(3) The test results are reported for each test standard, as necessary.
(4) When all the tests have been completed, the worksheet in Fig. VII–2 is filled out to determine the probability of detection.

Test No.	Prohibited item	Test location (head, waist, ankle, other)	Test speed (fast, slow, moderate)	No. of trials	No. of detections	No. of failures
1	Metal object	Head	Slow			
2	Metal object	Waist	Slow			
3	Metal object	Ankle	Slow			
4	Metal object	Head	Moderate			
5	Metal object	Waist	Moderate			
6	Metal object	Ankle	Moderate			
7	Metal object	Head	Fast			
8	Metal object	Waist	Fast			
9	Metal object	Ankle	Fast			
10	Metal object	Head	Slow			
11	Metal object	Waist	Slow			
12	Metal object	Ankle	Moderate			
13	Metal object	Head	Moderate			
14	Metal object	Waist	Fast			
15	Metal object	Ankle	Fast			
Total						

FIG. VII–1. Example of a worksheet for a metal portal detector test.

Total detected alarms for all the test locations	[No. of alarms] out of [No. of tests]
No. of failures	[No. of failures]
Probability of detection	[Probability of detection] at confidence level of [goal confidence level]
Record whether the element met, or failed to meet, the goal	
Goal probability of detection	88% at a confidence level of 85%
Did the test meet or fail to meet the performance level?	[Meet or fail]

FIG. VII–2. Example of a worksheet for a metal portal detector performance test to determine probability of detection. In this performance test plan, the goal probability of detection is 88% at a goal confidence level of 85%.

Annex VIII

EXAMPLE OF A PERFORMANCE TEST PLAN FOR FENCE DELAY

VIII–1. Fences are commonly used as access delay barriers around security areas. Understanding how much delay time the fence provides against different penetration methods is important for security planning. An example of a performance test plan for determining fence delay times is provided below.

PERFORMANCE TEST PLAN FOR FENCE DELAY

Performance test goal

The performance test is designed to determine the effectiveness of the barrier delay values of the facility fence through the use of different barrier breaching techniques.

Objectives

The performance test determines and documents the delay time for each defeat technique using the adversary tools established in the design basis threat or the representative threat statement. It also determines whether the barrier delay times are consistent with the effectiveness evaluation values documented in the approved facility security plan.

Location

Given the destructive nature of this testing, a mock-up of the facility fence is used to test different defeat techniques.

Protection elements to be tested

The physical protection system elements to be tested are:

(a) The delay time for the welded wire fence;
(b) The ability to receive alerts from multiple alarms and to disseminate information to responders in a timely manner.

Compensatory measures

No compensatory measures are needed for this mock-up test.

Scenario description

Two adversaries use handheld wire cutters, mechanical saws and grinders to breach the mock-up fence of the nuclear material storage area, activating the fence alarm. The alarm is received by the central alarm station, it is assessed using a closed circuit television camera, and a response is dispatched in accordance with the facility security plan. The adversaries do not proceed past the cut fence, and upon termination of the test, they will remain in place.

Test methodology

Equipment

The following equipment is used for the conduct of the test:

(a) A mock-up of the fence, with at least three panels for testing;
(b) Handheld wire cutters;
(c) A battery powered saw with a metal-cutting blade;
(d) A battery powered grinder with a metal-cutting blade.

Procedure

The test consists of the following steps:

(1) A security supervisor starts a stopwatch to document the amount of time it takes for two adversaries to cut a hole through the welded wire fence using one of three different tools in three different sections of the fence.
(2) The adversaries use handheld wire cutters to cut a hole in one section of the fence. The hole has to be large enough for one person to pass through the fence.
(3) A second security supervisor in the central alarm station documents the amount of time it takes for the alarm to be received and for the response to be initiated.
(4) The times are evaluated to determine whether they would allow responders to get into position within the times stipulated in the security plan.
(5) Steps 1–4 are repeated using a battery powered saw with a metal-cutting blade to cut the same size breach in another section of the fence.
(6) Steps 1–4 are repeated using a battery powered hand grinder with a metal-cutting blade to cut the same size breach in a third section of the fence.

Annex IX

EXAMPLE OF A PERFORMANCE TEST PLAN FOR COMMUNICATIONS SYSTEMS

IX–1. Communication is an important element of response in a physical protection system. An example of a performance test plan for communications systems is provided below.

PERFORMANCE TEST PLAN FOR A COMMUNICATIONS SYSTEM

Performance test goal

The performance test is designed to evaluate the effectiveness of the central alarm station of the facility, the radio communications system and communications procedures.

Objectives

The performance test ensures the effectiveness of the following:

(a) The central alarm station in notifying the response forces, as approved in the facility security plan;
(b) The response communications system, as outlined in the approved facility security plan, procedures and training;
(c) The response radio communications equipment and usage, in accordance with the approved facility security plan, procedures and training;
(d) The radio equipment, in accordance with its design.

Location

The performance test is conducted in the central alarm station of the facility.

Protection elements to be tested

The physical protection system elements to be tested are the following:

(a) Communications. The ability to disseminate information to the response forces.

(b) Equipment. The ability of radios to transmit and receive messages as designed and the identification of potential dead spots.
(c) Procedures. The ability to issue effective notifications in a timely manner and to use the radio protocol.

Compensatory measures

Communications testing can occur as part of routine guard duties. The central alarm station and the guard who is testing communications measures use clear testing protocol announcements prior to and following the conduct of the test.

Scenario description

A fence sensor system is activated on the perimeter, and the central alarm system operator notifies the response forces by radio. While the response forces move to the sensor location for assessment, the radio communications between the response forces, the supervisor and the central alarm station are monitored.

Test methodology and evaluation criteria

Evaluation criteria

A pass/fail test criterion is used, with a test being considered to have failed if any response or communications procedure is not followed as outlined in the approved facility security plan or procedures. The response communications equipment involved is evaluated for effective performance and potential dead spots.

Test controls

No simulated adversaries are used during the test. A pre-test notification is announced. Weapons will remain in 'safety on' configuration throughout the test. The response management assigns performance test controllers and evaluators.

Procedure

The test consists of the following steps:

(1) The central alarm system operator is notified that the test has started and informed that a fence sensor has been activated at a specific location on the perimeter.

(2) The central alarm system operator announces the test on the radio and then proceeds to communicate with the response forces, as described in the approved facility security plan and procedures.
(3) Once these communications have taken place, the response forces move to the sensor location, assess the alarm and communicate by radio to the central alarm station any potentially unauthorized activities.
(4) Ten test iterations are conducted to allow multiple response personnel to participate in the test.

Annex X

EXAMPLE OF A PERFORMANCE TEST PLAN FOR POWER AND BACKUP SYSTEMS

X–1. The power system for a physical protection system (PPS) has to provide a reliable power source during both normal operations and emergency conditions. If normal power is lost, the transition to the backup power system has to be automatic, with minimal interruption in the operation of the PPS. An example of a performance test plan for backup power supply is provided below.

PERFORMANCE TEST PLAN FOR BACKUP POWER SUPPLY

Performance test goal

The performance test is designed to determine if the facility's uninterruptable power supply is maintained and functions as designed to support the PPS.

Objectives

The performance test determines if the facility's backup power supply and PPS batteries meet the State's recommendations for uninterruptable power supply for the protection of Category I and Category II nuclear material.

Location

The locations for the performance test are the backup power supply unit and the central alarm station of the facility.

Protection elements to be tested

The PPS elements to be tested are the facility's backup power supply and the PPS batteries. The loss of primary electrical power alarm functions at the central alarm station and the alarm communication and display system are also tested.

Compensatory measures

The operator, the central alarm station personnel and the guard force are notified well in advance that a backup power test will occur. Prior to the actual

conduct of the test, the operator, the central alarm station personnel and the guard force will provide authorization to the testing organization to indicate that it can begin testing.

Failure of backup power equipment during the conduct of this test could result in a temporary loss of power to the PPS. Compensatory measures may include stationing guards on the facility perimeter and in buildings prior to testing. The guards maintain communication with the central alarm station during the test and report any criminal or intentional unauthorized acts to the central alarm station. The guards remain in place until the test is complete and the PPS power supply has returned to normal operation.

Scenario description

The adversary tactic is to attempt to defeat the primary power supply to the facility's PPS to increase the probability of achieving a criminal or intentional unauthorized act, such as the unauthorized removal of nuclear material or sabotage.

Test methodology and evaluation criteria

Evaluation criteria

The test result is a 'pass' if all the following items are successfully completed:

(a) Following the loss of power, the backup power supply automatically begins operation.
(b) A total of 98% of all PPS alarm functions remain in operation during the power changeover (i.e. local battery supplies are operational and PPS functions operate as required).
(c) The alarm communication and display system of the central alarm station indicates a loss of primary power, in accordance with State requirements.
(d) The alarm, communication and display functions remain operational, as required by the State.

Procedure

The test consists of the following steps:

(1) Performance test personnel are located in the central alarm station and at the backup power unit to evaluate the loss of power functions of the alarm communication and display system.

(2) The maintenance personnel for the PPS at the facility simulate a loss of primary power supply to the PPS at the backup power supply unit.
(3) The performance test personnel observe the operation of the system.

The State might not have a requirement for all the PPS measures to operate continuously during the changeover to the backup power supply. For example, modern closed circuit television camera contrast during low light conditions might be sufficient to provide assessment during the lighting restart period at the perimeter of the protected area.

Annex XI

EXAMPLE OF A PERFORMANCE TEST PLAN FOR TAMPER AND LINE SUPERVISION

XI–1. Tamper sensors installed in hardware, and line supervision incorporated into communication lines, are designed to detect attempts to access and compromise the physical protection system (PPS). An example of a performance test plan for tamper and line supervision is provided below.

PERFORMANCE TEST PLAN FOR TAMPER AND LINE SUPERVISION

Performance test goal

The performance test is designed to determine whether the facility's PPS alarm lines are protected against tampering and defeat by an adversary.

Objectives

The performance test examines the PPS alarm junction boxes for tamper switch operation and alarm signal and determines if the PPS alarm line supervision is sufficient to meet State requirements.

Location

The locations for the performance test are the facility's PPS alarm junction boxes and the central alarm station.

Protection elements to be tested

The PPS elements to be tested are the facility's PPS alarm junction boxes and the power supplies and alarm functions of the alarm communication and display system of the central alarm station.

Compensatory measures

A guard is positioned close enough to the testing location to perform visual alarm detection and assessment during the test. The guard maintains communication with the central alarm station during the test and reports any

criminal or intentional unauthorized act to the central alarm station. A second knowledgeable maintenance person participates in the test to maintain the two-person rule and report any criminal or intentional unauthorized acts. The guard remains in place until the test is complete and the PPS has returned to normal operation.

Scenario description

The adversary tactic is to attempt to defeat the facility's PPS alarms by accessing the alarm and closed circuit television (CCTV) junction boxes to interrupt alarm and CCTV communications and substitute signals in an effort to increase the probability of achieving a criminal or intentional unauthorized act, including the unauthorized removal of nuclear material or sabotage.

Test methodology and evaluation criteria

Evaluation criteria

The test result is a 'pass' if the alarm communication and display system of the central alarm station indicates a tamper alarm, a loss-of-signal alarm and a line supervision alarm, in accordance with State requirements.

Procedure

The test consists of the following steps:

(1) The performance test personnel randomly select a predefined number of alarms and junction boxes to test.
(2) In the central alarm station, the performance test personnel evaluate the alarm communication and display system for the identification of loss of signal and/or alarm, tampering, and alarm signal.
(3) The PPS maintenance personnel of the facility access selected PPS junction boxes to determine if a tamper switch alarm is operational and whether an alarm is received in the alarm communication and display system of the central alarm station.
(4) The PPS maintenance personnel also interrupt the alarm and/or CCTV signals to determine if a line supervision alarm or a loss-of-signal alarm is received in the central alarm station.

Annex XII

EXAMPLE OF A PERFORMANCE TEST PLAN FOR EVALUATING THE EFFECTIVENESS OF THE PHYSICAL PROTECTION SYSTEM DURING AN EMERGENCY EVACUATION PROCEDURE

XII–1. Emergency evacuations present significant challenges to a physical protection system (PPS). To quickly evacuate personnel from a building, normal PPS measures have to be bypassed, presenting opportunities for insiders to exploit an evacuation so as to remove material from the facility. An example of a performance test plan for evaluating the effectiveness of the PPS during an emergency evacuation is provided below.

PERFORMANCE TEST PLAN FOR EMERGENCY EVACUATION PROCEDURE

Performance test goal

The performance test is designed to evaluate the effectiveness of the PPS of a nuclear facility when responding to the unauthorized removal of nuclear material during an emergency evacuation. The test evaluates the interface of measures for physical protection and nuclear material accounting and control, as well as the nuclear security culture.

Objectives

The performance test evaluates the response to an emergency evacuation of the facility to ensure that, following a planned or unplanned evacuation, the control of personnel can be maintained until the evacuated personnel have been searched, to ensure that a criminal or intentional unauthorized act has not occurred. The test is performed during normal working daytime hours.

Location

The locations for the performance test are the designated personnel monitoring location and the access control point of the protected area of the facility.

Protection elements to be tested

The compliance of the guard force with evacuation procedures is evaluated in this test, particularly:

(a) The control of evacuated personnel during an emergency evacuation, including channelling them to the evacuation monitoring location and preventing them from leaving the protected area of the facility;
(b) The search of evacuated personnel using a portable radiation detector at the monitoring location, in accordance with the procedure to sweep the area after an evacuation, and the detection of any concealed nuclear material.

Compensatory measures

The operator, the central alarm station personnel and the guard force are notified well in advance that an emergency evacuation test will occur. Prior to the actual conduct of the test, the operator, the central alarm station personnel and the guard force provide authorization to the testing organization, indicating that the test can proceed. Compensatory measures may include stationing guards on the facility's perimeter access control points and building emergency exit locations prior to testing. The guards maintain communication with the central alarm station during the test and report any criminal or intentional unauthorized acts (i.e. any actions not included in the test plan) to the central alarm station. The guards remain in place until the test is complete and the PPS has returned to normal operation.

Scenario description

The adversary tactic is to exploit an insider to achieve unauthorized removal of nuclear material from the facility during an emergency evacuation, with the insider concealing the material outside the facility for later retrieval. This limited scope performance test focuses on the following elements:

(a) The ability of an insider to exit the access control point of the protected area without proceeding directly to the evacuation gathering point.
(b) The ability of an insider to conceal nuclear material on their person without being monitored for nuclear material at the gathering point. (This test does not address the guard's effectiveness in detecting the nuclear material, only that monitoring is indeed performed.)
(c) The ability of an insider to conceal nuclear material along the evacuation route for later retrieval.

Test methodology and evaluation criteria

Evaluation criteria

The test result is a 'pass' if all the following are successfully completed:

(a) The guards or facility personnel prevent the trusted agent from exiting the protected area of the facility and redirect the agent to the emergency evacuation monitoring location.
(b) All personnel at the monitoring location have been monitored for unauthorized removal of nuclear material.
(c) Areas outside the building have been systematically and effectively searched, and the concealed simulated nuclear material has been detected.

Optional evaluation criteria

The following criteria can also be used for the evaluation of the test:

(a) Access control records are used to verify that all personnel who were in a facility are accounted for at the monitoring location prior to the conclusion of the emergency evacuation test.
(b) It has been determined that the access control point for the protected area is restricted for entry and/or exit until the conclusion of the evacuation test.

Pre-test activities

The following activities are conducted before the test:

(a) Simulated nuclear material is placed outside the facility, between the emergency exit and the monitoring location.
(b) All nuclear material in the facility is securely stored.
(c) As a compensatory measure, a guard and a radiation protection specialist are located outside the emergency exit to monitor personnel exiting the facility for unauthorized removal of nuclear material during the test.
(d) A trusted agent is located in the facility.

Procedure

The test consists of the following steps:

(1) At the start of the test, a controller announces the beginning of a fire evacuation test and instructs the personnel to follow the procedures for a fire alarm.
    (i) Personnel exiting the emergency evacuation door are directed to stop. They are then monitored by the guard and the radiation protection specialist prior to traversing to the emergency evacuation gathering point.
    (ii) Personnel exiting through the access control point of the facility comply with the approved search and monitoring procedures prior to traversing to the emergency evacuation gathering point.

(2) A trusted agent attempts to exit the protected area of the facility through the access control point.
    (i) If challenged by the guard or facility personnel, the trusted agent does as instructed and proceeds to the emergency evacuation gathering point.
    (ii) If not challenged, the trusted agent proceeds to the access control point but does not leave the building in which the gathering point is located.

(3) The controller ends the test when all the personnel at the gathering point have been monitored and the path along the evacuation route has been searched for concealed simulated nuclear material.

Annex XIII

EXAMPLE OF A PERFORMANCE TEST PLAN FOR NUCLEAR MATERIAL ACCOUNTING AND CONTROL

XIII–1. An accurate nuclear material accounting database combined with effective controls and periodic inventories provides detection of unauthorized removal of nuclear material. An example of a performance test plan for evaluating the effectiveness of nuclear material accounting and control is provided below.

PERFORMANCE TEST PLAN FOR NUCLEAR MATERIAL ACCOUNTING AND CONTROL

Performance test goal

The performance test is designed to assess the accuracy of the nuclear material accounting database.

Objectives

The performance test evaluates the accuracy of the nuclear material accounting database by verifying the location of the nuclear material, the identification numbers of tamper-indicating devices and the gross weights of the material containers.

Location

The test takes place within the confines of the storage room or processing area of the facility.

Protection elements to be tested

The nuclear material accounting and control element to be tested is the nuclear material accounting records, specifically their agreement with the locations of nuclear material, the tamper-indicating device identification numbers, and the gross weights of the material containers.

Compensatory measures

Compensatory measures are not needed for this test, since routine approved nuclear material accounting and control procedures and measures are followed during testing.

Scenario description

The performance test verifies the accuracy of the nuclear material accounting and control records and confirms the likelihood of detecting unauthorized removal of nuclear material (i.e. for abrupt or protracted theft strategies) between physical inventories.

Test methodology and evaluation criteria

Evaluation criteria

The test result is a 'pass' if no discrepancies are identified between the data in the database and the actual conditions.

Procedure

The test consists of the following steps:

(1) The controller obtains the book inventory report to have access to the nuclear material accounting and control records for the storage room, which include the recorded location, the tamper-indicating identification device number (if applicable), and the container and content gross weight for each item in storage.
(2) The controller randomly selects a specific number of items from the inventory for verification. The locations, tamper-indicating device identification numbers and gross weights of these items are then noted for verification.
(3) The performance testing personnel (i.e. the tester and the verifier), with the assistance of facility personnel, enter the storage room or process area of the facility to verify that all selected items are present in their recorded locations and that the tamper-indicating device identification numbers and the gross weights correspond to each item's recorded data. If a selected item is in use and unavailable for the inventory as a result of an authorized activity, then another item is selected from the inventory list.
(4) The performance testing personnel note all the discrepancies and/or defects, to be investigated at the conclusion of the test.

(5) While in the area, the controller may randomly select a specific number of additional items that are physically present in the material balance area and record each item's location, tamper-indicating device identification number and gross weight for comparison with the book inventory.
(6) The performance testing personnel then verify the data for the items selected and compare the values against the book inventory report for nuclear material accounting and control. All discrepancies and defects are noted and investigated at the conclusion of the test.

An example of an advanced performance test for nuclear material accounting and control repeats steps 1–6 with a trusted agent, who could move a preselected item to another location in the storage room prior to the conduct of the performance test. Such an approach would need additional management, coordination and approvals.

Annex XIV

EXAMPLE OF A PERFORMANCE TEST PLAN FOR RESPONSE TIME

XIV–1. Response is a key element of the physical protection system (PPS), and response time is therefore an important performance metric for evaluating the effectiveness of the PPS. An example of a performance test plan for response time is provided below.

PERFORMANCE TEST PLAN FOR RESPONSE TIME

Performance test goal

The performance test is designed to test and evaluate the time it takes the facility response force to reach the nuclear material storage room in response to an alarm.

Objectives

The performance test assesses:

(a) The ability of the central alarm station to effectively direct the response force in accordance with facility procedures;
(b) The time taken to respond, in accordance with the security response plan, and whether the responders possess the approved weapons and equipment, in accordance with the facility security plan and relevant procedures.

Location

The performance test is conducted at the nuclear material storage room of the facility.

Protection elements to be tested

The specific elements to be tested are the following:

(a) Whether the central alarm station personnel are able to direct the response force to the alarm location;
(b) Whether the responders are properly armed and equipped to respond;

(c) Whether the responders can get into position within the time stipulated in the facility response plan.

Compensatory measures

Prior to the actual conduct of the test, the operator and the central alarm station personnel provide authorization that the testing can proceed, to ensure that facility operations and PPS measures are not adversely affected.

Facility response testing can occur as part of routine guard duties, and the test follows approved response plans and procedures. The operator, central alarm station personnel and guards who are testing communications ensure that the test is being conducted, with clear testing protocol announcements prior to and following the conduct of the test.

Scenario description

The scenario to be tested is a response to alarms at the nuclear material storage room. Following notification of the alarms, a response is initiated in accordance with the approved contingency plan.

Test methodology and evaluation criteria

Evaluation criteria

A 'pass' score is given to each responder if the responder in question responds with all the issued equipment and is able to get into an effective and appropriate response position in a timely manner, in accordance with the security plan.

Test controls

The central alarm station operator is instructed to include a statement that it is a test in every announcement and notification during the test.

Pre-test activities

Evaluators are located at the designated response locations. The evaluators are equipped with stopwatches and checklists listing the weapons and equipment that the responders are expected to bring.

Procedure

The test consists of the following steps:

(1) To begin the test, the central alarm station operator is notified that the test has been initiated. The central alarm station is instructed to complete the following actions:
    (i) Announce that alarms have been triggered at the facility's nuclear material storage rooms, and include a statement that it is a test.
    (ii) Advise the appropriate personnel, as prescribed in the facility security plan.
(2) Response personnel then respond to the alarm in accordance with the approved contingency plan.
(3) Ten tests are conducted to allow multiple response personnel to participate.
(4) A pass/fail criterion is used, along with a checklist. A 'pass' score is given to each responder if the responder in question responds with all the issued equipment and is able to get into an effective and appropriate containment position in a timely manner, in accordance with the security plan.
(5) The operator of the central alarm station obtains a 'pass' score if all the appropriate personnel are notified and dispatched in a timely manner, using the prescribed radio procedures.

Annex XV

EXAMPLES OF ROOT CAUSES OF DEFICIENCIES IN A PHYSICAL PROTECTION SYSTEM

XV–1. The effectiveness of a physical protection system (PPS) can be influenced by many factors, including equipment malfunction or failure, as well as deficiencies in policies, procedures or training. Evaluation methods, such as performance testing, can determine if protection elements are functioning as required and as documented in models and simulations. Intrusion detection systems can be subject to nuisance and false alarms, which are examples of deficiencies in the PPS. The nuisance alarm rate — that is, the number of alarms generated over a specified period by occurrences not associated with the intrusion of an adversary — need to be as low as possible for an effective PPS. These occurrences might be caused by environmental factors, such as wind, rain or wildlife, or by authorized personnel inadvertently setting off alarms. They may also result from poor system installation or design. Nuisance alarms generated by the equipment itself (e.g. alarms caused by poor design or component failure) are described as false alarms and are not addressed further in this annex. A high rate of nuisance and false alarms might lead to a decline in operator attention, potentially decreasing the overall effectiveness of the PPS. Controlling and maintaining the environment around the sensor can help minimize nuisance and false alarms and therefore contribute to the overall effectiveness of the PPS (see IAEA Nuclear Security Series No. 40-T, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities [XV–1]).

XV–2. Once protection deficiencies are identified, corrective actions can be implemented. The development of corrective actions for PPS deficiencies includes the identification of the root causes of those deficiencies. Corrective actions that address the root causes of deficiencies will help prevent the reoccurrence of those deficiencies in the future. This annex provides examples of root causes that can lead to deficiencies in a PPS.

IMPROPER INSTALLATION, CALIBRATION OR ALIGNMENT OF ELEMENTS OF A PHYSICAL PROTECTION SYSTEM

XV–3. Periodic maintenance and calibration testing are useful to determine whether the PPS elements and subsystems are correctly installed, aligned and calibrated. Improper installation, calibration or alignment of sensors might

significantly reduce their sensitivity and contribute to false alarms, making them potentially less effective in the case of a criminal or intentional unauthorized act. More detailed information on PPS installation, calibration and alignment can be found in Ref. [XV–1].

INADEQUATE TESTING AND MAINTENANCE PROGRAMME

XV–4. PPS devices are continuously exposed to operational conditions that can reduce the life of the components (e.g. weather conditions, mechanical impacts, voltage variations, radiation). The physical protection network's operational life is extended and PPS availability increases with periodic preventive maintenance. PPS network maintenance and testing activities have to comply with computer security requirements.

XV–5. PPS network maintenance can be preventive (i.e. scheduled) or urgent (i.e. unscheduled or associated with an outage or deviation of system components from their specifications). The conduct of periodic maintenance and operability tests can assist with monitoring the performance of the PPS. It can also assist with ensuring that the network continues to operate and that it is reliable, available and effective for the collection and communication of data from automated physical protection subsystems. Additional information is provided in Ref. [XV–1].

PHYSICAL AND ENVIRONMENTAL CONDITIONS

XV–6. Physical and environmental conditions at the facility can affect the performance of PPS elements. These conditions include camera selection, camera placement, topography, vegetation and lighting conditions. The failure to accurately assess a sensor alarm owing to environmental conditions inevitably limits the ability of the command and control function to direct a response. Additionally, a high rate of nuisance alarms caused by the environment might lead to a decline in operator attention, with a potential effect on the response to alarms for actual criminal or intentional unauthorized acts and alarms. Failing to accurately assess an alarm can thus reduce the effectiveness of the PPS.

UNRELIABLE POWER SOURCES

XV–7. The purpose of the electrical power system is to provide a reliable power source for the PPS and its subsystems during normal operation and emergencies.

Redundancy can prevent individual component failures from leading to a failure of the whole system. The alarm records of the central alarm station can be reviewed to determine the frequency of loss of power signals, which might reduce the effectiveness of the PPS.

REFERENCE TO ANNEX XV

[XV–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).

Annex XVI

USE OF NUCLEAR MATERIAL ACCOUNTING AND CONTROL ELEMENTS TO EVALUATE THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEMS

XVI–1. This annex addresses how nuclear material accounting and control elements — including records, physical inventories, measurements and controls — interface with elements of physical protection and can be evaluated to determine the overall effectiveness of the protection of nuclear material and nuclear facilities.

MAINTENANCE OF RECORDS

XVI–2. An effective nuclear material accounting and control system provides accurate and complete records that are essential for resolving irregularities involving nuclear material. The records include information about the identity (e.g. unique item identification number), type, form, quantity and location of all nuclear material in the facility. Records have to be updated each time an item of nuclear material is received, transferred, relocated, processed, produced, shipped or discarded. Records have to be updated in a timely manner, with nuclear material transactions being recorded as soon as practicable after they occur. For the purposes of evaluating the effectiveness of physical protection systems (PPSs), nuclear material accounting and control records are relied on to validate the late detection of theft or diversion of nuclear material. An insider threat scenario involving the protracted theft of small quantities of nuclear material over several inventory periods might result in a late detection when the detection relies on the comparison of nuclear material accounting and control records over several inventory periods. In the case of missing nuclear material, whether stolen, diverted, lost or misused, the nuclear material accounting and control records provide evidence of the nuclear material that ought to be in the facility, and these records can be used to determine what is missing. The nuclear material accounting and control records are essential for resolving questions about missing or diverted[1] nuclear material.

[1] Missing material might or might not be diverted by an insider, and material is not considered to be stolen until it leaves the site.

PHYSICAL INVENTORY CHECKS

XVI–3. Physical inventories confirm the presence of nuclear material and the accuracy of the accounting records or the book inventory. They provide evidence that the facility's nuclear material accounting and control system is effective. The frequency of the physical inventory checks depends on the quantities and category of the nuclear material. Conditions and methods for the physical inventory are described in IAEA Nuclear Security Series No. 25-G, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities [XVI–1]. All nuclear material has to be measured at the time of the physical inventory. Alternatively, there would need to be a prior measurement whose integrity had been ensured through a tamper-indicating device. The material would also need to have been subject to an effective material surveillance programme. The physical inventory is an element for consideration during the evaluation and performance testing processes. For evaluation purposes, the frequency of inventory checks can be used to limit the period when an insider threat activity can occur. For example, if the insider theft strategy is to remove multiple small quantities of nuclear material that are lower than the detection limit of the radiation detection portal, the number of trips that would be needed between scheduled inventory periods and the amount that could be taken in each attempt is an indication of the effectiveness of the PPS. If 5 kg of ^{235}U is the target quantity and the inventory period is every two months (60 days), with the facility operating five days a week, the insider would need to successfully remove 125 g each day to reach the target quantity in two months. The evaluation interface between the PPS measures and the nuclear material accounting and control measures is the relationship between the inventory periods and the sensitivity limit of the radiation detection portal to detect low quantities of nuclear material. This example simply outlines the interface between these measures.

XVI–4. A physical inventory check, if properly executed, is a performance test of the nuclear material accounting and control procedures and system. If the physical inventory does not agree with the book inventory, it is evidence either that there is a problem with the nuclear material accounting and control system or that nuclear material has been lost or stolen.

XVI–5. A physical inventory check conducted as part of the evaluation of the PPS may involve all of the facility's nuclear material or only part of it, depending on the extent of the performance test.

MEASUREMENTS OF NUCLEAR MATERIAL

XVI–6. Measurements of nuclear material are an important element of the nuclear material accounting and control system. Knowledge about the quantities of nuclear material helps deter and detect unauthorized removal. If a container of nuclear material is missing, an investigation and search has to be conducted. If the missing container is located, a measurement has to be taken to ensure that the appropriate type and quantity of nuclear material is still present in the container, assuming that the nuclear material was measured before it went missing and that records of the nuclear material and its measurements were prepared and maintained. In addition to determining whether 'found' nuclear material is the same nuclear material that was lost, accurate and precise measurements help deter and detect unauthorized removal. Inaccurate and imprecise measurements could conceal unauthorized removal. The quantity and type of nuclear material received, stored, processed or shipped from the facility has to be established through measurements.

XVI–7. Measurements can be an effective protection element against insider threats and therefore need to be considered during the evaluation and performance testing processes. The frequency of measurements, the location in a process line where a measurement is taken, and the accuracy of the measurements are all important evaluation considerations. Other applicable protection elements that interface with nuclear material accounting and control and physical protection during measurements include the detection of unauthorized activity by other personnel (i.e. the two-person rule), the monitoring of processes using cameras, the protection of measurement equipment and data, and the response to a measurement discrepancy.

XVI–8. In the example outlined in para. XVI–3, the theft strategy of the insider includes a material acquisition step that involves either a single action or multiple actions to obtain the target quantity of nuclear material for the theft. The facility processes and protection elements determine the nuclear material accounting and control and PPS interface for the facility's insider threat mitigation strategy. One example may be the process of dividing and repackaging a larger quantity of nuclear material into smaller containers. Typically, measurements of nuclear material are conducted during this process to establish and maintain accurate records. The starting value agrees with the total of the smaller, final values (assuming minimal process loss) within a defined limit of error, which varies according to the initial state of the material (i.e. powder or pellets). The insider threat mitigation strategy includes protection measures during the insider's nuclear material acquisition step, as well as other interface protection measures.

These protection measures are effective in limiting the amount of nuclear material that can be removed during the repackaging activity, and probabilities of detection can be assigned using the statistical analysis of measurement errors and expert judgement.

NUCLEAR MATERIAL CONTROLS

XVI–9. The purpose of nuclear material controls is to preclude the unauthorized use of nuclear material. Controls need to be established to authorize activities for handling, processing or storing nuclear material. Nuclear material controls can consist of activities associated with maintaining the integrity of the records system for nuclear material; coordination with PPS controls for access to nuclear material, equipment and data; material confinement; material surveillance; radiation monitoring; and item control. Control measures can also include tamper-indicating devices, separation of duties, dual locks, and process or item monitoring.

XVI–10. Nuclear material control measures are designed to deter and detect any actions that could lead to unauthorized removal or misuse of nuclear material, especially such actions taken by an insider adversary. If a nuclear material accounting and control system is effective, the accounting and control measures together detect removal or unauthorized activities involving nuclear material.

XVI–11. Most nuclear material controls provide ‘delayed’ detection of a criminal or intentional unauthorized act. These controls may include passive tamper-indicating devices and seals, process monitoring, container restraints or tiedowns.

XVI–12. Some nuclear material controls may provide prompt detection during the event. These measures may include electronic (active) tamper-indicating devices that send an alarm either to operations or to the central alarm station; observation of the two-person rule; radiation monitoring equipment that produces an alarm when the containment has been breached; and procedural steps or checks to immediately verify that an activity has been properly completed.

XVI–13. Nuclear material controls may also include process monitoring, with in-process measurements, to determine if the nuclear material throughput of a process is consistent with historical statistical values or if a gain or loss of nuclear material has occurred. Statistical models can be useful tools for process monitoring to determine or detect abnormalities in the process. Depending

on the process and the associated protection measures that are designed and implemented, nuclear material controls that interface with other protection measures can provide timely detection. An example of an interface between nuclear material accounting and control and the PPS that could be evaluated is a scenario in which the insider adversary has to defeat a combination of nuclear material control measures and PPS measures during the unauthorized removal attempt. In the repackaging example described in para. XVI–8, the insider strategy is either to divert a small amount of nuclear material in each repackaging action or to acquire a container of repackaged material prior to it being recorded in the nuclear material accounting and control records system. The protection against this insider threat may include the following measures: the two-person rule, item control, material surveillance, and pre- and post-measurements or item counts, as well as other nuclear material accounting and control measures and PPS measures, which may interface. These measures are effective in limiting the amount of nuclear material that can be removed during the repackaging activity. The associated probabilities of detection for each of these elements, or for a combination of elements, can be assigned based on procedural compliance, statistical analysis for measurement error and expert judgement.

XVI–14. Performance testing of procedures and personnel actions can be used to verify compliance with approved procedures, while the use of expert opinion or direct observation is commonly used to establish detection values.

REFERENCE TO ANNEX XVI

[XVI–1] 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).

Annex XVII

EXAMPLE OF AN INSIDER ANALYSIS METHOD

XVII–1. A qualitative tabletop methodology is one of the assessment modelling tools that can be used to systematically evaluate the effectiveness of a physical protection system (PPS) through the use of subject matter experts. This methodology follows a scenario approach that is based on the opinion of subject matter experts, documented values or a combination of both. The methodology can use either qualitative or quantitative input to document the effectiveness of physical protection against defined insider threats.

XVII–2. Evaluating the effectiveness of protective measures involves scenario development and analysis to ensure comprehensive and credible insider scenarios. The effectiveness of the PPS is evaluated against these scenarios. If deficiencies in the PPS are identified, then upgrades are proposed and analysed for effectiveness prior to their implementation.

XVII–3. Insiders pose a unique problem because they can choose optimum strategies as they have more opportunities to select the most vulnerable target and the best time to attempt a criminal or intentional unauthorized act. Such an act can extend over a long period or abruptly, maximizing the likelihood of success. The insider can, for example, defeat operational and safety systems to delay detection and response. The insider might be able to falsify accounting records and repeatedly steal small amounts of nuclear material. Additionally, evaluating an abrupt theft can involve an insider acting either alone or in collusion with another insider. Generally the evaluation considers target acquisition followed by removal through security layers 1 through N. The total probability of detection for the scenario is a function of the probability of detection at each step or layer of the scenario. The example in paras XVII–4 to XVII–19 shows five security layers ($N = 5$) but could have as many layers as exist in the system being modelled.

ABRUPT THEFT

XVII–4. One process for evaluating the PPS against abrupt theft by an insider involves the following steps:

(1) Developing a list of actions for the theft of a selected target;
(2) Identifying insider strategies and protection measures;

(3) Assigning a preliminary protection probability and identifying the best insider strategy for theft;
(4) Describing the detailed insider adversary action and a specific defeat strategy;
(5) Combining the analysis into a final system effectiveness evaluation table.

XVII–5. During this process, the evaluator selects the insider threat group(s) with the highest threat for each specific target as a starting point and ensures that all insider threat groups and target combinations are evaluated. Many of the details developed for the higher threat groups also apply to the lower threat groups, since analysing all targets and all insiders for all scenarios is generally not possible.

XVII–6. In terms of a specific example, it is assumed that the nuclear material targets are contained in drum containers located in a stand-alone, locked building and that the nuclear material technician is the insider adversary. Table XVII–1 shows the hypothetical initial actions of this insider.

XVII–7. In actions 1 and 2 in Table XVII–1, the insider follows the normal two-person rule and performs authorized actions — as far as possible — to enter the protected area and the storage room. These two security layers can be removed from further analysis.

TABLE XVII–1. HYPOTHETICAL INITIAL ACTIONS FOR THEFT BY AN INSIDER

Action No.	Area	Insider action
1	Protected area	Enter the protected area using authorized access
2	Storage room	Enter the storage room using authorized access
3	Inside storage room	Acquire the target
4	Storage room	Remove the target from the storage room
5	Protected area	Exit the protected area with the target

XVII–8. In action 3 in Table XVII–2, once the insider deviates from routine activity, sensing and assessment opportunities are possible. When the insider deviates from routine activity, they try to minimize detection and, in the case of an active 'violent' insider, they act overtly to minimize detection.

XVII–9. The analyst then identifies the possible insider strategies that support a successful insider action. Each insider action of the evaluation needs to examine the potential strategies an insider can take, creating multiple insider strategies per insider action (see Table XVII–2). The analyst then identifies all the existing protection measures that might detect or delay each listed insider strategy. Note: The insider strategies listed in Tables XVII–1 and XVII–2 are hypothetical and are used for demonstration purposes only.

XVII–10. The next step in the analysis is to assign preliminary, 'independent' probability of sensing (P_S) and probability of assessment (P_A) values for each protection measure, based on the potential insider (defeat) strategies for that adversary action. In this example of abrupt theft evaluation, preliminary P_S and P_A qualitative values are assigned using expert judgement. These preliminary values are assigned based on factors such as the facility conditions, PPS and nuclear material accounting and control procedures and compliance, the two-person rule, line of sight conditions, and the security culture. Assigning the P_A assumes that sensing has occurred. This approach ensures the proper determination of which protection element is deficient and needs to be improved. In other words, if sensing is not assumed to have occurred, the P_A cannot be properly evaluated nor can the actual conditions and potential improvements be determined.

XVII–11. The evaluation continues by comparing protection measure P_S and P_A values for each defeat strategy. The lowest probability for either sensing or assessment determines the lowest level of protection against that insider strategy, as compared with the other strategies for that adversary action (see Table XVII–3).

XVII–12. Table XVII–3 reflects that the best potential combined strategies to acquire the target would be by falsifying shipping papers to open a target container (action 3), then hiding the target using tools or equipment (action 4), then at a later time and once outside the storage location, throwing the target over the fence (action 5).

TABLE XVII–2. HYPOTHETICAL INSIDER STRATEGIES AND PROTECTION MEASURES AT EACH INSIDER ACTION

Action No.	Area	Action	Insider strategy	Existing protection measure
3	Inside storage room	Acquire the target	Remove the target from the container and hide on person, on another person or in another location	Access control to the target, two-person rule
			Falsify shipment to acquire material	NMAC shipment procedure, NMAC records, two-person rule
4	Storage room	Remove the target from the storage room	Hide on person	Two-person rule
			Hide using tools or equipment	Two-person rule
			Falsify shipment to remove material	NMAC shipment procedure, NMAC records, guard escort
			Hide inside waste	Separation of duties, two-person rule
5	Protected area	Exit the protected area with the target	Hide on person	Nuclear material detection and manual search
			Hide using tools or equipment	Nuclear material detection and manual search
			Hide inside waste	Nuclear material detection for vehicles and manual search
			Falsify shipment	NMAC shipment procedure, NMAC records, guard escort
			Throw over the fence	General observation, random patrols, 20 m clear zone

Note: NMAC — nuclear material accounting and control.

TABLE XVII–3. ASSIGNED PRELIMINARY PROTECTION PROBABILITIES AND IDENTIFICATION OF THE BEST INSIDER STRATEGY FOR THEFT AT EACH INSIDER ACTION

Action No.	Area	Action	Insider strategy	Existing protection measure	P_S	P_A
3	Inside storage room	Acquire the target	Remove the target from the container and hide on person, on another person or in another location	Access control to the target, two-person rule	M	VH
			Falsify shipment to acquire material	NMAC shipment procedure, NMAC records, two-person rule	M	M
4	Storage room	Remove the target from the storage room	Hide on person	Two-person rule	M	VH
			Hide using tools or equipment	Two-person rule	M	H
			Falsify shipment to remove material	NMAC shipment procedure, NMAC records, guard escort	H	VH
			Hide inside waste	Separation of duties, two-person rule	M	VH

TABLE XVII–3. ASSIGNED PRELIMINARY PROTECTION PROBABILITIES AND IDENTIFICATION OF THE BEST INSIDER STRATEGY FOR THEFT AT EACH INSIDER ACTION (cont.)

Action No.	Area	Action	Insider strategy	Existing protection measure	P_S	P_A
5	Protected area	Exit the protected area with the target	Hide on person	Nuclear material detection and manual search	VH	VH
			Hide using tools or equipment	Nuclear material detection and manual search	H	VH
			Hide inside waste	Nuclear material detection for vehicles and manual search	H	H
			Falsify shipment	NMAC shipment procedure, NMAC records, guard escort	VH	VH
			Throw over the fence	General observation, random patrols, 20 m clear zone	M	L

Note: Possible values are indicated as follows: VL — very low (0.00–0.20); L — low (0.21–0.40); M — moderate (0.41–0.60); H — high (0.61–0.80); VH — very high (0.81–1.00). NMAC — nuclear material accounting and control; P_S — probability of sensing; P_A — probability of assessment.

XVII–13. The next step in the analysis is to develop a detailed adversary action sequence (see Table XVII–4) by describing various insider actions and protection elements to create credible insider theft scenarios, for example as follows:

(1) Developing the list of actions and strategies into detailed descriptions;
(2) Determining the credibility of insider actions;
(3) Describing specifically how the insider accomplishes each action;
(4) Describing protection measures, if any.

TABLE XVII–4. DETAILED DESCRIPTION OF SEQUENCE OF INSIDER ACTIONS

Action No.	Insider action against the established protection measure
3	Falsify shipment to acquire material — provide a detailed description for this strategy to be successful in defeating the protection measures. NMAC shipment procedure, NMAC records, two-person rule — provide a detailed description for these protection measures to either detect the insider strategy or to be defeated.
4	Hide using tools or equipment — provide a detailed description for this strategy to be successful in defeating the protection measures. Two-person rule — provide a detailed description for this protection measure to either detect the insider strategy or to be defeated.
5	Throw over the fence — provide a detailed description for this strategy to be successful in defeating the protection measures. General observation, random patrols, 20 m clear zone — provide a detailed description for these protection measures to either detect the insider strategy or to be defeated.

Note: NMAC — nuclear material accounting and control.

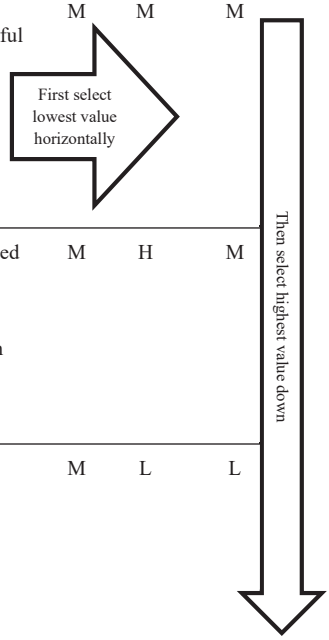
XVII–14. During the process of detailing the insider actions against the established protection measures, as shown in Table XVII–4, the preliminary protection probabilities assigned (see Table XVII–3) may be revised (see Table XVII–5), based on additional input.

XVII–15. The next step in the analysis is to develop a table, such as the one shown in Table XVII–5, that evaluates the system effectiveness for this scenario. This step in the analysis is undertaken by analysing each documented adversary action as follows:

(a) Within each adversary action, the P_S and the P_A is evaluated individually. To assign the P_A, sensing has to be assumed to have occurred. Therefore, the P_A value is assigned after the P_S has been assigned. This approach helps determine whether sensing and/or assessment capabilities are lacking for this step.

TABLE XVII–5. SYSTEM EFFECTIVENESS EVALUATION

Action No.	Insider action against the established protection measures	P_S	P_A	Adversary action score
3	Falsify shipment to acquire material — provide a detailed description for this strategy to be successful in defeating the protection measures. NMAC shipment procedure, NMAC records, two-person rule — provide a detailed description for these protection measures to either detect the insider strategy or to be defeated.	M	M	M
4	Hide using tools or equipment — provide a detailed description for this strategy to be successful in defeating the protection measures. Two-person rule — provide a detailed description for this protection measure to either detect the insider strategy or to be defeated.	M	H	M
5	Throw over the fence — provide a detailed description for this strategy to be successful in defeating the protection measures. General observation, random patrols, 20 m clear zone — provide a detailed description for these protection measures to either detect the insider strategy or to be defeated.	M	L	L
System effectiveness				M



Note: Using expert judgement, assign probability of sensing (P_S) and probability of assessment (P_A) values based on the insider strategy versus the protection measures. Possible values are indicated as follows: VL — very low (0.00–0.20); L — low (0.21–0.40); M — moderate (0.41–0.60); H — high (0.61–0.80); VH — very high (0.81–1.00).

(b) Each documented adversary action has to both ‘sense’ the insider action and ‘assess’ the insider action for the step protection to be considered effective (i.e. both assigned values need to be high to very high).

(c) The score for each adversary action is determined using the lowest qualitative value, horizontally, in the table for the assigned P_S or P_A. This value is recorded in the last column as the action score. This process is an intuitive approach, where the lowest contributing factor to the probability of detection determines the maximum protection value or scope for the adversary action.

The system effectiveness score is determined by selecting the highest value in the action score column of the table, and recording that value in the system

effectiveness line (see Table XVII–5). This approach identifies which protection element contributing to the probability of detection is lacking. This process is an intuitive approach where the adversary action that has the highest probability of detection determines the maximum protection value against the scenario.

XVII–16. In this example, the effectiveness of the PPS against the insider for unauthorized removal is 'moderate'.

XVII–17. IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures Against Insider Threats [XVII–1], presents scenario analysis as an example method for assessing a facility's PPS against an insider threat.

XVII–18. Evaluating collusion between two or more insiders is a difficult process since there is a large number of combinations of potential insiders to consider, each with different access, authority and knowledge.

XVII–19. If the design basis threat or the representative threat statement includes collusion between insiders, then the evaluation of the effectiveness of measures that would help prevent collusion (e.g. compartmentalization and surveillance, along with preventive measures) may be the best approach.

PROTRACTED THEFT: QUALITATIVE EVALUATION

XVII–20. For the evaluation of scenarios involving protracted theft, P_S and P_A are a function of elapsed time, the number of acquisition attempts and the quantity of nuclear material taken per attempt. P_S and P_A generally increase as the rate of thefts and/or the quantity per theft increases, and they also change depending on the number of cumulative attempts.

XVII–21. For scenarios involving protracted theft from the target area (i.e. repeated attempts), the following assumptions can be made:

(a) Small quantities of nuclear material are easier to remove undetected than large quantities.
(b) Multiple theft attempts are necessary to obtain a large target quantity of nuclear material.
(c) The multiple theft attempts extend the overall timeline, resulting in a longer timeline than for an abrupt theft.
(d) The chance of being detected increases as the number of attempts increases.

The same process can be applied to a protracted diversion to an unauthorized location within the facility to prepare the target for a later abrupt theft from the facility.

XVII–22. Using the same method as the one demonstrated to create the outputs of Table XVII–5 to determine system effectiveness, Table XVII–6 is created but with expert judgement accounting for the additional repeated adversary actions in an acquisition step for a protracted theft.

XVII–23. Typically, each action in Table XVII–6 describes a single adversary action with assigned P_S and P_A. In the protracted acquisition described in action 1 of Table XVII–6, the expert group considers the number of repeated attempts to be 100 and also considers a certain amount of nuclear material to be diverted in each attempt. As this occurs over a 12 month period, the expert group needs to make judgements in relation to the P_S and the P_A for that adversary action. The P_S and P_A values are based on actual facility conditions and on protection

TABLE XVII–6. EXAMPLE OF AN INSIDER PROTRACTED THEFT SCENARIO ANALYSIS

Action No.	Insider action against the established protection measure	P_S	P_A	Adversary action score
1	Acquisition step — The insider removes X g of nuclear material for later retrieval once the goal quantity has been accumulated. The insider repeats this process for 100 assumed attempts over 12 months. Given the number of repeated attempts, the P_S and P_A, which are based on several assumed effective protection measures and material accounting elements, are assumed to be high.	H	H	H
2	Insider exits through security layer 1.	M	H	M
3	Insider exits through security layer *N*.	M	H	M
System effectiveness				H

Note: Possible values are indicated as follows: VL — very low (0.00–0.20); L — low (0.21–0.40); M — moderate (0.41–0.60); H — high (0.61–0.80); VH — very high (0.81–1.00). P_S — probability of sensing; P_A — probability of assessment.

measures and material accounting elements intended to defeat such insider actions, for multiple attempts over time to acquire the material and a single attempt or multiple attempts to exit the facility.

PROTRACTED THEFT: QUANTITATIVE EVALUATION

XVII–24. Figure XVII–1 illustrates how the probabilities of detection for physical protection, for material control and for material accounting work together in a generic scenario. The timeline is separate for the acquisition stage, the accumulation stage and the exit stage.

XVII–25. In a protracted theft scenario, the material accounting system works independently from the PPS. When the insider acquires nuclear material (in this case, through protracted theft (small or large)), the probability of detection ($P_S \times P_A$) timeline starts (illustrated by Fig. XVII–1(a)).

XVII–26. The timeline continues as the insider accumulates nuclear material inside the facility for later removal. During accumulation, either through a random nuclear material accounting and control physical inventory check, a process activity, or the identification of material being out of place, the material accounting system may identify an abnormality (illustrated by Fig. XVII–1(b)).

XVII–27. The timeline concludes when the insider removes the nuclear material from the site through one or more attempts. During the exit of the nuclear material through security layers 1,…*N*, the PPS has a given value for the probability of detection (illustrated by Fig. XVII–1(c)).

XVII–28. Material accounting systems for protracted theft might identify an abnormality but might not identify the cause of the abnormality. Protection measures for nuclear material accounting and control need to consider the elapsed time between acquisition attempts, the number of acquisition attempts and the quantity of material taken per attempt. The ability of measures for nuclear material accounting and control to detect theft increases as the cumulative number of attempts, the rate of attempts and the quantity of material per theft increases [XVII–2]. The evaluation of the total probability of detection for protracted theft using a quantitative method is demonstrated below and in Fig. XVII–1.

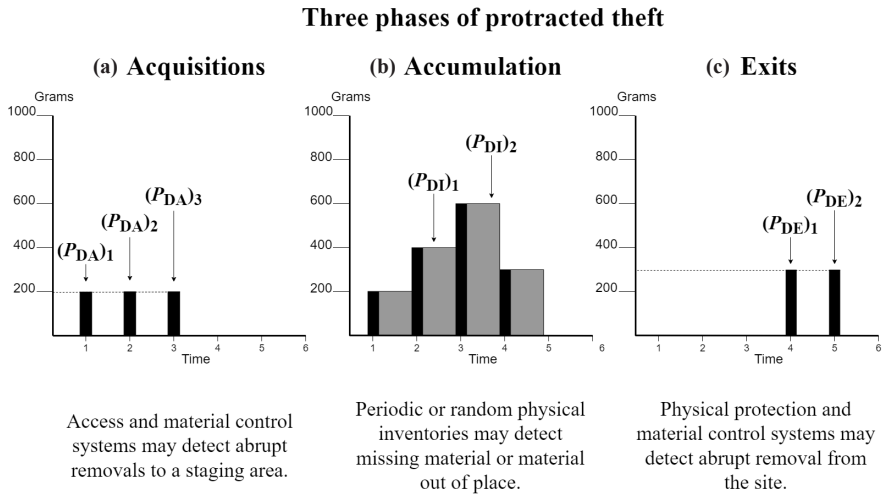


FIG. XVII–1. Probability of detection for three phases of protracted theft of nuclear material: (a) acquisitions, (b) accumulation, (c) exits.

$$P_{\text{D total}} = 1 - \prod_{i=1}^{l} \left(1 - (P_{\text{DA}})_i\right) \times \prod_{j=1}^{m} \left(1 - (P_{\text{DI}})_j\right) \times \prod_{k=1}^{n} \left(1 - (P_{\text{DE}})_k\right)$$

where

$(P_{\text{DA}})_i$ is the probability of detection during an acquisition *i*;

$(P_{\text{DI}})_j$ is the probability of detection during a physical inventory *j*;

$(P_{\text{DE}})_k$ is the probability of detection during an exit *k*;

$\prod_{i=1}^{l} \left(1 - (P_{\text{DA}})_i\right)$ is the total avoidance of detection for *l* acquisitions;

$\prod_{j=1}^{m} \left(1 - (P_{\text{DI}})_j\right)$ is the total avoidance of detection for *m* physical inventories;

and $\prod_{k=1}^{n} \left(1 - (P_{\text{DE}})_k\right)$ is the total avoidance of detection for *n* exits.

There is a special case that the probabilities of detection for all acquisitions, all physical inventories and all exits are the same, respectively. This allows the avoidance of detection for acquisitions, physical inventories and exits to be represented as follows:

$$\left(1-\left(P_{\mathrm{DA}}\right)\right)^{l}$$

$$\left(1-\left(P_{\mathrm{DI}}\right)\right)^{m}$$

$$\left(1-\left(P_{\mathrm{DE}}\right)\right)^{n}$$

where l is the total number of acquisition events, m is the total number of physical inventories, and n is the total number of exit events. Therefore, in this special case $P_{\mathrm{D\ total}}$ is represented as:

$$P_{\mathrm{D\ total}} = 1-\left(1-\left(P_{\mathrm{DA}}\right)\right)^{l} \times \left(1-\left(P_{\mathrm{DI}}\right)\right)^{m} \times \left(1-\left(P_{\mathrm{DE}}\right)\right)^{n}$$

SABOTAGE

XVII–29. Evaluation of sabotage scenarios involves consideration not only of unauthorized acquisition of material but also of attacks on the facility. All preventive and protective measures applied to theft can be applied to sabotage; the evaluation method for sabotage is the same as for abrupt theft. For sabotage, the insider does not need to leave the facility with nuclear material, so the preventive and protective measures against exiting the facility might not apply. Additional considerations for sabotage include potential attacks on, or the compromise of, systems or equipment such as cooling pumps, control equipment or valves.

REFERENCES TO ANNEX XVII

[XVII–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[XVII–2] SICHERMAN, A., "Evaluating late detection, capability against diverse insider adversaries," UCRL-97740, paper presented at American Nuclear Society Topical Conf., San Diego, 1987.

IAEA
International Atomic Energy Agency

CONTACT IAEA PUBLISHING

Feedback on IAEA publications may be given via the on-line form available at:
www.iaea.org/publications/feedback

This form may also be used to report safety issues or environmental queries concerning IAEA publications.

Alternatively, contact IAEA Publishing:

Publishing Section
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530
Email: sales.publications@iaea.org
www.iaea.org/publications

Priced and unpriced IAEA publications may be ordered directly from the IAEA.

ORDERING LOCALLY

Priced IAEA publications may be purchased from regional distributors and from major local booksellers.