IAEA NUCLEAR SECURITY SERIES NO. XX

NST029

July 2022

Step 8 Member State Review

NST 029 EVALUATION OF PHYSICAL PROTECTION SYSTEMS AT NUCLEAR FACILITIES

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

FOREWORD

[to be added later]

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The physical protection of nuclear material and nuclear facilities is a major part of the national nuclear security regime for those States that have such material and facilities. IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [1], provides recommendations for States on developing or enhancing, implementing and sustaining effective physical protection. IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [2], provides guidance on how to implement those recommendations. Reference [1] emphasizes the importance of evaluating physical protection systems, including performance testing.

1.2. The Convention on the Physical Protection of Nuclear Material [3] provides a framework for ensuring the physical protection of nuclear material used for peaceful purposes while in international transport. 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 [3] to cover nuclear material and nuclear facilities in domestic use, storage and transport used for peaceful purposes, as well as sabotage thereof. Reference [1] provides guidance to States that are parties to Convention [3] and its Amendment [4] on meeting their obligations.

1.3. Ensuring that the physical protection system (PPS) at a nuclear facility is operating as designed is crucial for the security of nuclear material and nuclear facilities. An evaluation of the individual components and the system as a whole provides a measure of the effectiveness of the facility's PPS. This publication provides guidance on methods that can be used to conduct these evaluations.

OBJECTIVE

1.4. This Technical Guidance provides Member States with practical guidance on methods for evaluating the effectiveness of PPSs in protecting nuclear material in use and storage against unauthorized removal, and in protecting nuclear material and facilities against sabotage. This publication focuses on methods to evaluate the system effectiveness of the PPS as well as performance testing.

1.5. This Technical Guidance addresses roles and responsibilities, methods that may be required or recommended by a competent authority, the need for documentation, and the frequency of effectiveness evaluations and testing.

SCOPE

1.6. This Technical Guidance describes methods for evaluating PPS effectiveness and methods for evaluating nuclear material accounting and control procedures and systems. Although intended for nuclear material and nuclear facilities, the concepts and guidance in this publication may also be applied to other radioactive material and associated facilities and activities [16 and 17].

1.7. This Technical Guidance does not address the evaluation of computer security for the protection of nuclear facilities, although some aspects of blended attacks (combined cyber and physical attacks) are addressed in the context of the evaluation of physical protection systems. Information on this topic can be found in [11] and [12].

1.8. In addition, this publication does not address security of nuclear material in transport; information on this topic can be found in [1] and [19].

1.9. The following are outside the scope of this publication:

— Response to a nuclear or radiological emergency that might result from a nuclear security event (response to nuclear or radiological emergencies can be found in [20]);

— Mitigation or minimization of the radiological consequences of sabotage at nuclear facilities (response to nuclear or radiological emergencies can be found in [20]);

— Location and recovery of nuclear material out of regulatory control (information on this topic can be found in [21]);

— Physical protection considerations in the siting of nuclear facilities (information on this topic can be found in [22]).

STRUCTURE

1.10. Section 2 of this publication provides an overview of the evaluation of PPSs, Section 3 provides a detailed description of PPS evaluation processes and methods to verify that protection requirements are met, and Section 4 provides guidance on considerations when developing a performance based evaluation programme for the PPS. Appendix A describes considerations to be taken into account when planning a PPS effectiveness evaluation. Annex I provides examples of test plans for different protection elements. Annex II provides examples of root causes that can lead to deficiencies in a PPS. Annex III provides methods for evaluating nuclear material accounting and control elements. Annex IV describes the path analysis method. Annex V provides an example of an insider analysis method for abrupt theft and 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 [5] 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."

2.2. The evaluation of a PPS is essential to maintaining its effectiveness and determining if the applicable security requirements for a facility are met. The State should define the assessment frame of reference used to conduct the evaluation. When applicable, it should be consistent with the capabilities described in the national threat statement. Below, FIG.1 illustrates a methodological framework for evaluating the effectiveness of a PPS.

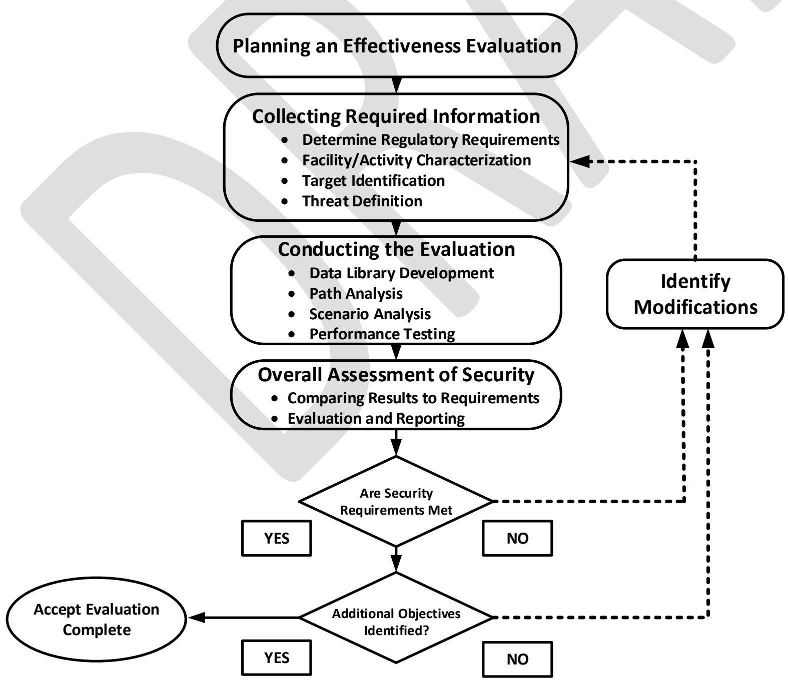


FIG. 1. The effectiveness evaluation methodological framework

2.3. As outlined in FIG. 1, the first step of any evaluation of PPS is planning the evaluation process. The second step is collecting the required information. The third step is conducting the evaluation. The fourth step is to assessment the overall security against the regulatory requirements. The last step is to determine if security meets the regulatory requirements. If security does not meet the regulatory requirements, then security upgrades or modifications are identified and evaluated for effectiveness. If security meets the regulatory requirements, then the process is complete.

METHODS FOR EVALUATION OF PHYSICAL PROTECTION SYSTEMS

2.4. The methods for the evaluation of PPSs can be based on different approaches defined by the competent authority, and can be prescriptive, performance based or a combination of both.

2.5. When using a prescriptive approach, the methods for evaluating the PPS should include reviews of operational plans and procedures, records and logs, personnel training, interviews, and observations of the PPS operation. These methods follow a checklist approach, verifying if each applicable prescriptive requirement is met or not.

2.6. When using a performance based approach, the methods for evaluating the PPS should include performance testing, simulations and analysis tools. These methods demand a higher level of involvement, taking more time and resources than the prescriptive methods. Performance based evaluations determine if the PPS design is effective against the adversary capabilities defined in the State approved national threat statement.

2.7. A combined approach should use methods from both the prescriptive approach and the performance based approaches. These approaches are presented in more detail in Section 3 and additional guidance can be found in Refs. [1] and [2].

2.8. Details on specific performance assurance methods that can be used for conducting evaluations of physical protection measures can be found in TABLE 1.

THE ROLE OF RISK MANAGEMENT IN EVALUATIONS

2.9. 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."

2.10. 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."

Risk management may 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. Additionally, the State or the competent authority may manage risk based on a facility by facility basis. Risk management decisions are derived through effectiveness evaluations of PPS and performance testing. More detailed guidance on risk management can be found in Ref. [2].

PERFORMANCE METRICS FOR A PHYSICAL PROTECTION SYSTEM

2.11. The performance metrics for a PPS should be developed by the regulatory body and used to evaluate the functions of the PPS: detection, delay and response. The individual performance of each of these PPS functions are used as input to determine qualitative and quantitative PPS system effectiveness values.

2.12. Detection is a process in a PPS that begins with sensing a potentially malicious or other unauthorized act and that is completed 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.

2.13. 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.

2.14. Response is the function of the PPS that seeks to interrupt and neutralize an adversary before the completion of a malicious act. There are two performance metrics associated with response: the probability of interruption, and the probability of neutralization. The probability of interruption is the probability that the response will reach the adversary before the malicious act is accomplished, and the probability of neutralization is the probability that the response can stop an adversary before their goal is accomplished or cause an adversary to abandon their attempt.

ELEMENTS OF CHARACTERIZATION OF THE PERFORMANCE METRICS

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

2.16. Models and simulations should be used for characterizing performance metrics when direct testing cannot be performed. This often occurs because of safety concerns relating to testing or if the level of testing needed to achieve the collection of 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 address those facilities that have performance based requirements. Modelling and simulation methods include manual or computer based mathematical models, computer simulations, tabletop exercises, and exercises.

2.17. The use of statistical data for characterizing performance metrics is based on recording multiple data points through statistical sampling and testing. Statistical data may also be derived from other sources national testing organizations, civil or military agencies, vendors, or national or international publications, or similar testing.

2.18. Expert judgement can be used for characterizing performance metrics when insufficient or limited data exists and there is no effective way to conduct tests to correctly collect the data. In such cases, the evaluation would depend on values elicited from subject matter experts.

2.19. Owing to the strengths and limitations inherent in each evaluation method, multiple methods might be needed to obtain a comprehensive understanding of the effectiveness of the PPS.

INTERFACE OF THE NMAC SYSTEM WITH THE PPS

2.20. Nuclear material accounting and control measures are an important element for protection against the threat posed by a malicious insider who attempts unauthorized removal or sabotage of nuclear material. Measures to address this threat are presented in detail in IAEA Nuclear Security Series Nos 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [7] and 32-T, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement [8].

2.21. To adequately determine the effectiveness of any PPS to protect against the national threat statement, a comprehensive analysis should be carried out that includes addressing the insider threat either acting alone or in collusion with external adversaries.

2.22. The nuclear material accounting and control system operates in coordination with the PPS to control access to the areas where nuclear material is stored or used and to provide measures for controlling the nuclear material itself. Many of the technical measures are also used for or compliment physical protection measures (e.g. video surveillance systems, two-person rule, daily checks, radiation detection alarms). Information received from NMAC can be used to determine physical protection items, their categorization and location and for appropriative protective measures selection. A comprehensive evaluation of the PPS should include the evaluation of the nuclear material accounting and control system, especially where the nuclear material accounting and control measures and the physical protection measures interface.

2.23. Protecting the nuclear material at a facility relies on knowledge of the isotopic composition, type, quantity, location, use and movement of the nuclear material within the facility by and can be achieved by keeping records of the nuclear material. Protecting the nuclear material at a facility should also include maintaining control over it. The facility’s nuclear material accounting and control system includes maintaining records of the nuclear material as well as administrative and technical control measures. The accounting records, data and associated systems must be protected and secured from unauthorized access or data removal.

2.24. Examples of evaluation methods for nuclear material accounting and control are provided in Annex III. 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 at Facilities [9].

REGULATORY BODY STAFFING FOR EVALUATIONS

2.25. The staffing requirements for the regulatory body to conduct evaluations of PPS are impacted by the regulatory approach used (prescriptive, performance-based, or combined) and the various types and numbers of nuclear facilities and activities.

2.26. A performance-based regulatory approach to PPS evaluation usually includes a combination of analysis and performance testing. Often, the approach is to require the operator to conduct the analysis and testing, which is then reviewed by the regulator; this type of review takes time and sufficient knowledge to verify that it has been performed correctly and the conclusions are accurate. An approach that includes independent analyses and testing conducted by the regulator will take more time and requires significant knowledge, skills and experience in analysis and performance testing methods.

2.27. Assessments conducted under a prescriptive regulatory approach generally are not as resource intensive as a performance-based approach; however, sufficient time should be allotted to ensure all of the prescriptive requirements are met. Additionally, personnel conducting the assessment should have enough knowledge, skills, and experience to determine if PPS measures in place adequately meet the prescriptive requirements.

2.28. Facilities that store or use category I or II nuclear materials, or have the potential for unacceptable or very high radiological consequences, have higher associated risks and require more frequent, in-depth evaluation than lower risk facilities. A performance-based or combined regulatory approach should be applied to these kinds of facilities. Consequently, these facilities have significantly more impact on the resources of the regulatory body than other types of facilities.

2.29. Given the critical nature of the facilities that are assessed, it is important that the staff conducting the assessments are not overburdened to a degree that they cannot effectively perform their job. A realistic evaluation should be made regarding time, effort, and skill set required to perform an assessment of each type of facility falling under the purview of the regulatory body based on the regulatory approach and the potential risk associated with the facility. This evaluation, combined with the numbers of each type of facility, should be factored into determining optimum staffing levels and qualifications for conducting assessments.

3. PROCESS FOR THE EVALUATION OF PHYSICAL PROTECTION SYSTEMS

EFFECTIVENESS EVALUATION PROCESS

3.1. The effectiveness evaluation methodological framework is outlined in FIG 1 and provides a high-level summary of the methodology and of the key milestones during the conduct of an effectiveness evaluation.

Planning the effectiveness evaluation

3.2. The activities undertaken during the evaluation plan may be incorporated into a project plan or other planning document and may include the involvement of different internal or external organizations. The planning process may include the development of an effectiveness evolution security plan (See APPENDIX A for more detail).

3.3. Deciding the purpose of the evaluation includes the determination of the nuclear security system objectives, the proposed design or characterization of an existing nuclear security system, the evaluation of the design, and possibly a redesign or refinement of the PPS system.

Collecting required information

3.4. Information collected during the planning of the effectiveness evaluation should include:

(a) Gathering relevant regulatory requirement, reports, etc. - The starting point of the methodology is understanding the existing State regulatory framework, policies and guidance on which the security system is based. This may include oversight inspection reports, previous evaluations, and other inputs.

(b) Gathering any facility configuration and activity information for characterization - The evaluation continues with performing a facility/activity characterization which involves gathering information about facility/activity operations and conditions, such as a comprehensive description of the facility/activity, operating conditions and nuclear security requirements as well as regulatory requirements. The assessment considers the effectiveness of a system of elements that work together to ensure protection rather than regarding each element separately.

(c) Identification of facility target – Nuclear material targets as well as vital areas are identified based on information collected during facility/activity characterization. Determination of whether nuclear/radioactive materials are attractive targets is based mainly on the type of material and the goal of the adversary threat. This allows the for the identification of the objectives of the nuclear security system (what to protect against whom).

(d) Defining the threat for analysis - The step defines the national threat statement to be used for the evaluation based upon policy as defined by the competent authority and upon other considerations such as local conditions and factors about potential adversaries including intent, motivation, types, capabilities and the range of tactics.

Conducting the evaluation

3.5. Conducting an effectiveness evaluation typically includes the following activities:

(a) Data library development - Data libraries are a collection of performance test data that can be used as a basis to justify nuclear security element probability of detection, assessment or delay times used in modelling and simulation activities. Data libraries can be developed and maintained as part of any evaluation programme or process. Data is collected in the initial stages of the evaluation process and is essential to the characterization of the facility to provide documented evidence for the facility effectiveness evaluation results.

(b) Conduct path analysis - Path analysis is an evaluation method to determine whether the PPS is effective across a wide variety of paths that an adversary might take to cause unauthorized removal of nuclear material or sabotage at a facility. ANNEX IV provides a general overview of path analysis.

(c) Conduct scenario analysis - Scenarios are hypothetical sets of conditions and sequences of events constructed for the purpose of focusing attention on causal processes and decision points. Scenario Analysis consists of four steps:

1. Identify scenario sets to analyse;
2. Develop detailed scenarios;
3. Review and select final scenarios to evaluate;
4. Determine effectiveness against final scenarios.

Figure 2 illustrates how scenario analysis corresponds to the process of using paper models, tabletop exercises, 2D and 3D computer simulations, and other evaluation methods.

Overall assessment of security

3.6. The next step should include comparing the evaluation results to the regulatory requirements. The results should verify that the physical protection system as designed, or as characterized (for an existing system), satisfies the physical protection requirements as well as identifying any system deficiencies in the design or implementation that need to be addressed to meet the system requirements.

3.7. An assessment report should be developed to document the results of the evaluation, including corrective actions needed and, where appropriate, reporting the results and findings to the regulator or competent authority.

3.8. Many of these steps described above require specific background information before they can be completed. The evaluation of this information may reveal security shortcomings that need to be addressed before carrying out an effectiveness evaluation. Once the regulator is satisfied that regulatory requirements have been met, the effectiveness evaluation can then be conducted by the operator. A detailed description of this process is described in APPENDIX A.

METHODS FOR THE EVALUATION OF THE PPS

3.9. In conducting PPS evaluations, the primary approaches are the prescriptive approach, the performance-based approach and the combined approach.

3.10. Types of effectiveness evaluation methods range from simple to complex, prescriptive based to performance based, limited scope to full scope performance tests, response tests, manual evaluation methods to complex computer simulations, as well as combinations of methods. Table 1 lists types of effectiveness evaluation methods with a short description and an example for each method.

TABLE 1. EFFECTIVENESS EVALUATION METHODS

By Hand	**Description**
Checklists against prescriptive requirements	A checklist is a qualitative tool for determining presence/absence of required features or of adequacy/inadequacy of a required capability (so called because the user checks off whether the presence/absence or adequacy is present). Checklists are valuable for looking at how a system meets requirements from a high level perspective, allowing the user to identify areas that need deeper evaluation. Note that the checklist may also record adjectival scores that are assigned by an expert, such as ‘high’, ‘medium’ or ‘low’ effectiveness of some equipment or security procedure against the national threat statement based on inspection of the equipment or an analysis of a procedure.
Observation	Watching a process taking place or a procedure being performed to provide insight about how well the process is taking place or procedure is being performed. This method is often used where the evaluator does not want to disrupt the process/procedure with more intrusive methods, say for determining if a two-person rule is being performed correctly. An example of observation is when the evaluator sits in an alarm station to see whether the alarm station operators are assessing alarms correctly.
Random sampling	A method for determining a set of items to examine (selecting intelligently from that set of items) and then assigning some conclusion about the set. Sampling can be used to determine items to inspect (that is to review or examine for certain required features) or to performance test. As an example, the evaluator may select from a set of material transfer forms, see whether each of the forms are filled out correctly, and then make a determination of how well site personnel are adhering to procedures for filling out the forms. As another example, sampling might be used to determine which sensors to test during an audit if that site has many alarms. Sampling may involve selecting all items, either in the complete set itself or in a subset meeting some criteria or may involve random sampling.
Tabletops	**Description**
Map exercises	An exercise performed by people using small models of guards, RFs and adversaries performed on one or more maps
Scale model (sand table) exercises	An exercise performed by people using small models of combatants performed on a scale model of a facility or area with terrain features, vegetation, roads and buildings shown in scale. (This is called a sand table exercise because it was historically performed on a table where the terrain was modelled in sand.)
Computer based exercises	An exercise performed by people using icons of guards, RFs and adversaries that are moved on a computer display of a facility
Computer Simulations	**Description**
Human in the loop	Humans control activities performed by computer generated adversaries and defenders within an environment modelled in a computer
Constructive simulations (automated behaviour)	Computer generated adversaries and defenders are controlled by software routines (not people) within an environment modelling in a computer
Single path	Calculates P_I for one path
Performance Testing	**Description**
State/competent authority testing laboratories for barrier testing only	Facilities funded and operated to support testing of access delay systems involving either active or passive delay. Such facilities may be run by other State agencies, such as the military. Experts from these facilities develop delay times against the national threat statement to be used in evaluations and provide guidance for facilities on making upgrades.
State/competent authority testing laboratories for RF equipment	Facilities funded and operated to support testing of RF equipment, such as weapons, protective gear and fighting positions. Such facilities may be run by other State agencies, such as the military. Experts from these facilities provide guidance on RF equipment to use at facilities, training required for such equipment, and may support FoF exercises.
Facility level tests (includes component testing and subsystem testing)	These include functional/operability tests that ensure individual components are working, standardized maintenance performance tests that insure that such components meet performance requirements, simulated adversarial attack tests by skilled testers, and tests of physical protection subsystems to determine, for example, if an alarm generated on the perimeter is acknowledged and assessed properly by alarm station personnel.
Alarm response test	Performance test of RF readiness and response to an alarm by a group of responders that move to a specific location.
Response Tests	**Description**
Limited scope performance test	Tests to determine the level of a single person in performing security force or guard force responsibilities. Examples: effectiveness of searches, assessment of alarms by Central Alarm Station, use of force procedures.

Force-on-force exercises t	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 national threat statement. Typically, this is a full scale field simulation of an attack on a site involving all on-site guards and RFs.

Prescriptive approach evaluation

3.11. 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."

3.12. An evaluation of a PPS against prescriptive requirements should consist of understanding the requirements, gathering information, and then comparing the information against the requirements to determine compliance. The prescriptive approach should result in an objective assessment of the compliance of the PPS against each prescriptive requirement.

3.13. For the prescriptive approach, an evaluation of the PPS requirements should be completed prior to the conduct of any assessment or evaluation. This evaluation should establish the regulatory prescriptive baseline by reviewing the State regulatory requirements to determine the scope and criteria to be evaluated against. The competent authority can choose to develop a simple checklist outlining the requirements for evaluation to guide the review and document the results.

3.14. The State establishes specific prescriptive physical protection measures that it considers necessary to meet the State's defined physical protection objective for each category of nuclear material and each level of radiological consequences [2]. The prescriptive physical protection measures should be based on the results of the national threat statement.

3.15. Compliance with the prescriptive requirements can usually be evaluated by direct observation at the nuclear facility. The evaluation should include the following:

(a) Reviews of security plans and procedures, and records, including personnel training;
(b) Interviews and knowledge testing;
(c) Reviews of specific PPS features.

3.16. The prescriptive approach evaluation is effective when determining compliance, but is limited in the determination of the PPS effectiveness.

Review of security plans

3.17. One of the objectives of an evaluation should be to verify that the physical protection measures described in the approved security plan comply with the regulatory requirements and applicable licence conditions. This evaluation can be performed through a direct prescriptive comparison of the details of the approved security plan with the facility security programme implementation. Detailed guidance on security plans and the suggested contents of a security plan can be found in Ref. [2].

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

(a) Does the security organization structure of the facility and the responsibilities of the personnel comply with those outlined in the approved security plan?
(b) Are the security operational plans developed and up to date, as required; is there evidence that the procedures are being followed?
(c) Are external response memorandums of understandings in place and up to date?
(d) Does the security plan document facility management and organizations, as well as external responders, that are outside of the facility's security organization but have physical protection responsibilities?

Review of procedures

3.19. 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 conducted, maintained and periodically revised in accordance with the security plan. The evaluation and plan must be protected and secured from unauthorized access or data removal.

3.20. For example, the review of procedures and processes could be conducted using the following questions:

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

Review of records, including personnel training

3.21. A prescriptive evaluation should include a review of the facility, operational and personnel training records to assess compliance with the regulatory requirements. These records should be reviewed using standard inspection sampling techniques to verify if they have been consistently developed, are up to date, accurately completed and effectively managed.

3.22. Security related training should be evaluated by examining the training plans and course materials, observing the training and interviewing the personnel, to determine if the personnel are able to carry out the procedures or activities covered in the training programmes.

Interviews and knowledge testing

3.23. A prescriptive evaluation should include interviews of and discussions with the facility personnel to determine the extent of their knowledge about current facility policies, plans and procedures. Interviews regarding normal operating procedures as well as emergency operating procedures should be conducted. This evaluation process can aid in determining the effectiveness of the nuclear facility training programme. Reference [10] provides additional information on interview techniques and good practices for regulatory inspectors.

Reviews of specific PPS features

3.24. A prescriptive evaluation should ensure that the requirements (which can be either State requirements, or those contained in the approved security plan) for specific PPS features are met, such as prescribed fence heights, detection zone distances, wall and barrier thicknesses and door types. This should include a review of procurement data to certify that the barrier doors meet the design specifications and minimum delay values used in the effectiveness evaluation. Facility walk-downs should be conducted to ensure that physical protection measures on building elements (e.g. doors, windows, vents) are in place and performing as required. Walk-downs are an effective method to assess the facility conditions (e.g. access controls, guard duties, lighting conditions). Facility walk-downs should be used to provide an initial insight and impression of the nuclear security operations at the facility and to determine if a more detailed evaluation is needed.

Performance based approach evaluation

3.25. 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."

3.26. To determine if the physical protection measures are effective, analysis of the facility design by simulations and performance testing should be performed. Simulations and performance testing can validate the ability of a PPS to meet the performance requirements and may be needed where a prescribed measure is expected to meet a technical criterion or specification. Following initial modelling, the evaluation will produce a list of PPS components that may require more data to ensure effectiveness. Determining which PPS component to analyse or test can be based on the identification of the component as an important physical protection element, historic performance testing results, or it can be directed by the competent authority. In addition, specific areas can be tested more frequently based on lessons identified, results of previous analysis and testing, inspections, security incidents, or other information suggesting a potential weakness in the PPS.

3.27. The performance based approach evaluation may include the following:

(a) Conduct of modelling and simulations;
(b) Conducts of performance tests;
(c) Direct comparative reviews of other test data.

Conduct of simulations

3.28. Modelling and simulations can be used to evaluate the effectiveness of the PPS in meeting performance requirements. Modelling and simulation tools range from manual semi-quantitative tools that assess physical protection against predominantly prescriptive requirements to complex computerized tools for facilities that follow performance based requirements. Modelling and simulation tools can consist of simple path analysis, manual paper or tabletop models, 2D and 3D computer simulations, and virtual reality simulations. Simulations at existing facilities may be conducted in the following cases:

(a) To collect statistical data over multiple simulation runs in order to quantitatively evaluate the effectiveness of the PPS;
(b) To investigate PPS elements that are not practicable to assess through performance testing;
(c) When access to the operational environment of a nuclear facility is limited or restricted;
(d) When there are resource restrictions and/or safety concerns.

3.29. When a nuclear facility is still under design, direct performance testing of certain physical protection measures is not possible. In such cases, effectiveness evaluations may comprise modelling and simulations to determine the PPS effectiveness for detection, delay and response measures. Additional information on modelling and simulations can be found in Ref. [6].

Conduct of performance tests

3.30. Performance tests can include limited scope (e.g. testing a single PPS component) and full scope exercises (e.g. force-on-force exercises), and are designed to determine if the personnel, procedures and equipment are effective in protecting against malicious acts.

3.31. The performance based approach can be highly effective in determining the PPS effectiveness because it displays as close as possible to real situations actual actions and performance of equipment and personnel in different scenarios. However, conducting performance based evaluations requires detailed planning and extensive involvement of the personnel, presents scheduling challenges and can involve significant costs. See Section 4 for more detail.

Direct comparative reviews of other test data

3.32. When performance testing or modelling of specific physical protection measures is not possible, statistical test data for physical protection measures might be available through testing performed by national testing organizations, civil or military agencies or qualified vendors, national or international publications, or through testing of similar PPS measures (e.g. delay values of similar barriers).

3.33. Other sources of data could include the examination of test results collected as part of testing or validation activities of the facility's quality assurance programme, or through data from other sources, such as safety evaluations, safeguards validation or maintenance testing. When testing data for a specific physical protection measure are not available, expert judgment can be used to estimate the input for the effectiveness evaluation.

Combined approach evaluation

3.34. The combined approach includes elements from both the prescriptive and the performance based approaches. More information on the combined approach can be found in Ref. [2].

3.35. The combined approach evaluation allows for greater flexibility and uses the strengths of both the prescriptive and performance based approaches. The evaluation against prescriptive requirements should be performed before other performance based or combined evaluations can proceed. The rationale is that if, at a minimum, the prescriptive requirements are not met, any identified deficiencies should be corrected prior to performing more extensive performance based or combined evaluations to ensure reliable results.

IDENTIFYING AND MANAGING DEFICIENCIES

3.36. Using the prescriptive, performance based or combined approaches, potential deficiencies can be detected through modelling, simulation or testing. Once these deficiencies are identified, they should be promptly corrected, or compensatory measures implemented until corrective actions are completed. The impact and potential consequences of a failure should be the basis to determine the need for compensatory measures until the appropriate corrective action is taken. A graded approach may be applied based on the severity of the deficiency and to the urgency to complete the corrective action. Identified PPS deficiencies range from deficiencies with minor impact (i.e. procedures not being revised in the specified timeframe) to deficiencies with significant impact (i.e. physical protection measures are not functioning).

3.37. The PPS effectiveness can be affected by many factors, including equipment malfunction or failure, deficiencies in policies, procedures or training. The development of corrective actions for PPS deficiencies should include identification of their root causes. Corrective actions that address the root causes should prevent the reoccurrence of the deficiencies in the future. Examples of possible root causes of PPS deficiencies can be found in Annex II.

3.38. 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 re-assessment once the corrective actions are completed.

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

(a) Identifying the immediate causes associated with the deficiency;
(b) Identifying the root causes associated with the deficiency and ensuring that these are not just symptoms;
(c) Developing corrective action plans for the deficiencies by addressing the root causes;
(d) Prioritizing which deficiencies to correct, starting with the deficiencies with the highest impact, rather than correcting those identified most recently;
(e) Establishing a corrective action schedule with appropriate milestones;
(f) Assigning responsibility for completion of the corrective actions to specific organizations and individuals;
(g) Continually updating the plan if new milestones are needed to resolve the deficiency;
(h) Ensuring that adequate resources are applied to correcting the deficiencies in a timely manner;
(i) Maintaining a tracking system for the implementation of the corrective actions.

EVALUATING DESIGN OPTIONS AND THEIR EFFICIENCY

3.40. There are multiple reasons to evaluate design options including new facility design, changes to existing facilities, correction of identified deficiencies, or changes to the national 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.

Evaluating design options

3.41. 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 and simulations and/or analytical methods have to be used. There should be, however, no difference in the scope of the evaluation. The evaluation of proposed designs should address both prescriptive and performance based requirements, aiming at identifying advantages and limitations of the designs, and enabling a comparison between alternative solutions.

Evaluating the efficiency of PPS designs

3.42. The design of a PPS should factor in the long term sustainability of the PPS throughout its lifetime, including implementation costs, and maintenance and testing activities. The design should also incorporate efficiencies in maintenance and testing activities. For example, the placement of sensors, CCTV cameras and lighting should take into account the ease of access by facility maintenance personnel during routine testing, component failure, preventive maintenance or calibration activities.

EVALUATION OF THE PPS AGAINST BLENDED ATTACKS

3.43. A blended attack is a malicious act involving the coordinated use of both a cyber-attack and physical attack. For example, the PPS system or a sub-system is compromised by a cyber-attack as a precursor to a physical attack. In this case, the cyber-attack could occur immediately before the physical attack or could be carried out much earlier.

3.44. A comprehensive PPS effectiveness evaluation should include an analysis of a blended attack. 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 compromise of the computer network as part of an overt attack, a malicious act by an insider or other security events. Such evaluations could include simulations and performance testing to simulate, for example, an undetected compromise of alarm communications or CCTV signal in which false data are sent to the central alarm station. In such evaluations, the impact of the blended attack on the overall PPS effectiveness should be determined. If any deficiencies are identified, the operator should ensure physical protection measures and procedures are implemented to provide defence in depth. For more information, see IAEA Nuclear Security Series Nos 42-G, Computer Security for Nuclear Security [11] and 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities [12].

EVALUATION THROUGH MODELLING AND SIMULATION

3.45. The modelling and simulation methods used to assess the PPS effectiveness should be systematic, structured, comprehensive and appropriately transparent. Each type of evaluation method used has strengths and weaknesses; therefore, multiple evaluation methods should be used in a complementary fashion to take advantage of the strengths and offset the weaknesses of each individual method.

Path analysis

3.46. A path is a time ordered series of adversary tasks or actions along with some description of where those tasks/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 is detected early enough to interrupt them before an act of unauthorized removal or sabotage can be completed. This method should be used to identify the adversary paths having the lowest probability of interruption, which are the most vulnerable paths. The effectiveness of the PPS design in providing interruption is measured as the value of 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. Path analysis is useful primarily by providing insight into the performance of a PPS across many possible paths simultaneously but also serves to efficiently determine which paths have the lowest associated performance against the national threat statement. Annex IV provides a general overview of path analysis. Additional information for path analysis can be found in Ref. [6].

Neutralization analysis

3.47. Neutralization analysis is a method of determining the probability of neutralization, i.e. the probability that response forces can stop an adversary before a malicious act is accomplished, or to cause an adversary to abandon the attempt. Neutralization analyses should factor in legal and regulatory requirements as well as the effectiveness of response plans.

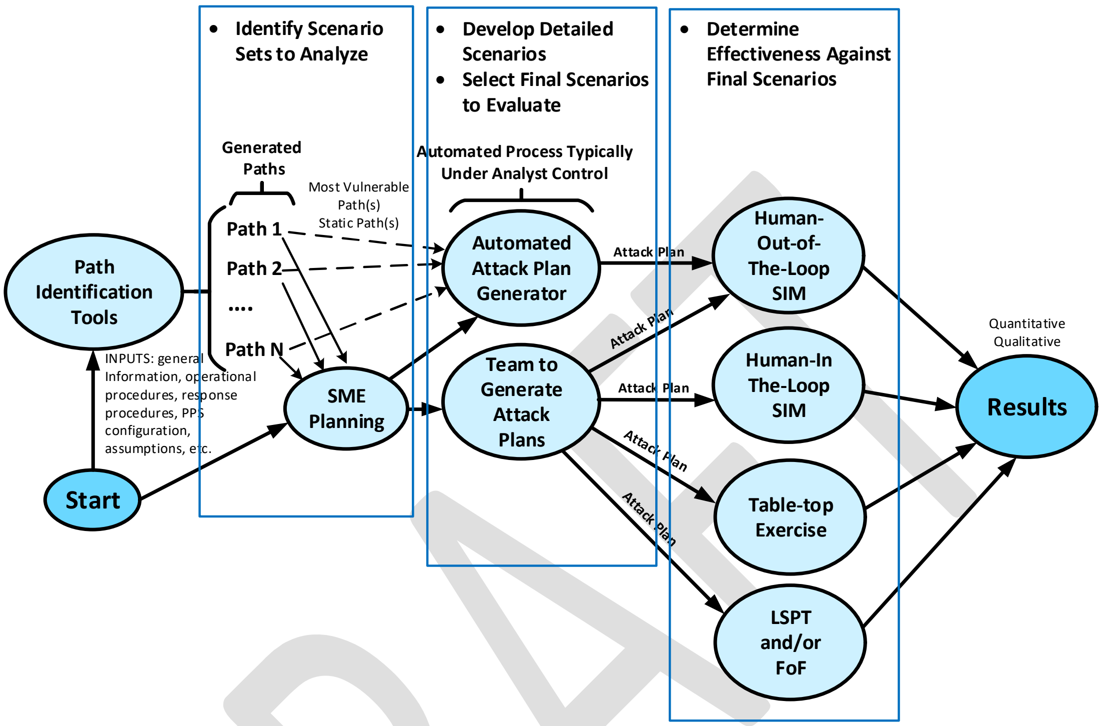
3.48. Several methods can be used to assist in the determination of the probability of neutralization. These methods range from qualitative methods, quantitative methods, tabletop methods, simulations, and limited and full scope performance tests. Each method has advantages and disadvantages, in terms of the time and cost of the analysis and its accuracy; therefore, multiple analytical methods should be used to determine the probability of neutralization.

Scenario analysis

3.49. Scenario analysis is an evaluation technique for the PPS effectiveness that is based on postulating adversary attack scenarios and determining the probability of PPS effectiveness directly without the need to calculate the probability of interruption in one tool and the probability of neutralization in another. The process involves identifying PPS components that might be susceptible to defeat and developing scenarios to exploit them. This includes defeat methods for sensors, barriers and communication systems, and possible diversion or elimination of portions of the response forces. This method can also be used to evaluate more advanced adversary tactics, such as diversionary attacks, split team attacks, and the potential role of insiders in collusion with an external adversary.

3.50. The scenario analysis process of the effectiveness evaluation may use modelling and simulation tools and other evaluation methods as reflected in Fig. 2. The analysis process begins at the Start Node. If the tool or method uses a path analysis approach, the node ‘path identification tools’ would be highlighted along with the paths Path 1, Path 2, …, Path N. The description of the path can then be used by a subject matter expert (SME) to develop an adversary attack plan or can be used internally to the software to identify an adversary attack plan automatically. Some tools do nothing more than generate paths.

3.51. SME developed attack plans can be used in human in the loop simulations, TT exercises, force-on-force (FoF) exercises or as part of limited scope performance tests (LSPTs).



(Courtesy of M. Snell, Sandia National Laboratories)

FIG. 2. How scenario analysis steps correspond to the process for using software tools and evaluation methods

Insider adversary analysis

3.52. One of the most difficult tasks for nuclear security is protecting a facility and its nuclear material from an insider intent on committing a malicious act. An insider is an individual with authorized access to the facility 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, associated facilities, or associated activities or other acts determined by the State to have adverse impact on nuclear security. Access, authorization, and knowledge provide the insider adversary with enhanced opportunity to commit a malicious act. Due to the complex nature of insider adversaries, the evaluation should include a combination of path analysis and scenario analysis. Annex V provides an example of an insider analysis method. This insider analysis method can also be applied to collusion of outsider and insider scenarios directly or in combination with other evaluation tools. For example, if an insider can divert nuclear material outside its authorized location, other analysis tools may be used to evaluate the outsider scenario from the new target location. Additional insider analysis information can be found in Annex V.

Nuclear material accounting and control analysis

3.53. An effective nuclear material accounting and control system is essential for ensuring the security of nuclear material, especially against an insider adversary intent on doing damage by misusing nuclear material. Reference [1] recommends that the facility operator manage the PPS and the nuclear material accounting and control system in such a manner that these are mutually supportive of one another.

3.54. Nuclear material accounting and control relies on the PPS to limit access to the nuclear material and protect it. Physical protection relies on the nuclear material accounting and control system for information about the nuclear material it is assigned to protect. Because the PPS relies on the nuclear material accounting and control system, analyzing the effectiveness of a facility's PPS should include evaluating elements of its nuclear material accounting and control system, especially where the nuclear material accounting and control measures and the PPS measures interface. Annex III provides examples of how elements of nuclear material accounting and control, including records, physical inventory taking, nuclear material measurements, nuclear material controls and nuclear material movements, interface with PPS elements and can be evaluated to determine the overall effectiveness for the protection of nuclear material and nuclear facilities.

EVALUATION THROUGH PERFORMANCE TESTING

3.55. During or following the initial modelling and simulation process, performance testing is conducted. Performance testing evaluates the performance of people, procedures, equipment, technology and hardware. Performance testing should be used to validate the ability of a PPS to meet the performance requirements and should be conducted as part of the evaluation process. 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 PPS effectiveness.

PPS performance requirements

3.56. Requirements should be established by the State for acceptable performance of the PPS against unauthorized removal or sabotage, based on the threats defined in the national threat statement. Performance requirements for unauthorized removal should be based on the highest category of the nuclear material protected by the PPS. Performance requirements for sabotage should be based on the State's established thresholds for unacceptable radiological consequences and high radiological consequences. Additional information on national threat statement found in reference [18].

Selection of PPS elements to test

3.57. The competent authority should define testing as a regulatory requirement. The requirement should prescribe a testing frequency for essential physical protection elements, or alternatively, require a documented and approved testing schedule.

3.58. Analysis of the PPS should also be used to identify which protection elements should be tested. This analysis should determine the testing priorities based on the significance of the physical protection measure and should consider elements that are deemed critical to the overall effectiveness of the PPS, as well as protection elements whose performance is uncertain.

3.59. The most essential elements for the operation of the PPS, such as sensors, locks, cameras and communications systems, should be considered when determining when and what is to be tested. In addition, consideration should be given to those elements that demonstrate failure rates most often. Decisive factors for selecting elements to test also include the skills needed by the personnel, such as the ability to operate the equipment, and comply with procedures and physical requirements If any changes (upgrades or modifications) are made to equipment and/or policies and procedures, those changes should be subject to testing to determine that they are effective as designed.

3.60. 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 elements of the facility's PPS. A graded approach should be used when a performance testing programme is established, so that testing of the PPS measures is proportional to the consequences of a malicious act.

Facility operations

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

3.62. Planning elements that should be considered include the type of nuclear material, its location and use, the radiation levels, the potential impact of testing on operations, any difficulties to access testing locations during operations, the proper coordination with and the necessary approvals by all facility organizations, the frequency of testing, and the types of PPS elements or procedures to be tested.

Determining PPS element testing schedule

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

(a) The regulatory requirements;

(b) The manufacturer’s recommendations;
(c) International and national standards;
(d) The facility specific conditions;
(e) The maintenance standards or strategies;
(f) The past performance of equipment or procedures, including any failures;
(g) The outcomes of any corrective actions;
(h) The past performance of the personnel in carrying out security functions;
(i) The facility procedures;
(j) Any changes in the national threat statement.

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

Lessons learned and operational experience

3.65. A process of continuous improvement should be adopted at the facility level whereby performance testing should be established based on lessons learned from the experience of previous tests and maintenance activities. Owing to operational and site specific conditions, PPS elements may have different maintenance and testing demands. When possible, the facility should engage with other nuclear facilities to exchange information on and experience from lessons learned through operational testing and maintenance.

3.66. Data from previous test results and operational experience could indicate the need to re-test physical protection measures on a more frequent basis. This is of particular importance for essential PPS measures and physical protection measures associated with critical detection points.

Security events

3.67. Data collected by the competent authority or the facility concerning previous security events or violations, as well as other malicious events relevant to nuclear security should be used, if available, in determining important elements for testing.

Other information

3.68. Information gathered from other States, including best practices, should be considered. Training exercises pertaining to nuclear and other radioactive material and results of such exercises should be taken into account in determining the path forward and enhancing the evaluation processes. Any intelligence on actual malicious events or potential planned events, including any resources being used for those events, should be used in determining evaluation objectives. Continuous monitoring of pertinent information that could assist in enhancing the PPS and the evaluation of the PPS should be considered.

Performance metrics

3.69. The PPS performance should be defined by measurable metrics such as detection probabilities, delay times and response times that collectively provide a level of confidence as to the overall effectiveness of the PPS. Requirements for the evaluation of metrics should be defined by the State; for example, evaluations could be based on specific standards (particularly in a prescriptive approach) or based on capabilities described in the national threat statement. In order to consider factors influencing overall effectiveness, performance testing should include all potential defeat methods and tactics as per the national threat statement, and to include different environmental conditions and different times of day and night. In addition, personnel to be tested should not have prior knowledge of a particular scenario. and if response forces are being evaluated, it should be comprised of the team of normal schedule of responders and not select personnel.

Detection probabilities

3.70. 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 a sensor's expected performance, it can be stated as a percentage, and it should be determined statistically through multiple tests. If a sensor has a probability of detection (P_D) of 90%, then the sensor will successfully detect an intrusion attempt at least 90% of the time. For more details on detection probabilities, see Section 4 and Ref. [6].

Delay times

3.71. The delay time is a key performance metric for physical barriers. Delay can be accomplished simply by increasing the distances and areas that have to be crossed and by introducing barriers, such as fences, gates, portals, doors, locks, cages and activated delay systems, that 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 so that the responders can interrupt and neutralize the adversary's attack before their objective 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."

3.72. The time needed to defeat a component using a specific tool set is referred to as the delay time. The delay time for a specific component should be tested by installing the component in a realistic setting and then determining 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 described in the national threat statement, and should be established or validated by the competent authority (particularly in a prescriptive approach).

Response times

3.73. Another key performance metric is the amount of time it takes for the response force to respond to different events. The response forces consist of persons on-site or off-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, communicate the assessment of the alarm to the response commander, dispatch the responders, and 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 national threat statement.

Neutralization of an adversary

3.74. The ability for the response forces to effectively neutralize an adversary attack can also be a key performance indicator. Factors to consider along with timeliness, are communications, command and control, equipment, training, and compliance with laws, policies and procedures. The response forces not only have to be in position in time to first interrupt the adversary but also need to have the sufficient number of personnel, avoid attrition (ambushes, snipers, etc.), have sufficient equipment as compared to the national threat statement, training to use that equipment effectively and effective policies and procedures to then neutralize the adversary.

Statistical confidence

3.75. Performance metrics can be determined statistically using the results of multiple tests, and statistical confidence is the likelihood that the derived performance metric is accurate. Examples of performance metrics include delay times for an intruder to defeat a barrier, times for responders to arrive, the probability that the operator at a central alarm station properly assesses an alarm and the probability that an alarm is triggered when someone enters the area that the alarm is monitoring. Where such data exists, classical statistical techniques can be used such as maximum likelihood estimations, confidence intervals and hypothesis tests.

3.76. Statistical confidence is determined by the number of tests conducted; i.e. the more tests conducted, the higher the confidence in the results. When a numerical performance metric is specified (e.g. probability of detection), it should be accompanied by a desired confidence level. For example, if a test plan involves a number of tests of a detection sensor in order to assure a minimum 85% probability of detection with a 95% confidence level, then the pass/fail criteria is that at least 85% of the tests are successfully detected, and the total number of tests is large enough to provide a 95% confidence that the detection probability is at least 85%.

3.77. A testing strategy should include selecting an acceptable and achievable confidence level. The higher the desired confidence level, the more testing and resources will be needed to arrive at statistical probabilities of detection which approach the measured detection rates. Statistical confidence level is described in more detail in the appendix.

Determination of defeat methods

3.78. Performance based evaluations should factor in the different methods an adversary might use to try to defeat the PPS. A library of defeat methods using different threat capabilities, including blended attacks, should be collected to assist in the timely and realistic assessment of the PPS. This should include a facility specific evaluation of how adversaries would likely attempt to defeat the PPS by attacking PPS computers and networks as a precursor to a physical attack. In addition, consideration should be made for potential vulnerabilities of the PPS elements, such as CCTV blind spots, sensor's detection dead zones, or communication dead zones. The determination of defeat methods should be a continuous process to account for changes in the national threat statement.

Other test considerations

Test plan development

3.79. Developing effective test plans not only ensures efficient use of resources, but also ensures that the test results provide useful and accurate results. See Section 4 for more detail.

3.80. Performance test plans should be designed to ensure the following:

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

3.81. See Section 4 for a detailed description of a test plan as well as Annex I for examples performance test plans.

Frequency of testing

3.82. The frequency of testing of specific PPS protection measures should depend on the overall importance of the measures for ensuring effective detection, delay and response. Other factors determining the frequency of testing should include the history of failure rates and the resource needs for large scale tests (e.g. force-on-force exercises). For additional detail concerning frequency of testing see Section 4.

3.83. In determining the specific testing to be done, the planning should take into consideration the following:

(a) How will the testing be conducted (e.g. type of test, specific techniques, test objectives, realistic conditions, available resources, appropriate device settings, types of data needed);
(b) Where will the testing be conducted (e.g. location of the test element, environmental factors to be tested against);
(c) When will the testing be conducted (e.g. time of day, time of year, weather conditions);
(d) How many tests will be conducted (e.g. availability of resources, precision needed in the results, number of unknown factors being tested);
(e) What is the type of data desired as a result of the testing.

Test criteria

3.84. Test criteria should specify the information to be gathered from the evaluation, and what performance metrics should be used. The test criteria should identify how the evaluation will be deemed successful or unsuccessful; for example, an evaluation of response times can be measured against the time specified in the security plan, and the result can be a simple 'Pass' or 'Fail' depending on if the responders get into position in the specified time or not.

Documenting test results

3.85. Test results should be documented to ensure an effective evaluation and performance testing programme. Proper documentation also allows for determining any corrective actions that might be necessary. Performance testing data should be maintained in a data library which can then be used as a basis to justify assumptions about probabilities of detection and assessment, and delay and response times used in physical protection evaluations. If this information is sensitive, it should be protected in a manner consistent with applicable regulatory requirements. Detailed information concerning documenting test results are provided in Section 4.

Integration of test data

3.86. Integration of test data is the process of collecting individual test results and characterizing a physical protection element or multiple physical protection elements working together. For example, to determine the total time for an adversary to breach a facility perimeter, several smaller individual tests may be necessary. In this case, the total perimeter delay time is determined by combining the individual test results for each specific adversary task.

Limited scope performance testing

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

3.88. Limited scope performance tests can be used to evaluate many PPS measures without disrupting facility operations or using extensive resources or numbers of personnel. Limited scope performance tests can provide an indication of a specific physical protection capability, while multiple tests for a series of actions can provide increased assurance of an overall capability.

Testing individual PPS measures

3.89. Limited scope testing of an individual physical protection element should be used to verify if a specific element is functioning as designed, or if a procedure is being performed correctly. The pass/fail criteria should be clear and direct. Limited scope tests can include the evaluation of the general knowledge of procedures or equipment operation by the personnel.

Benefits of testing individual PPS measures

3.90. The benefits of testing individual PPS measures include the following:

(a) Simple, direct pass/fail criteria;
(b) High reliability of test results;
(c) High repeatability of test results;
(d) Less impact on facility operations;
(e) Less planning and coordination needed than for more complex tests;
(f) Generally low overall cost to conduct.

Drawbacks of testing individual PPS measures

3.91. The drawbacks of testing individual PPS measures are the following:

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

Testing combinations of PPS measures

3.92. Limited scope testing of a combination of PPS measures should be used to determine if multiple interdependent physical protection measures are operating effectively. For example, the sensor meets the detection sensitivity criteria as defined in the requirements and the CAS operator accurately assesses the alarm and notifies the response.

Benefits of testing combinations of PPS measures

3.93. The benefits of testing combinations of PPS measures are:

(a) Ability to determine if the interdependencies and interfaces of the selected PPS measures are effective;
(b) Collection of more test data than individual element testing;
(c) Reliable test results;
(d) Repeatability of test data;
(e) Lower impact on facility operations than more complex testing;
(f) Smaller planning and coordination needs than for more complex testing;
(g) Lower overall cost to conduct than full scope testing.

Drawbacks of testing combinations of PPS measures

3.94. The drawbacks of testing combinations of PPS measures are the following:

(a) More complex planning is needed compared to individual element testing;
(b) More complex testing criteria and understanding of interdependencies and interfaces is necessary.

Full scope PPS performance testing

3.95. Full scope PPS performance testing (also described as 'whole system PPS performance testing') focuses on the evaluation of the overall performance of all the elements of the PPS system working together. Testing the whole system should ensure that individual components work together to provide an effective detection, delay, and response. The performance criteria should be evaluated for each essential physical protection element along the adversary pathway being tested, as well as how effectively the overall PPS performs. Depending on the testing criteria and facility limitations, some physical protection elements, such as detection and barrier delay can be simulated during the test, while other elements, such as traversal times, alarm assessment times, response times, interruption and neutralization, should be tested. Force-on-force exercises can be conducted as limited scope performance tests to evaluate a certain element or elements of the PPS. A force-on-force exercise may also be conducted as a full scope performance test to include all elements of the PPS.

3.96. The full scope PPS performance test is a large and complicated test, involving a large number of staff and multiple organizations, and planning for such a test can be complex. Some of the important topics to consider during planning are the following:

(a) Coordinating with the personnel and the organizations involved in or impacted by the test;
(b) Establishing clear test objectives;
(c) Selecting the attack scenario;
(d) Use of simulations;
(e) Defining the adversaries and their capabilities;

(f) Need for compensatory measures;
(g) Safety aspects and controls;
(h) Communications.

Planning and coordination

3.97. Planning and coordination are crucial for performance testing to ensure that the testing objectives are met, sufficient resources are allocated, and the tests are conducted safely. This includes the coordination with and approval from multiple stakeholders.

Establishing objectives

3.98. The objectives of performance testing should be clear and well established, should contain clear criteria for evaluation, and should be fully understood by all stakeholders. These objectives may include the following:

(a) Validation of the input data, assumptions, activities, results and conclusions of the vulnerability analysis;
(b) Demonstration of the protection capabilities;
(c) Ensuring that the performance of protection measures is effective.

Selection of attack scenario

3.99. Attack scenarios can be identified through various methods including modelling, simulations, and tabletop evaluations. When a range of scenarios has been developed, a scenario or scenarios should be selected for testing. Considerations for selection include identifying a 'worst case' scenario or bounding scenarios (scenarios that present more difficult tests for the PPS, and thereby can determine the effectiveness for less demanding scenarios), selecting a scenario to test a specific feature of the PPS, or testing a range of scenarios over time. Scenario selection should consider cyber-attacks on computer based systems that compromise their function. Whichever scenario is selected needs to be such that the testing objectives can be met.

Use of simulations

3.100. Various simulation techniques are available and can provide a useful tool for development and implementation of performance tests. These types of simulation provide useful insights into the effectiveness of the PPS, including contingency plans, command control and communication, and training levels of the response force. Computer simulations of many types have been developed to allow analyses that are similar in certain aspects to force-on-force tests. These simulations range from simulations with relatively low fidelity, simulating factors such as engagement, weapons effects, personnel movement, and two-dimensional terrain, to simulations with relatively high fidelity, with three-dimensional terrain, and algorithms that calculate the ability to see, hear, move, and engage opposing forces with various weapons systems. Despite their many limitations, simulations have the ability to gauge the performance of protection measures that are not well modelled by path analysis or other mathematical models.

Adversaries and their capabilities

3.101. Adversaries and their capabilities as described in the national threat statement are used as input to the effectiveness evaluation processes. Performance testing evaluates the PPS effectiveness against the threat described in the national threat statement to ensure effective physical protection of nuclear facilities.

Compensatory measures

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

Safety aspects and controls

3.103. Owing to the safety requirements necessary to operate a nuclear facility and the conduct of non-routine response force actions during a full scope performance test (e.g. force-on-force), it is necessary to establish safety controls during the test activities. These controls can include the determination of actual test activities versus simulated activities in the nuclear facility to ensure the safety of the facility and personnel. Additionally, to ensure that the tests are conducted safely, trained test controllers can be used (see also paras 4.45–4.47). The primary controller's functions are to ensure the safe conduct of the test and control the activities of the scenario. In addition to ensuring that the test is conducted safely, the controller may document observations for later analysis.

Communications

3.104. A communication plan should be developed that establishes how and when facility and/or site personnel and 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 what communications measures will be necessary to reduce those risks.

For example, if a full scale performance test (i.e. force-on-force) is to be conducted, then a communication plan should be implemented to reduce the potential for unintended real-world response by the facility and/or site personnel and the off-site personnel.

Benefits of full scope PPS performance testing

3.105. The benefits of conducting full scope PPS performance testing are as follows:

(a) Most PPS interdependencies and interfaces are tested;
(b) Equipment, procedures and personnel are tested at the same time.

Drawbacks of full scope PPS performance testing

3.106. The drawbacks of conducting full scope PPS performance testing are the following:

(a) They are resource intensive, both financially and in terms of personnel;
(b) They are time consuming to plan, conduct and evaluate;
(c) There is an increased potential for disruption of the operations at the facility;
(d) There is an increased potential for injury or radiation exposure of the personnel.

4. PERFORMANCE BASED EVALUATION FOR THE PHYSICAL PROTECTION SYSTEM

4.1. An organized evaluation programme should be established for verifying the effectiveness of the PPS. An evaluation programme should be established by the competent authority as a means of ensuring consistent and effective oversight of nuclear security. Additionally, an evaluation programme should be established by the operator that can provide an in depth, comprehensive look at the physical protection system This allows the evaluations conducted by the competent authority to focus more on validating the effectiveness of the operator's evaluation programme rather than conducting their own comprehensive evaluations. Utilizing an evaluation programme can enhance the validity of the State mandates and can help to identify if any upgrades or changes are needed to the physical protection system. A graded approach should be used when a performance testing programme is established, so that testing of the PPS measures is proportional to the consequences of a malicious act.

DEVELOPMENT OF A PERFORMANCE BASED EVALUATION PROGRAMME

4.2. Developing an evaluation programme considers detailed planning and execution of various programme elements in order to implement an effective programme. Programme planning elements may consider necessary testing to meet regulatory requirements, programme management systems, resource requirements to meet the requirements, funding, training and qualification of personnel, data management, communications with internal and external stakeholders, and issue resolution processes. The programme management system details the methods, processes and tools that should be used by the management of the nuclear facility to create a framework to carry out all work activities, including evaluations and performance testing in a safe and secure manner while ensuring that the objectives of the operator are achieved within the legal and regulatory framework of the State.

4.3. The evaluation programme for the PPS should be organized and conducted within an integrated management system that incorporates the management of all aspects of the nuclear facility into one comprehensive management system to address all the objectives of the facility operator, including safety, health, environmental, nuclear security, quality, economic and information management, and self-assessment. The coordination of programme planning elements described in the previous paragraph are performed within the facility integrated management system. The evaluation programme should cover all stages in the lifetime of the facility.

Coordination with other organizations

4.4. Due to the complexity of operations, the potential risks for the safety of the personnel, and the impact of security at nuclear facilities, effective coordination and integration with other facilities should be done when planning and conducting performance testing. For example, if the response forces intend to conduct a test in a material access area, coordination should be conducted with: the safety personnel so that compliance with the safety rules and policy is ensured; the operating personnel of the facility so that the impact to normal operations is minimal; and possibly the maintenance personnel in the case that equipment needs to be immediately repaired or restored during the conduct of the test. Planning and conducting performance tests should involve all the relevant stakeholders and organizations.

4.5. Depending on the scope of the performance testing, the number of entities involved may vary. Organizations and stakeholders to be considered should include the following:

- The competent authority;
- Different departments of the facility, such as facility security, operations, training, safety, response department;
- Law enforcement, security and military agencies, emergency and medical services.

4.6. Effective communication is essential during the planning and implementation of performance testing as part of an evaluation. Communication should not be limited to the personnel conducting the test, but also to other facility and/or site personnel who might be affected by the test. Off-site notifications may be necessary to ensure both test objectives and safety objectives are met. In the case of a security incident, several organizations should be involved to effectively respond and mitigate the incident. In order to have each of these organizations become familiar with each other's duties and responsibilities, the planning and conduct phase should include representatives from each organization. Regulatory oversight of the performance based evaluation programme by the competent authority is an effective approach to avoid potential conflicts of interest.

Programme planning

4.7. Programme planning is essential for the effective conduct of any evaluation process. The level of planning should be determined by the type and complexity of the evaluation programme. A graded approach should be applied based on risk management approaches previously described. Other aspects of graded approach for consideration include regulatory requirements, the number of protection elements to test, the frequency of testing, available resources, items to be protected, representative threat statement, etc. For example, a nuclear power plant with a limited access area(s), central alarm station(s), protected area(s) and multiple vital areas with hundreds of alarms will require a rigorous testing programme and large number of resources to implement, where a testing programme for a category III nuclear material storage area with a limited access area and fewer alarms will normally require much less testing and resources to meet regulatory requirements.

4.8. A nuclear facility should implement performance testing programmes that make use of ongoing testing conducted by the facility maintenance personnel in addition to dedicated PPS testing to make efficient use of available data.

4.9. Several considerations should be factored in to ensure that tests are meaningful, realistic and cost effective. Such considerations include the following:

- National laws and regulations;
- National threat statement;
- Results from effectiveness evaluations that identify critical systems
- Specific PPS components and subsystems to be tested;
- Objective of the test;
- Evaluation criteria, including specific, applicable pass/fail criteria;
- Personnel and equipment needed;
- Impact on the facility and/or site operations;
- Compensatory measures needed;
- Length of time needed to conduct the test;
- Lessons identified from previous tests;
- Costs to conduct the test;
- Specific and general safety considerations;
- Current facility and/or site plans and procedures;
- Current training of the personnel.

4.10. 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 can be formal and rigorous to ensure the inspection is conducted and completed within a strict timeframe.

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

4.12. 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 valid, testing by different experts using the same test plan should yield comparable results.

4.13. The evaluation plan should clearly specify the evaluation methodology, test objectives, roles and responsibilities, approval authorities and coordination processes with the facility personnel. It should also define how the evaluation will be carried out, the frequency and the evaluation criteria, the approach for implementing corrective actions and where appropriate integration with other organizations is necessary.

4.14. The evaluation plan should include evaluation and testing of all essential components and subsystems of the PPS. The effectiveness evaluation process identifies critical elements (components or subcomponents) of a PPS that directly affect the PPS effectiveness. Critical elements can consist of equipment, procedures or personnel.

Frequency of testing

4.15. As part of the programme planning for a performance testing, a testing schedule for physical protection measures should be established. The criteria for establishing the frequency of testing should factor in the following:

- The applicable manufacturer's recommendation, consensus standards, facility and/or site specific conditions and operational needs or other criteria that will ensure system effectiveness;
- The results of the effectiveness evaluation of the PPS;
- The category of the nuclear material;
- The facility protection strategy;
- Any changes in the facility and/or site operations;
- Any changes in the security mission at the facility and/or site;
- Any changes in the national threat statement;
- The degree of success observed in previous tests;
- The reliability of the equipment.

Statistical confidence

4.16. The evaluation plan should identify the desired level of statistical confidence to be achieved when determining performance metrics. This should include selecting an acceptable and achievable confidence level.

4.17. When a numerical performance metric is specified as a test criterion (e.g. probability of detection), it should be accompanied by a desired confidence level; for example, a test plan for a sensor could specify that the criteria for the sensor is to demonstrate a 90% probability of detection at a 85% confidence level.

4.18. The confidence level is the probability that the results from testing are correct, and the more trials (samples) that are conducted as part of the test, the more confidence we have in the results. If we conducted ten trials on a sensor and at least nine of them were successfully detected, we could say that the probability of detection is at least 90%; however, if we conducted 100 trials and at least 90 of them were successfully detected, we could say that the probability of detection is at least 90% with a much higher confidence level.

4.19. Table A.1 gives the number of trials required for three different probabilities of detection and three different confidence levels. This table is based on a pass/fail criterion of zero failures (misses).

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

Table A.1. Example trial sizes with zero failures

4.20. Using the example above, in order to demonstrate a 90% probability of detection at a 85% confidence level, 18 trials must be conducted without any failures. If there is one missed detection, then the sensor fails the test. Increasing the level of confidence requires increasing the number of trials. For example, demonstrating a 90% probability of detection with a 90% confidence level increases the number of trials to 22 without any failures.

Independent testing and reviews

4.21. The competent authority should consider using an independent party with appropriate expertise to conduct performance testing [2]. One example would be to perform delay tests of sample barriers, which might need the specialized skills of personnel trained in breaching techniques. Another example would be to use a team from the military or national police to act as the adversary in force-on-force performance tests; this could provide a better simulation of the knowledge and motivation of an external adversary, rather than using guards and responders that are assigned to the facility.

Interpreting and applying test data

4.22. In planning and conducting performance testing, the performance metrics and associated performance requirements should be established in the beginning and should be used in determining the specific data to be collected from the test. Performance tests can then be designed to capture the desired data in an efficient and effective manner. The methodology for interpreting and applying the data to the performance metrics should also be established, i.e. conducting statistical analyses or applying a basic pass/fail criterion.

Feedback and improvement

4.23. The evaluation programme should include a process for obtaining feedback from the performance testing activities. This feedback should include the following:

- Effectiveness of the test plan in addressing the test goals and objectives;
- Suggested adjustments to the testing schedule;
- Suggested improvements to the test plan;
- Safety concerns regarding the test;
- Security concerns regarding the test;
- Level of training needed for the test personnel in conducting specific tests.

4.24. This feedback should be used as a basis for adjusting and improving the evaluation programme on a periodic basis.

Performance testing conduct

4.25. The conduct of the performance test commences after the completion of the planning. The test should not begin until all pre-test activities noted in the test plan are complete and verified to be complete. This should include all necessary coordination activities and briefings, including safety briefings for the test participants.

4.26. The test should be conducted by qualified personnel that are sufficiently trained on how to conduct the test, and have sufficient knowledge of the test subject to understand the test results. The test should exactly follow the test plan to ensure the integrity of the results. If it is necessary to deviate from the test plan, the changes should be documented and factored into the analysis of the test results.

Briefings and meetings

4.27. Depending on the components, scope and scale of the tests to be conducted, the planning process should include pre-meetings and briefings to ensure that the purpose and objectives are pertinent and proportionate to the test to ensure coordination and approval by all relevant stakeholders.

4.28. Final approvals by all stakeholders should be obtained once the final test plan has been developed. These may include approvals by the following:

- Facility management;
- Facility security management;
- Facility safety representatives;
- Competent authority, as necessary

Safety aspects

4.29. During the conduct of performance tests, it is essential to ensure the safety of the personnel. The type of test and its scope can introduce a variety of non-routine safety risks. A thorough safety plan can assist in mitigating safety risks. The safety plan should describe all the resources involved in the test, including all equipment to be used, and it should include any necessary emergency medical procedures explaining the relevant arrangements and procedures for notifications, as needed.

4.30. All test participants, including personnel conducting the test, personnel being tested, and anyone observing the test, need to be adequately briefed on potential safety issues, including environmental concerns, radiation protection concerns, health concerns, concerns regarding the use of simulated weapons, rules of engagement, boundaries and out-of-play areas, and test procedures if a safety issue arises during the test. For unannounced, limited scope performance tests, strict controls should be implemented to avoid escalation of unplanned or unsafe actions outside the scope of the approved test plan.

4.31. When conducting effective evaluation tests, the overlap between conducting the test safely and at the same time maintaining the necessary level of security should be addressed. As part of the planning process, qualified personnel should be involved, including facility safety management and facility security management. The objectives of the test should be discussed to determine how they can be accomplished while protecting the participants and adequately securing the facility.

Performance test data management

4.32. Effective data management is essential for ensuring the integrity of any evaluation programme that includes performance testing.

Data collection

4.33. The test plan should specify what data to collect from the test. The personnel conducting the test should clearly record all data, including the name of the data recorder and the date on which the data were gathered. If data cannot be obtained for any reason, the circumstances should be recorded.

4.34. When testing response functions, information from the controller and/or evaluators is important. The collective observations from each controller and/or evaluator often is the most accurate information source for test results. Careful development of the evaluation forms is essential to recording this information. The topics of the evaluation forms should reflect the goals and objectives of the test.

4.35. If during the analysis deficiencies are identified in security equipment that might be outside the objectives of the original test, a determination should be made as to how significant the deficiency is to the security design and operation of the facility and if it is a maintenance or operator issue. Analysis of adequate compensatory measures should also be conducted.

Data integration with other testing

4.36. In many instances, the integration from multiple data sources or tests is necessary to determine if individual physical protection measures or the overall PPS are effective. Integration of test data with data from other sources should be used as input to increase the confidence that similar nuclear security element configurations will provide comparable detection, assessment and delay values for similar facilities.

Analysis and maintenance of data

4.37. Test results should be maintained for analysis and validation purposes of the PPS. Data management is necessary to collect, organize, analyse and retrieve data for historical and future validation activities of the PPS effectiveness. Data management can also be used as a basis to justify the probability of detection, assessment, delay times and response times used in modelling and simulation activities and in physical protection evaluations. Performance testing data should be maintained in a data library.

Confidentiality of results

4.38. During the management of the evaluation data, it is necessary to pay attention to protecting the confidentiality of the produced or recorded data, both in digital and hard copy format. The confidentiality of the results should be determined during the planning phase of the evaluation as the sensitive information has to be appropriately managed from the beginning. More information on sensitive information can be found in IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [13].

Periodic equipment and software testing

4.39. Specific testing of security equipment and software should be conducted periodically in accordance with national regulations and manufacturer's recommendations. Periodic equipment testing should also include testing of the equipment to identify potential computer security vulnerabilities. More information on periodic equipment testing is provided in IAEA Nuclear Security Series No. 40-T, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities [14].

Performance testing considerations

4.40. Performance testing considerations include testing approaches such as on-site testing (i.e. testing that uses the nuclear facility locations and equipment) and the use of off-site locations (e.g. dedicated test beds).

On-site testing

4.41. On-site testing involves close coordination with the facility management to minimize the disruption of operations at the facility. The testing can be conducted at a limited scale or in full scale, it can be conducted to demonstrate compliance with the regulatory requirements or it can be initiated by the management of the facility.

4.42. On-site testing provides the opportunity to evaluate the security design and procedures used to protect the actual equipment and facilities. It should be ensured that physical protection measures are operating as intended during testing and their operation should be closely coordinated with the site security personnel. If a deficiency is identified through testing or a physical protection element is defeated as part of a test (e.g. a fence is cut), corrective actions should be initiated as soon as testing is completed. If necessary, compensatory measures should remain in place until the corrective actions are completed.

4.43. Designing a test should include effective communications as an integral planning element. Pre-established communication procedures are necessary to ensure the effectiveness and efficiency of performance testing. The personnel involved in the test should be equipped with the appropriate knowledge and resources to ensure they are capable of performing their test tasks as needed. The personnel should have a clear understanding of the information that they are expected to communicate and when and how they are expected to communicate it. For example, if performance testing of an intrusion detection system is to be conducted, the personnel should know the established communication procedures to ensure the effectiveness of the test.

4.44. Communication should not be limited to personnel conducting the test, but also to other facility and/or site personnel who might be affected by the conduct of the test. Off-site notifications may be necessary to ensure that test objectives are met and the personnel is protected

Use of dedicated test beds

4.45. Performance testing on dedicated test beds located at the facility or at another testing location should be considered for testing the effectiveness of PPS components under a wide range of conditions and against a wide range of tactics. A dedicated test bed allows testing under realistic conditions without affecting facility operations or security. The test bed could include facilities to test the interior and exterior PPSs and the infrastructure to support sensor testing, data gathering and data recording. The test bed could include access control systems, delay systems, prohibited item detection sensors, lighting, assessment, and power distribution systems, as well as alarm communications, monitoring, and recording systems. It is important that computer security concerns be addressed for any equipment that is shared between the facility and the test bed.

DEVELOPING TEST PLANS

4.46. A test plan is a structured approach to the development and implementation of the performance test. Once the determination is made on the type of performance test to be conducted, the development of the test plan can commence. See FIG. 3 and FIG. 4 for an example of a sample test plan and subsequent description.

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	☐ Safety glasses
• Review the facility security plan	☐ Respirator
• Review any Effectiveness Evaluation documentation	☐ Confined Space
• Review Immediate Actions book in CAS/SAS	☐ Roof access
• Create test plan for area being tested	☐ Elbow pads
• Coordinate and schedule test	☐ Knee pads
• Notify PSS and Protective Force of test prior to start	☐ 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 performance 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.

I. TEST OBJECTIVES

1.
2.
3.

II. LOCATION(S) (to be tested)

Classification Level 1

4.47.

FIG. 3. Sample performance test plan format – page 1

I. **TEST SCENARIO (threat description and equipment, procedure, personnel being evaluated)**

II. **PHYSICAL PROTECTON MEASURES TO BE TESTED**

III. **TEST COMPENSATORY MEASURES**

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

IV. **TEST METHODOLOGY AND EVALUATION CRITERIA**

Planning

Test methodology and evaluation criteria

Procedure for testing

- Operability/Functional Testing
- Effectiveness Testing
- Scenario Testing

Testing 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 may 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 system*

- **Test Controls**
- **Resource Requirements:**
  - Facility
  - Personnel
  - Equipment
- **Test Controllers and Evaluators**

V. **TEST COORDINATION**

Identify coordination activities with operations and support elements (Operations, QA, Radiation Control, etc.)

VI. **OPERATIONAL IMPACTS**

Describe any operational impacts that may result during testing (Operations, Security, Overtime, etc.)

VII. **TESTING REFERENCES**

A. Facility Security Plan
B. Effectiveness Evaluation Special Requirements
C. Regulatory Requirements
D. Previous Test Reports

Classification Level 2

FIG. 4. Sample performance test plan format – page 2

Performance test goal

4.48. The goal of the test should state the desired outcome of the test and should describe the expected results. The goal also establishes the reasons why the test is being conducted. Some of these reasons can be the following:

- To satisfy regulatory requirements;
- To identify PPS deficiencies;
- To test and evaluate PPS components and subsystems and/or to evaluate the overall PPS effectiveness.
- Identify the training needs and areas that need improvements or upgrades.
- Validate the implementation of changes or upgrades.

Test preparation and safety equipment

4.49. A number of planning steps should be conducted during the preparation process. These steps include review of the facility security plan, facility procedures, protective force coordination, etc. Safety equipment requirements and safety reminders should also be identified during test planning.

Goals, objectives and performance standards of the test

4.50. An important part of developing test plans for performance testing is the development of clear goals, objectives and performance standards.

4.51. The goals should describe the expected result of the performance test and should identify the specific element to be tested. The objectives should include the specific tasks to be tested and observed in the performance test. The objectives should be based on performance standards by which the performance test will be evaluated.

Test location to be tested

4.52. All test locations to be tested should be clearly identified in the test plan to ensure effective coordination and facility approvals prior to testing.

Test scenario

4.53. Scenario development is the process used to outline the details of the test. It should include consideration of the measures designed to prevent and respond to malicious acts, including sabotage of the facility. The scenario should be credible, based on the capabilities and timelines of both the adversaries and the response forces.

4.54. 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 upon with relevant stakeholders to ensure that it meets the test objectives. Regardless of the type of test, the scenario should be designed taking into consideration the components and subsystems of the PPS, including the response forces.

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

- The current national threat statement;
- The defeat methods for different PPS elements involved in the test or exercise;
- The adversary capabilities in accordance with the applicable national threat statement.

Physical protection measures to be tested

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

- The element(s) that will be tested;
- The elements that will be excluded from the test;
- The location and time where the test will be conducted;
- The duration of the test.

Test compensatory measures

4.57. If any degradation of safety and security readiness is expected to be experienced 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 the major failure should be identified, and measures taken to prevent a future reoccurrence.

Test methodology and evaluation criteria

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

- Random sample selection of PPS elements to be tested, as appropriate
- A list of the steps for executing the test;
- The number of tests to be performed for each scenario, based on statistical confidence, as appropriate

- The criteria for assessing the test results (e.g. pass/fail criteria);
- A checklist for each objective tested;
- The methods for data analysis.

4.59. Test criteria should specify the information to be gathered from the evaluation, and what performance metrics should be used. The test criteria should identify how the evaluation will be deemed successful or unsuccessful.

Procedures for testing

4.60. During operability and functional testing, no attempt is made to defeat the PPS component or subsystem or to determine how well the component works, but only to confirm its operation. See REF NSS 40T for additional information.

4.61. Effectiveness testing is used to determine if the protection measure is operating as designed. This can include determining if it meets both technical and regulatory requirements. For example, does the sensor provide proper coverage of a specific location (door, window, storage location, room volume, etc.)

4.62. Scenario testing is the process of using the national threat statement criteria to identify and test PPS components that might be susceptible to defeat.

Test controls

4.63. Test controls are imposed to maintain the integrity of the test and minimize safety and security risks. They can apply to people, procedures and equipment.

4.64. Test controls should include limiting the number of personnel who have knowledge of the scenario to a need-to-know basis. Additional measures may include providing minimum notice in advance of tests, controlling lighting levels, or testing equipment under specific environmental conditions.

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

Resource requirements

4.66. In conducting performance tests of response measures, besides the personnel being evaluated, other personnel involved in planning, conducting and evaluating results are essential for the tests to be effective. The personnel involved include the following:

- Security management;
- Material control specialists;
- PPS equipment specialists;
- Management of the response forces;
- Safety management;
- Facility management;
- Crisis emergency manager;
- Analyst(s) responsible for conducting assessments of PPS effectiveness.

4.67. The test participants should be subject matter experts in their areas. The positions that they occupy qualify them to take part in the performance testing.

Controllers

4.68. Controllers should be used when conducting performance tests for the response measures, particularly if the performance test includes simulated engagements. It is the responsibility of the controllers to ensure that safety and security are maintained during performance tests. The controllers are also responsible for the introduction of simulations, communication injects and monitoring the general progression of the scenario.

4.69. At a minimum, all personnel should receive an orientation briefing and handout materials that cover the test plan including scenarios, objectives, procedures and rules. Additional training should be included for controllers in large scale tests. Training should emphasize the roles and responsibilities of the controllers and evaluators as well as functional interactions between them. Controllers need to understand and have training on how they are to interact with the personnel being tested, especially in large scale tests. Training on how to maintain exercise safety and security, and stay in line with the objectives without interfering in the integrity of the exercise is an important part of a successful test. Other considerations are training on how to start the test, deliver test inputs, what to do if the test goes off track, and how to end a test.

4.70. In a large-scale test, there should be a lead or senior controller, assistant controllers for the different elements being tested and a controller for the players acting as the adversary. The lead or senior controller should report to an exercise director. The exercise director is responsible for the approval of the exercise scenario and maintains overall accountability throughout the exercise. All controllers need to be fully informed of the test plan and the timing of the sequence of steps to make sure the test objectives are met.

Evaluators

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

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

4.73. Evaluators should be familiar with the following:

- Facility-specific security management measures and contingency response plans
- Purpose and objectives of the test
- The PPS Components being evaluated
- Scenario events and timelines
- Evaluator roles and responsibilities
- Evaluation techniques
- Procedures for monitoring and tracking player actions
- Procedures for recording player actions and feedback
- Procedures for reacting to player questions
- Procedures for communicating test problems or deviations

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

Test coordination

4.75. Testing coordination with all stakeholders involved in the planning, approval and conduct or the testing is essential to a successful, safe, and minimal operational impact for all stakeholders. The more complex the testing, the more coordination and planning is necessary.

Operational impacts

4.76. Any activity in a nuclear facility has the potential to impact ongoing operations Describe any operational impacts that may result during testing (Operations, Security, Overtime, etc.)

Testing references

4.77. Testing references are listed in order to determine a baseline for testing requirements and criteria. These references include security plan requirements, effectiveness evaluation performance-based requirements, regulatory basis, and potential identified weaknesses from previous test results.

APPENDIX A – PLANNING A PPS EFFECTIVESS EVALUATION

A.1. The PPS effectiveness evaluation methodology can be applied to evaluations of security measures against unauthorized removal and/or sabotage. The methodology is intended for use with fixed site facilities that handle, store, manage and/or transport nuclear and high activity radiological materials. This methodology can also be adapted for use at facilities where low activity radioactive materials and processes are used. Although not strictly part of the methodology, preparations for other considerations are also necessary to conduct a thorough effectiveness evaluation and testing.

DEFINING THE PURPOSE OF THE EFFECTIVENESS EVALUATION

A.2. The primary purpose of a security based effectiveness evaluation and testing is to determine if the applicable security requirements for the facility or activity are met. These requirements can be based on prescriptive requirements, performance requirements or a combination of both, as defined by the relevant competent authority or state body. In addition, the purpose of the assessment is to provide insight into the strengths and weaknesses of the PPS under evaluation. If effectiveness evaluations repeatedly and consistently reveal the same or similar weaknesses in a security system, the results could suggest that the problems are general and best addressed at a strategic or governance level. Where weaknesses are identified, appropriate remedial actions can be taken to rectify the issue. The facility can then be re-evaluated.

A.3. The license holder (operator/carrier) is responsible and accountable for the security of the facility and its materials. As such, an operator ensures that security measures, as well as being compliant with regulations, are genuinely appropriate and effective. Even if not a regulatory requirement, it is in the operator's interests to carry out periodic performance based effectiveness evaluations since these activities can provide continued protection measure(s) assurance and strengthen stakeholder confidence.

A.4. The competent authority may also wish to initiate effectiveness evaluations to ensure that the physical protection measures in place are effective. The purpose of these effectiveness evaluation is not to evaluate regulatory compliance, which are normally performed through periodic inspections. Both competent authority and the operator have a common interest in identifying which elements of the security system are effective; the operator is also interested in determining how efficient and cost effective these protection elements are.

A.5. It is important that the effectiveness evaluation address the targets that have the highest potential radiological consequences or are most vulnerable. It is important to clearly define the principle purpose of the assessment. For example, is the intention to evaluate the PPS that an adversary may have to overcome, or is it to evaluate just the response to the adversary actions? The purpose of the effectiveness evaluation will determine what the evaluators will assess and the methods that they will use.

IDENTIFICATION REQUIREMENTS FOR AN EFFECTIVENESS EVALUATION

A.6. There is extensive documentation on the need for, and methods of achieving, the security of NM and processes from outsider threats (see Table 1). Publications range from obligations included in International Conventions, to recommendations and guidance based on expert experience that may be available to any State organization. The regulations, policies, and guidelines applicable to a facility will determine the security objectives to be met and the type of effectiveness evaluation to be performed.

A.7. It is advisable the competent authority ensures that the current regulations in force in a State are appropriate and reflect both international standards and best practice. An effectiveness evaluation takes place within that regulatory framework and there is likely to be a significant amount of pre-existing information of direct relevance to the effectiveness evaluation. Nevertheless, it may be beneficial to draw on the wider range of publications detailed in TABLE 1 (e.g. whether an operator could use internationally accepted guidelines to support the interpretation of state level requirements). A regulator could benefit from the same material as a basis for testing the effectiveness of its regulation.

A.8. An effectiveness evaluation, whether initiated by the competent authority or by the operator, is likely to clarify the purpose of the effectiveness evaluation and the target(s) to be assessed. These decisions will determine the regulatory basis for the effectiveness evaluation and will direct the evaluation team towards:

- Appropriate security requirements and plans;
- Previous security inspection reports;
- Relevant safety and risk mitigation measures;
- Previous operator effectiveness evaluation and facility records.

A.9. This information will also direct the evaluation team towards any issues which need particular investigation or reinvestigation, and towards the sort of adversary scenario(s) that might be the most informative. This process could be iterative and the purpose and target(s) of the effectiveness evaluation may change as information is acquired and the methods and tools chosen are identified.

A.10. The type of information specific to the effectiveness evaluation being conducted may also draw on other State policies and regulations. Some examples of the information to be considered include, but are not limited to:

- Provisions to prevent proliferation;

- Nuclear security laws and regulations;
- National threat statement;
- Responsibilities and legal authority of respective competent authorities to fulfil their assigned roles;
- Nuclear security system requirements;
- Physical protection system requirements;
- Material accounting and control system requirements;
- Radiological/nuclear transport security requirements;
- Requirements for protection of the confidentiality of sensitive information and protecting sensitive information assets;
- Personnel trustworthiness requirements;
- Responsibilities of licensees and operators.

MANAGEMENT OF AN EFFECTIVENESS EVALUATION

A.11. An effectiveness evaluation, particularly if it includes a full scope performance test, can be a major and costly project with potentially significant consequences for the operator and the competent authority. The effectiveness evaluation should be approved and overseen by an appropriate level of management that is responsible for acting on the outcomes of the effectiveness evaluation.

A.12. An effectiveness evaluation requires the same degree of rigorous management and planning as any other comparable project. This section proposes a project management approach for major effectiveness evaluations. Smaller effectiveness evaluations can be given the same logical approach but may not need such formalized structures. A hierarchy of oversight and control is suggested; Fig. 3 depicts one way to view the organization associated with an effectiveness evaluation.

A.13. An effectiveness evaluation is performed by a team consisting of one or more levels of security management, possibly including the Facility Security Manager for major evaluations. This team may report to internal stakeholders (e.g. a board of directors or the facility manager), and may interact with external stakeholders (e.g. the competent authority or regulator). Specifically, it is suggested that an effectiveness evaluation involving performance testing at the facility be coordinated with the facility performance testing organization that has the responsibility and authority for performing these tests. It is the project manager's responsibility to ensure that the evaluation is performed safely and does not adversely affect facility or plant safety.

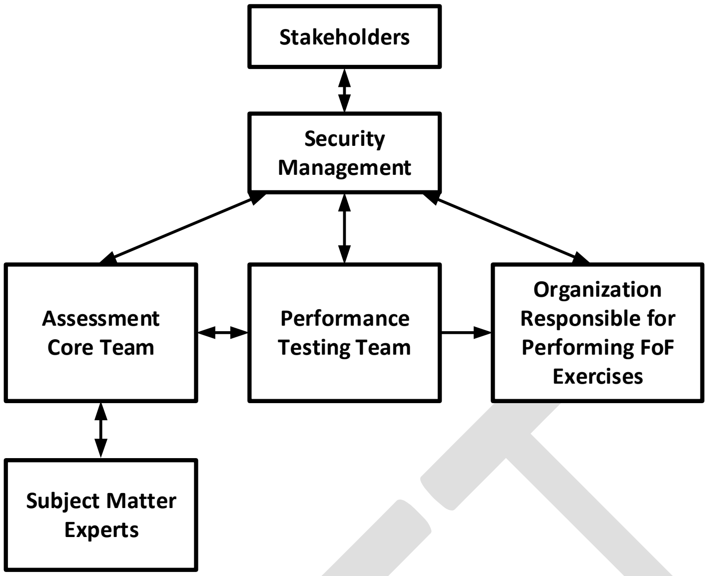


FIG. 3. Project control for security effectiveness evaluation

A.14. It is not reasonable to expect all evaluation team members involved in an effectiveness evaluation to have complete knowledge of all relevant requirements. Therefore, a core team will typically perform the evaluation. This core team will have access to one or more subject matter experts (SMEs) either in relevant nuclear security domains or in supporting areas such as intelligence or facility safety. In a performance based assessment, the core team will interact with a performance testing group responsible for planning, conducting and documenting appropriate limited scope performance test (LSPTs) to collect information such as task times and detection probabilities. If necessary, the assessment may require a FoF exercise, which is typically performed by a specialized group due to the cost and complexity of such exercises.

A.15. Clarifying roles is an essential element of an effectiveness evaluation because individuals may be exercising different levels of authority from those they exercise in normal circumstances.

A.16. It is suggested that the size and composition of the core team be commensurate with the facility size, complexity of the system(s) being assessed, and the areas to be addressed (such as nuclear material accounting and control, computer security, etc.).

A.17. Table 4 lists some examples of roles and expertise that core effectiveness evaluation team members and supporting SMEs may possess.

TABLE 4. EXAMPLE ROLES AND EXPERTISE FOR CORE EFFECTIVENESS EVALUATION TEAM MEMBERS

Core Team Members	Subject Matter Experts

Team leader (physical protection specialist)	Locksmith
Site/facility liaison member	Nuclear material accounting and control
Security system engineer	Assessment software specialist
Assessment analyst	Threat specialist
Operations representative	Safety representative
Response expert	Site/region security officer
Access delay/explosives expert	Security technicians
Alarm communication and display engineer	Security force personnel
	Construction/structural engineer
	Information technology administrators

Planning documents

A.18. To support the effectiveness evaluation, a number of planning documents and presentations may be developed:

(a) An approved work agreement describing the goal(s) of the effectiveness evaluation, an evaluation security plan, the scope of the system(s) to be assessed, project management structure, the schedule, budget and resources required;

(b) An initial briefing to effectiveness evaluation participants describing the information in the work agreement as well as a briefing by evaluation team leadership about assumptions used for the nuclear security systems being evaluated;

(c) An effectiveness evaluation participant guide which provides guidance, processes and procedures for performing all phases of the evaluation.

Effectiveness evaluation security plan

A.19. The existing security plan for the facility or activity is to be evaluated to determine if it gives sufficient support for the purpose of planned evaluation activities or if additional elements are necessary. The plan to protect sensitive and confidential information in compliance with security regulations and standards is an important element. Information security is also necessary to prevent unauthorized personnel from knowledge of no notice performance tests and exercises in order to reduce the likelihood of an adversary using the test as an opportunity to conceal or enhance a malicious activity. Further, whenever these tests and exercises are being executed at the facility, they are by nature, an attempt to overcome a facility's security system. However, the facility security effectiveness would need to be effectively maintained throughout the process. This will usually mean using supplementary measures. In particular, special attention needs to be paid to maintaining an effective security response capability and to ensuring that effective security is in place at all times during the effectiveness evaluation.

Defining the effectiveness evaluation

A.20. An effectiveness evaluation may be an evaluation of the security of an entire facility. However, an evaluation carried out in certain parts of a facility might be too operationally disruptive or too hazardous. In the interests of efficiency, economy and safety, it is advisable to precisely define the specific boundaries of the effectiveness evaluation.

A.21. The boundaries of the effectiveness evaluation need not correspond to a specific locale but could be a discrete part of the security system (e.g. personnel screening and access control). In such a case, it is imperative to decide the limits of the evaluation. For example, it could include 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 the effectiveness up to a particular vital area, the boundary of the evaluation will stop at the vital area perimeter. However, decisions may also be necessary as to whether to include parts of distributed systems, such as alarm or access control systems, that are actually located within that vital area.

Resources

A.22. An effective evaluation will demand funding, time and expertise. For the period while the effectiveness evaluation is taking place, it could have an impact on the normal activities of a facility. It is beyond the scope of this methodology to go into further detail, but managers may allocate resources and make provision for any disruptions caused by the effectiveness evaluation.

Effectiveness evaluation team guides

A.23. The effectiveness evaluation team develops a specific guide which can cover details such as:

(a) Skills, knowledge and attributes of the team members needed for the effectiveness evaluation team and how they will be selected. The size and composition of the team is dependent on the size and scope of the evaluation;

(b) Description of the processes and timeframes for acquiring sensitive site information and gaining access to the site;

(c) Gathering essential information data for the evaluation;

(d) Effectiveness evaluation team management structure.

Effectiveness evaluation team management structure

A.24. It is advisable that an effectiveness evaluation manager be assigned with the responsibility and authority to perform the evaluation. Given that most evaluations will take place at a facility, the assessment team will also require someone to coordinate with site management. It is the team manager's responsibility to ensure that the evaluation activities are coordinated with the site in order to ensure safety is maintained at all times.

A.25. The planning of the effectiveness evaluation will determine how unplanned external inputs are handled. For example, it may 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 of it, or by a real event outside the exercise.

Effectiveness evaluation documentation

A.26. An effectiveness evaluation is a complex, iterative and detailed process involving many areas of a facility and involving many people and decisions. It is highly suggested to document all of these factors as well as the uncertainties and assumptions taken into account during scenario development

Effectiveness evaluation training

A.27. It is advisable that the evaluation team involved in planning and performing an effectiveness evaluation be trained on how to conduct the evaluation according to the documents pertinent to the specific evaluation and facility. Training is also needed for others involved in the evaluation, such as the SMEs and stakeholders, so that they understand the purpose of the evaluation and their roles in it. It is important for all to understand that a performance based evaluation depends upon their cooperation and openness to uncovering and discussing strengths and potential vulnerabilities of the PPS 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)

[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, IAEA, Vienna (2016).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA-TECDOC-1868, IAEA, Vienna (2019).

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

[8] 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).

[9] 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).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook for Regulatory Inspections of Nuclear Power Plants, IAEA-TECDOC-1867, IAEA, Vienna (2019).

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

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[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, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

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

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standard Series No. GSR Part 7, IAEA, Vienna (2015).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear or Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

ANNEX I – PERFORMANCE TEST SAMPLE PLANS

I–1. Performance test plans include all elements of the test to be performed so that any stakeholder can review the plan and have a clear understanding of what, how, and where the test is to be conducted. The structure of the performance test plan indicates all resources to be used and criteria for how the test is to be analysed. This annex provides examples of plans for different elements of the physical protection system (PPS). These examples are not inclusive of the tests that can be performed.

INTRUSION DETECTION AND ASSESSMENT SYSTEMS

Interior motion sensor defeat test

I–2. Defeat tests for interior motion sensors, such as microwave sensors and passive infrared sensors, are conducted using a combination of walk tests and crawl tests. A defeat 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 performance test plan is presented in Table I-1.

TABLE I–1 PERFORMANCE TEST PLAN FOR INTERIOR MOTION SENSORS

Performance test goal

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

Objectives

This performance test will determine the effectiveness of interior motion sensor coverage. The adversary tactics (modes of attack) that will be used in the performance test include both walk and crawl tests.

Location

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

Physical protection measures to be tested

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

Test Compensatory Measures

A guard will be positioned outside the testing location door to perform visual alarm detection and assessment during the testing. The guard should maintain communications with the central alarm station during the testing and report any malicious action to the central alarm station. The guard will remain in place until all testing is completed and the PPS is placed back in normal operation.

Scenario description

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

Test methodology and evaluation criteria

A total of 6 walk tests and crawl tests will be performed. The tests will include the simulation of an adversary path from the nuclear material storage room door to the nuclear material storage rack, where the adversary will touch the nuclear material rack without being detected. The exact pathway will be predetermined prior to testing from the point of the storage room door entry to the nuclear material storage rack.

Evaluation criteria

The motion sensors will be considered to have passed the test if the simulated adversary is detected by at least two sensors prior to reaching the nuclear material items on the storage rack during both the walk and crawl tests.

Procedure

The following steps will be followed for the conduct of the test:

(1) The test subject is positioned at a point within 0.3 m of the entry. The test subject limits movements for at least 20 seconds before walking.

(2) Any observers will remain outside the storage room door (or in the central alarm station) so that they do not affect the test results.

(3) Using the paths drawn on Figure I–1, the test subject walks at a speed of approximately 0.3 m/sec from the entry toward 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 Worksheet I-1, the test observers mark the sensor(s) that alarmed.

(5) Using the same path, the test subject crawls at a speed of approximately 0.3 m/sec from the entry toward 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 Worksheet I-1, the test observers mark the sensor(s) that alarmed.

(7) Repeat Step 1 through Step 6 for each path indicated on the figure.

(8) Record the total number of alarms on Worksheet 1.

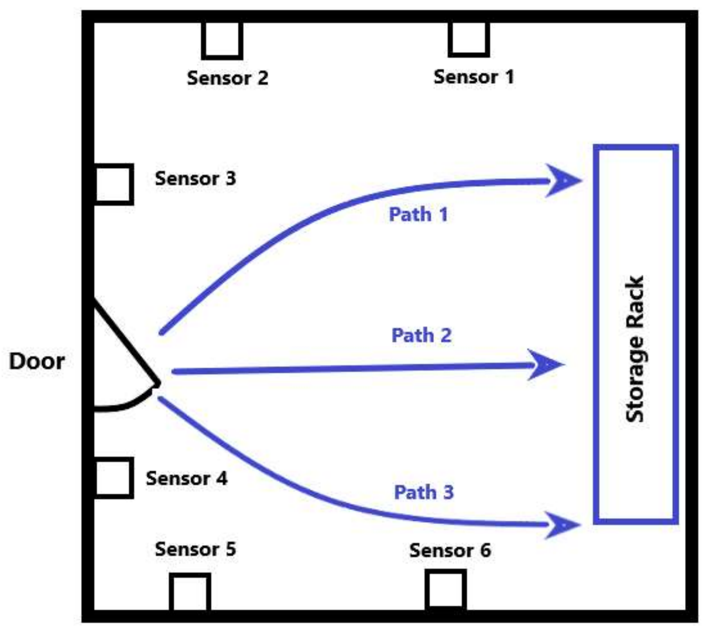


Figure I–1. Layout of the nuclear material storage room.

Worksheet: test results

Number of Tests	Motion Sensor Alarm (yes/no)						Total 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 _________							

Exterior bistatic microwave sensor performance test

I–3. 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 crawler, such as a metal sphere. An example performance test plan is presented in Table I-2.

TABLE I–2 EXAMPLE OF A PERFORMANCE TEST PLAN FOR EXTERIOR MICROWAVE SENSORS

Performance test goal

This performance test is designed to determine the probability of detection (P_D) for an exterior sensor (bistatic microwave) as part of a perimeter intrusion detection and assessment system.

Objectives

This performance test will determine the probability of detection for an exterior bistatic microwave sensor. The performance test will utilize a metal sphere to simulate a crawling intruder.

Location

The location of the performance test will be in the perimeter intrusion detection and assessment system.

Elements to be tested

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

Test compensatory measures

Position a guard in view of the testing location to perform visual alarm detection and assessment during the testing. The guard should maintain communications with the central alarm station during the testing and report any malicious action to the central alarm station. The guard will remain in place until all testing is completed and the PPS is placed back in normal operation.

Scenario description

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

Test methodology and evaluation criteria

Testing will be conducted in accordance with the procedure described below. The test will include the simulation of a crawling adversary by moving a metal sphere across the detection zone.

Equipment

The following equipment will be used for the conduct of the test:

- One hollow aluminium sphere, 30 cm in diameter, with a cord attached that is long enough to reach across the detection zone.

Evaluation criteria

The sensor will be considered to have passed if the probability of detection is determined to be 88% or greater with an 85% confidence level.

Procedure

The following steps have to be followed to use the aluminium sphere (ball) to simulate a stomach crawl:

(1) Record starting position (e.g. at crossover point near transmitter) and distance from centre line.
(2) Set the ball out of the detection zone, approximately 4.5 m from the centre line.
(3) Position one tester each on either side of the centre line.

(4) The tester on the left begins pulling the ball at a rate of 0.3 m/sec. The ball will be pulled across the field-of-view of the microwave sensor from outside to inside.

(5) Verify if an alarm occurs.

(6) Document results in Worksheet 1-1.

(7) Repeat Steps 1 through 6 from the other side of the centre line.

(8) Repeat Steps 1 through 7 for the remaining tests.

(9) When all tests are completed, fill in the information below to determine the probability of detection.

Total detected alarms for all test locations = __________ out of ___________tests.

Number of failures = _______________

Probability of detection (P_D) = ________________ with a confidence level = 85%.

Record if the element met or failed to meet the goal.

Goal probability of detection (P_D) = ***88 %, with a confidence level of 85%.***

Test failed or met the performance level? ________________

Exterior camera performance test

I–4. Exterior cameras are often installed in combination with perimeter sensors as a means of assessment. Table I-3 provides an example test plan for performance testing an exterior camera installed on a perimeter.

TABLE I–3 EXAMPLE OF A PERFORMANCE TEST PLAN FOR AN EXTERIOR CAMERA

Performance test goal

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

Objectives

This performance test will determine the capability of an alarm assessment system to cover an entire assessment zone on the central alarm station video monitor. This performance test will determine the alarm assessment system effectiveness for the (1) near field-of-view and (2) far-field resolution of an assessment zone. The test will be conducted during daylight hours.

Location

The location for the performance test will be within the perimeter detection zone of the facility.

Element(s) to be tested

The physical protection measures to be tested are the alarm assessment system of the protected area of the facility, and the alarm communication and display system of the central alarm station.

Test Compensatory Measures

Position a guard in view of the testing location to perform visual alarm detection and assessment during the testing. The guard should maintain communications with the central alarm station during the testing and report any malicious action to the central alarm station. The guard will remain in place until all testing is completed and the PPS is placed back in normal operation.

Scenario description

The performance of the alarm assessment system of the protected area will be tested to determine the ability of the system to display an entire assessment zone on the central alarm station video monitor and whether the alarm assessment system can provide the three levels of assessment resolution (assessment, classification, and identification). The results of the test will determine 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 will be conducted in the assessment zone of the protected area during normal operations.

Test methodology and evaluation criteria

The test will determine if the video assessment system meets the requirement of viewing the entire alarm assessment zone and whether the alarm assessment system has sufficient resolution to classify an object in the detection zone.

Two teams are needed for the conduct of the test: the field team on the perimeter and the monitor observation team in the central alarm station. The field team will consist of a team leader to direct the test, one person responsible for communicating to the central alarm station by radio, 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).

Equipment

The following equipment will be used for the conduct of the test:

- Handheld radios;
- 30-cm triangle, circle, and square geometric shapes (white on one side, black on the other).

Evaluation criteria

The camera is able to cover the entire assessment zone, including near and far fields of view and both the inner and outer fence lines, and has sufficient far-field resolution to classify a 30-cm target at the far field (far end of sector).

Procedure

The following steps will be followed for the conduct of the test:

(1) The monitoring observation team will verify 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. I-3). The monitoring observation team of the central alarm station will record the assessment view results.

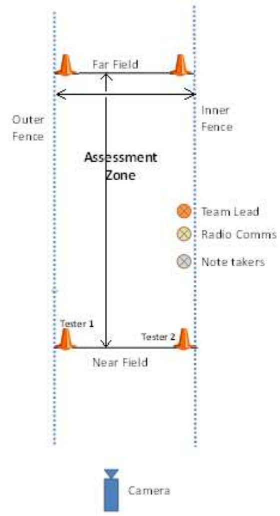


Figure I–2. Test configurations for CCTV

(2) The field team will take the triangle, circle, and square shapes to the end of each sector (see Fig. I–4). The purpose is to check the capability of each camera to resolve a 30 cm target at the far end of the assessment sector. The field team will verify with the monitoring observation team the identification of the shapes and the results recorded.

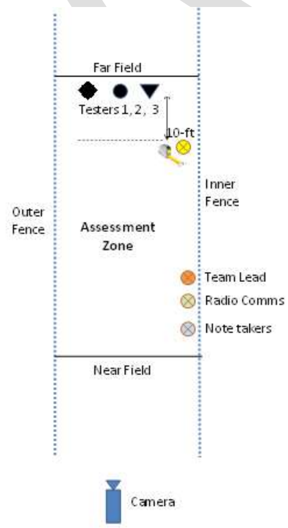


Figure I–3. Test configurations for CCTV

(3) With the black side of the three geometric shapes facing the camera the field team holds the shapes in front of and above their heads or on the perimeter ground surface. The shapes can be oriented in any order and varied, such as upside-down triangle and rotating square 45 degrees to make a diamond. Targets and order are switched around for each test. When in position, the field team will communicate using the radio with the monitor observation team

to record the order of the geometric shapes viewed on the monitor and the results. If the observed order was correct, the performance criterion has been met.

(4) If for any reason, the performance criterion is not met, the assessment system will be adjusted and retested.

Hand geometry unit

I–5. Hand geometry units are a form of biometric access control that verify an enrolled person's identity by measuring the dimensions of their hand. Table I-4 provides an example test plan for performance testing a hand geometry unit.

TABLE I–4 EXAMPLE OF A PERFORMANCE TEST PLAN FOR A HAND GEOMETRY UNIT

Performance test goal

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

Objectives

This performance test will determine if 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 will attempt to gain access using the hand geometry unit.

Location

The location of the performance test will be at the nuclear material storage room door of the facility.

Elements to be tested

The specific element to be tested is the hand geometry unit through assessing the following:

(a) Access control measures for individuals with authorized access, including the use of a personal identification number (PIN);
(b) Biometric data base of persons with authorized access;
(c) Ability of the hand geometry unit to control access.

Test Compensatory Measures

Position a guard at the door being tested to perform the manual access control function for access into the building and to conduct visual alarm detection and assessment during the testing. The guard should maintain communications with the central alarm station during the testing and report any access control malicious actions to the central alarm station. The guard will remain in place until all testing is completed and the hand geometry is placed back in normal operation.

Scenario description

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

Test methodology and evaluation criteria

Evaluation criteria

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

Procedure

One person with authorized access will test the hand geometry unit to ensure proper operation. Once it has been stablished that the hand geometry unit operates as designed, the person with authorized access will input their PIN and a second person will place their hand on the hand geometry unit in an attempt to gain unauthorized access. A total of 15 runs per test will be performed and recorded. If any of the 15 attempts results in a simulated unauthorized access, the system fails the test.

Search procedure using a handheld radiation detector

I–6. Handheld radiation detectors can be used to search personnel, packages, and vehicles for hidden nuclear or other radioactive material; however, their effectiveness is significantly impacted by the search procedures and skills of the person conducting the search. Table I-5 provides an example test plan for conducting a limited scope performance test of the procedure for conducting a search using a handheld radiation detector.

TABLE I–5 EXAMPLE OF 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 objective of this performance test is to evaluate a guard's ability to effectively search for and detect a radioactive source at the exit of the facility.

Location

The location for the performance test will be at the access control point at the exit of the facility.

Elements to be tested

The protection measure to be tested is the capability of the guard at the access control point to follow the approved search procedure and detect nuclear material using a handheld radiation detector.

Test Compensatory Measures

Position a second guard at the testing location to perform the routine access control search function while the testing is performed. The guard should maintain communications with the central alarm station during the testing and report any access control malicious actions to the central alarm station. The guard will remain in place until all testing is completed a 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 used. The guard at the access control point uses an approved procedure for searching with a handheld radiation detector to detect nuclear material that might have been removed. The purpose of the procedure is to detect an insider attempting to steal nuclear material. The guard's ability to follow the approved procedure will be tested using a test source simulating nuclear material. The test will occur during normal operating hours.

Test methodology and evaluation criteria

Evaluation criteria

The criteria for evaluation are:

1. The guard correctly follows the approved procedure for conducting the search;
2. The guard is able to locate and identify the test source.

Equipment

The following equipment will be used for the conduct of the test:

- Test source used for testing and calibrating the handheld radiation detector.

Test controls

The guard's supervisor and the person responsible for evaluating the test (evaluator) will be present to observe the guard and ensure the safety of all participants. The guard's supervisor will intercede when the test source is detected and stop the guard from taking further action.

Procedure

A test source simulating nuclear material will be hidden on a trusted person's body as that person exits the building through the access control point. The guard supervisor and the evaluator will position themselves to observe the search.

The test will be concluded when either the guard locates the test source or the search is concluded without locating the source. The evaluator will then question the guard on what actions should be taken if radioactive material were found on the person.

The following questions will be used for evaluating the search process:

(a) Did the guard ensure the handheld detector was operating properly?

(b) Did the guard follow the approved procedure for 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?

(c) Did the guard understand their responsibility to detain the person if radioactive material was discovered, and notify the appropriate organization identified in the approved search procedure?

Metal portal detector

I–7. Metal portal detectors are used to detect the introduction of prohibited metal items or removal of nuclear material using shielding, as appropriate. Table I-6 provides an example test plan for performance testing a metal portal detector.

TABLE I–6 EXAMPLE OF A PERFORMANCE TEST PLAN FOR A METAL PORTAL DETECTOR

Performance test goal

This performance test is designed to determine if the facility metal portal detector meets the State requirements for the prevention of the introduction of prohibited metal items or removal of nuclear material using shielding, as appropriate.

Objectives

This performance test will determine if the probability of detection for prohibited items such as weapons and radiation shielding meets the State's recommended threshold.

Location

The location for the performance test will be at the access control point of the facility.

Element(s) to be tested

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

Test Compensatory Measures

Position a second guard at the testing location to perform personnel metal detection searches using a handheld metal detector while the testing is performed. The guard should maintain communications with the central alarm station during the testing and report any access control malicious actions to the central alarm station. The guard will remain in place until all testing is completed and the metal portal detector is placed back in normal operation.

Scenario description

The adversary tactic will be to attempt to carry prohibited metal items into or out of the facility. The metal portal detector will be tested to detect an attempt by a person to introduce prohibited items such as a weapon or removal of nuclear material using shielding.

The test standard approved by the facility (i.e. simulated weapon and/or shielding item) will be used. The performance of the detector will be tested against the national threat statement. The test will be performed at the access control point of the facility during normal operating hours.

Test methodology and evaluation criteria

Evaluation criteria

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

Equipment

The following equipment will be used for the conduct of the test:

- Metal test source for weapons;
- Metal test source for shielding.

Procedure

The test standard will be carried through the metal portal detector at the head, waist, and ankle levels at slow, moderate, and fast speed for a total of 15 passes and each result will be recorded in the worksheet below. The test results will be reported for each test standard, as necessary.

Worksheet: Test description and test results for the detection of a prohibited item

Test Number	Prohibited Item	Test Location (head, waist, ankle, other)	Test Speed (fast, slow, moderate)	Number of Trials	Number of Detections	Number 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			

Test Number	Prohibited Item	Test Location (head, waist, ankle, other)	Test Speed (fast, slow, moderate)	Number of Trials	Number of Detections	Number of Failures
12	Metal object	ankle	Moderate			
13	Metal object	head	Moderate			
14	Metal object	waist	Fast			
15	Metal object	ankle	Fast			
Total						

Total detected alarms for all tests = _______________ out of ___________tests

Probability of detection (P_D) = ________________, with confidence level = 85%

Goal probability of detection (P_D) = *88 %, with a confidence level of 85%.*

Test failed or met the performance level? ________________

ACCESS DELAY BARRIERS, LOCKS, AND KEYS

Fence delay

I–8. Fences are commonly used as barriers around security areas. Understanding how much delay time the fence provides against different penetration methods is important for security planning. Table I-7 provides an example performance test plan for obtaining fence delay times.

TABLE I–7 EXAMPLE OF A PERFORMANCE TEST PLAN FOR FENCE DELAY

Performance test goal

This performance test is designed to determine the effectiveness of the barrier delay values of the facility fence using different barrier breaching techniques.

Objectives

This performance test will determine and document the delay time for each defeat technique using the adversary tools established in the national threat statement. It will also determine if the barrier delay times are consistent with the effectiveness evaluation values documented in the approved Facility "V" security plan.

Location

Due to the destructive nature of this testing, a mock-up of the fence barrier of the facility fencing will be used to test different defeat techniques.

Elements to be tested

The elements to be tested are:

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

Test Compensatory Measures

A compensatory measure is not required for this mock-up test.

Scenario description

Two adversaries will use hand wire cutters, mechanical saws and grinders to breach the fence at Sector A of the nuclear material storage area activating the fence alarm. The alarm will be received by the central alarm station, will be assessed using CCTV and response will be dispatched per the facility security plan. The adversaries will not proceed past the cut fence and upon termination of the test, they will remain in place.

Test methodology

Equipment

The following equipment will be used for the conduct of the test:

- A mockup of the fence with at least three panels for testing;
- Handheld wire cutters;
- Battery powered saw with metal cutting blade;
- Battery powered grinder with metal cutting blade.

Procedure

A security supervisor will use a stopwatch to document the amount of time it takes for two adversaries to cut a hole through the welded wire fence large enough for one person to get through using first manual wire cutters. The adversaries will then use a battery powered saw with a metal blade to cut the same size breach. The adversaries will then use a battery powered hand grinder using a metal cut off blade to again cut the same size breach.

A second security supervisor will be in the central alarm station and will document the amount of time it takes for the alarm to be received and the response to be initiated.

The times will be evaluated to determine that they allow for responders to get in position per security plan.

Three different tests will be conducted using three different breaching tools in three different sections of the fence.

COMMUNICATION SYSTEMS

I–9. Communication is an important element of response in a PPS. Table I-8 provides an example performance test plan for communication.

TABLE I–8 EXAMPLE OF A PERFORMANCE TEST PLAN FOR A COMMUNICATION SYSTEM

Performance test goal

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

Objectives

This test will ensure the effectiveness of:

(a) The central alarm station to notify 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 communication equipment and usage per the approved facility security plan, procedures and training;

(d) The radio equipment in accordance with its design.

Location

The central alarm station of the facility will be used for the performance test.

Elements to be tested

The elements to be tested are:

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

(b) Equipment: The ability of radios to transmit and receive 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.

Test Compensatory Measures

Communication testing can occur as part of routine guard duties. The central alarm station and guard testing communications should ensure that testing is being conducted with clear testing protocol announcements prior to and following the conduct of a test.

Scenario description

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

Test methodology and evaluation criteria

Procedure

The central alarm system operator will be notified that the test has started, and will be instructed that a fence sensor has been activated at a specific location on the perimeter.

The central alarm system operator will announce the test on the radio, and then proceed to communicate with the response forces as described in the approved facility security plan and procedures.

Once these communications have taken place, the response forces will move to the sensor location, assess the alarm and communicate to the central alarm station by radio of any unauthorized activities.

A total of 10 test iterations will be conducted to allow multiple response personnel to participate.

Evaluation criteria

A pass/fail criterion will be used along with an established checklist. A test will be 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 will be evaluated for effective performance and potential dead spots.

Performance Test Controls

No simulated adversaries will be utilized during the test(s). Pretest notification will be announced. Weapons will remain in "safety-on" configuration throughout the test. The response management will assign performance test controllers and evaluators.

SUPPORT SYSTEMS

Power and backup systems

I–10. The power system for a 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. Table I-9 provides an example performance test plan for backup power.

TABLE I–9 EXAMPLE OF A PERFORMANCE TEST PLAN FOR BACKUP POWER

Performance test goal

This performance test is designed to determine if the facility uninterruptable power supply is designed, is maintained and functions as designed to support the PPS.

Objectives

This performance test will determine if the facility back-up 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 location for the performance test will be the back-up power supply and central alarm station of the facility.

Element(s) to be tested

The PPS support systems to be tested are the back-up power supply of the facility, the PPS batteries. The loss of primary electrical power alarm function(s) at the central alarm station alarm communication and display system will also be tested.

Test Compensatory Measures

The operator, the central alarm station and guard force will be 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 and guard force will provide authorization to the testing organization that testing can proceed.

Failure of backup power equipment during the conduct of this test could result in temporary loss of power to the PPS. Compensatory measures may include stationing guards on the facility perimeter and building locations prior to testing. The guards should maintain communications with the central alarm station during the testing and report any malicious actions to the central alarm station. The guards will remain in place until all testing is completed and the PPS power is placed back in normal operation.

Scenario description

The adversary tactic will be to attempt to defeat the PPS primary power supply of the facility in order to increase the probability of achieving a malicious act of unauthorized removal of nuclear material or sabotage.

Test methodology and evaluation criteria

Evaluation criteria

The test result will be considered as 'PASS' if all the following are successfully completed:

(a) Following the loss of power, the back-up power supply automatically begins operation;
(b) 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 alarm station indicates a loss of primary power in accordance with the State requirements;
(d) The alarm and communication and display functions remain operational as required by the State.

Procedure

Performance test personnel will be located in the central alarm station and at the back-up power unit to evaluate the loss of power functions of the alarm communication and display system. The PPS maintenance personnel of the facility will simulate a loss of PPS primary power supply at the back-up power supply unit, and the performance test personnel will observe the operation of the system.

Note: The State may not have a requirement for all PPS measures to operate continuously during the change over to the back-up power supply (i.e. advances in CCTV contrast during low light conditions might be sufficient to provide temporary assessment during the lighting restart period at the protected area perimeter).

Tamper and line supervision

I–11. Tamper sensors installed in hardware and line supervision incorporated into communication lines are designed to detect attempts to access and compromise the PPS. Table I-10 provides an example performance test plan for tamper and line supervision.

TABLE I–10 EXAMPLE PERFORMANCE TEST PLAN OF TAMPER AND LINE SUPERVISION

Performance test goal

This performance test is designed to determine if the facility PPS alarm lines are protected against tampering and defeat by an adversary.

Objectives

This performance test will test PPS alarm junction boxes for tamper switch operation and annunciation and will determine if the PPS alarm supervision is sufficient to meet the State's requirements.

Location

The location for the performance test will be facility PPS alarm junction boxes and the central alarm station.

Element(s) to be tested

The PPS support systems to be tested are the Facility PPS alarm line junction boxes and power supplies and alarm function(s) at the alarm communication and display system of the central alarm station alarm.

Test Compensatory Measures

Position a guard in view of the testing location to perform visual alarm detection and assessment during the testing. The guard should maintain communications with the central alarm station during the testing and report any malicious action to the central alarm station. A second knowledgeable maintenance person will participate in the testing to maintain a two-person rule and report any malicious actions. The guard will remain in place until all testing is completed and the PPS is placed back in normal operation.

Scenario description

The adversary tactic will be to attempt to defeat the facility PPS alarms by accessing alarm and CCTV junction boxes for interruption and signal substitution to increase the probability of achieving a malicious act of unauthorized removal of nuclear material or sabotage.

Test methodology and evaluation criteria

Procedure

The performance test personnel will randomly select a predefined number of alarms and junction boxes to test. The performance test personnel will be located in the central alarm station to evaluate the alarm communication and display system for loss of signal/alarm supervision and tamper alarm annunciation.

The PPS maintenance personnel of the facility will access selected PPS junction boxes to determine if a tamper switch alarm is operational and if an alarm is received in the alarm communication and display system of the central alarm station. The PPS maintenance personnel will also interrupt the alarm and/or CCTV signals to determine if a line supervision alarm and loss of signal alarms is received in the central alarm station.

Evaluation criteria

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

Emergency evacuation procedures

I–12. Emergency evacuations present significant challenges to nuclear security; in order to get personnel out of the building quickly, the normal PPS measures have to be bypassed. This presents opportunities for an insider to exploit an evacuation to remove material from a facility. Table I-11 provides an example performance test plan for evaluating the effectiveness of security measures during an emergency evacuation.

TABLE I–11 EXAMPLE OF A PERFORMANCE TEST PLAN FOR EMERGENCY EVACUATION

Performance test goal

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

Objectives

This test will evaluate the response to an emergency evacuation of the facility to ensure that control of personnel is maintained following a planned or unplanned evacuation until appropriate monitoring of personnel can be completed to ensure that a malicious act has not occurred. The test will be performed during normal working daytime hours.

Location

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

Element(s) to be tested

The specific elements to be tested are the following:

(a) The compliance of the guards with the evacuation procedure(s):
   (i) To control personnel during an emergency evacuation and channel them to the monitoring location, and the ability to prevent personnel from leaving the protected area of the facility;
   (ii) To search evacuated personnel using a portable radiation detector at the monitoring location, in accordance with the procedure to sweep the area after an evacuation, and to detect concealed simulated nuclear material.

Test Compensatory Measures

The operator, the central alarm station and guard force will be 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 and guard force will provide authorization to the testing organization that testing can proceed.

Compensatory measures may include stationing guards on the facility perimeter access control points and building emergency exit locations prior to testing. The guards should maintain communications with the central alarm station during the testing and report any malicious actions (not included in the test plan) to the central alarm station. The guards will remain in place until all testing is completed and the PPS is placed back in normal operation.

Scenario description

The adversary tactic will be to exploit an insider during an emergency evacuation to achieve unauthorized removal of nuclear material from the facility, while the insider conceals the material outside the facility for later retrieval. This limited scope performance test will focus on the following elements:

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

Test methodology and evaluation criteria

Pre-test activities

The following activities should be conducted before the test:

(1) Simulated nuclear material will be placed outside the facility between the emergency exit and the monitoring location.
(2) All nuclear material in the facility will be securely stored.
(3) As a compensatory measure, a guard and radiation protection personnel located outside the emergency exit will monitor personnel exiting the facility for unauthorized removal of nuclear material during the test.
(4) A trusted agent will be located in the facility.

Procedure

The following steps will be followed for the conduct of the test:

(1) At the start of the test, a controller will announce the beginning of a fire evacuation test and instruct the personnel to follow the procedure for a fire alarm.

  (i) Personnel exiting the emergency evacuation door will be forced to stop and be monitored by the guard and radiation protection personnel prior to traversing to the emergency evacuation monitoring location.

  (ii) Personnel exiting through the access control point of the facility will follow the approved search and monitoring procedures prior to traversing to the emergency evacuation monitoring location.

(2) A trusted agent will attempt 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 will do as instructed and proceed to the emergency evacuation monitoring location.

  (ii) If not challenged, they will process through the access control point but not leave the building of the access control point.

(3) The controller will end the test when all personnel at the monitoring point are monitored and the path along the evacuation route has been searched for concealed simulated nuclear material, or when it is determined that the test has been concluded.

Evaluation criteria

The test result will be 'PASS' if all the following are successfully completed:

(1) The guards or facility personnel prevent the trusted agent from exiting the protected area boundary of the facility and redirect the agent to the emergency evacuation monitoring location.

(2) All personnel at the monitoring location have been monitored for unauthorized removal of nuclear material.

(3) Areas outside the building have been systematically and effectively searched, and the concealed simulated nuclear material has been detected.

Optional criteria:

- *Use of access control records 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.*
- *Determine that the protected area ACP is restricted for entry/exit until the conclusion of the evacuation test.*

NUCLEAR MATERIAL ACCOUNTING AND CONTROLS

Nuclear material accounting

I–13. An accurate nuclear material accounting database combined with effective controls and periodic inventories provides delayed detection of unauthorized removal of nuclear material. Table I-12 provides an example performance test plan for evaluating the effectiveness of nuclear material accounting and control.

TABLE I–12 EXAMPLE OF A PERFORMANCE TEST PLAN FOR NUCLEAR MATERIAL ACCOUNTING AND CONTROL

Performance test goal

The performance test will assess the accuracy of the nuclear material accounting database.

Objectives

The performance test will check the accuracy of the nuclear material accounting database by verifying the nuclear material locations, the tamper-indicating device (TID) numbers, and the gross weights.

Location

The performance test will be within the confines of the storage room or processing area of the facility.

Element(s) to be tested

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

Test compensatory Measures

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

Scenario description

This performance test will verify the accuracy of the nuclear material accounting and control records and will confirm the likelihood of detecting the unauthorized removal of nuclear material (for abrupt or protracted theft strategies) between physical inventory takings.

Test methodology and evaluation criteria

Evaluation criteria

The test result will be 'PASS' if there are no discrepancies identified between the database and actual conditions

Procedure

The following steps will be followed for the conduct of the test:

(1) The controller will obtain the book inventory report for the nuclear material accounting and control records for the storage room that includes the recorded location, tamper-indicating device number (if applicable), and the container and content gross weight for each item.

(2) The controller will randomly select a specific number of items for verification. The locations, tamper-indicating numbers and gross weights of these items will be noted.

(3) The performance testing personnel (tester and verifier) with the assistance of facility personnel will 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 numbers and the gross weights agree with each item's recorded data. If a selected item is in the process and unavailable for inventory taking due to an authorized activity, then an additional item will be selected from the inventory list.

(4) The performance testing personnel will note all discrepancies and defects, which will be investigated at the conclusion of the test.

(5) While in the area, the inspector may randomly select a specific number of additional items that are physically present in the MBA and record each item's location, tamper-indicating device numbers and gross weight.

(6) The performance testing personnel will 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 will be noted and investigated at the conclusion of the test.

NOTE: An advanced performance test for nuclear material accounting and control may include a trusted agent who would move a preselected item to another location in the storage room prior to the conduct of the performance test. This approach will need additional management, coordination and approvals.

RESPONSE

Response time

I–14. Response is a key element of the PPS, and response time is an important performance metric for evaluating the effectiveness of the PPS. Table I-13 provides an example performance test plan for response time.

TABLE I–13 EXAMPLE OF A PERFORMANCE TEST PLAN FOR THE FACILITY RESPONSE

Performance test goal

This performance test is designed to test and evaluate the facility response time to the nuclear material storage room.

Objectives

The performance test will assess:

(a) The ability of the central alarm station to effectively direct the response in accordance with the facility procedures.

(b) The time 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 will be conducted at the nuclear material storage room of the facility.

Elements to be tested

The specific elements to be tested are the following:

(a) The ability of the central alarm station to disseminate the response to the alarm location.

(b) Whether the responders were properly armed and equipped to respond.

(c) Whether the responders can get into position in accordance with the times included in the facility response plan.

Test Compensatory Measures

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

Facility response testing can occur as part of routine guard duties and the test should follow approved response plans and procedures. Operator, central alarm station, and guard testing communications should ensure that testing is being conducted with clear testing protocol announcemenmts prior to and following the conduct of a test.

Scenario description

The scenario to be tested is a response to alarms at the nuclear material store room. Based on 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 will be accomplished for each responder if they respond with all issued equipment and get into effective and appropriate response position in a timely manner as per the security plan.

Test controls

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

Pre-test activities

Evaluators will be located at the designated response locations. The evaluators will be equipped with stop watches and checklists listing the weapons and equipment the responders are expected to bring.

Procedure

The following steps will be followed for the conduct of the test:

(1) To begin the test, the central alarm station operator will be notified that the test has been initiated. The central alarm station will be instructed to complete the following actions:
   a. Announce that there are alarms at the nuclear material storage room locations of the facility, and include the statement that it is a test;
   b. Advise the appropriate personnel as prescribed in the facility security plan.

(2) Response personnel will respond to the alarm location in accordance with the approved contingency plan.

(3) A total of 10 tests will be conducted to allow multiple response personnel to participate.

(4) A Pass/Fail criterion will be used along with a checklist. A Pass score will be accomplished for each responder if they respond with all issued equipment and get into effective and appropriate containment position in a timely manner as per the security plan.

(5) The operator of the central alarm station will obtain a Pass score if all appropriate personnel are notified and dispatched in a timely manner using the prescribed radio procedures.

ANNEX II – EXAMPLES OF ROOT CAUSES FOR DEFICIENCIES OF THE PHYSICAL PROTECTION SYSTEM

II–1. The PPS effectiveness can be affected by many factors, including equipment malfunction or failure, 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. Once protection deficiencies are identified, then corrective actions are implemented. The development of corrective actions for deficiencies of the PPS includes identification of their root causes. Corrective actions that address the root causes will help prevent the reoccurrence of these deficiencies in the future. This annex provides examples of root causes that can lead to deficiencies in a PPS.

FALSE AND NUISANCE ALARMS

II–2. Intrusion detection systems are subject to false and nuisance alarms. The nuisance alarm rate is the number of alarms generated over a period of time by occurrences not associated with the intrusion by an adversary. These occurrences might include environmental factors, such as wind, rain or wildlife, authorized personnel inadvertently causing alarms, or might result from poor system installation or design. Nuisance alarms generated by the equipment itself are described as false alarms (e.g. alarms caused by poor design or component failure) and are not addressed further in this annex. Controlling and maintaining the environment around the sensor can help to minimize nuisance alarms and therefore contribute to the overall effectiveness of the PPS (see Ref. [II–1] for more detailed information on false and nuisance alarms).

IMPROPER INSTALLATION, CALIBRATION OR ALIGNMENT OF PPS COMPONENTS

II–3. Periodic maintenance and calibration testing are useful to determine whether the PPS components and subsystems are correctly installed, aligned, and calibrated. Improper installation, calibration, or alignment of sensors might significantly reduce sensitivity and contribute to false alarms, and might not be effective in the case of a malicious action. More detailed information on PPS installation, calibration, and alignment can be found in Ref. [II–1].

INADEQUATE TESTING AND MAINTENANCE PROGRAMME

II–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 and radiation). Periodic preventive maintenance of the physical protection network will increase PPS availability and extend its operational life. PPS network maintenance and testing activities have to comply with computer security requirements.

II–5. PPS network maintenance can be preventive (scheduled) or emergency (unscheduled or associated with an outage or deviation of system components from their specifications). Periodic maintenance and operability tests can help to monitor performance and ensure continued operability, reliability, availability, and effectiveness of the network to collect and communicate the data from automated physical protection subsystems. See Ref. [II–1] for additional information.

PHYSICAL AND ENVIRONMENTAL CONDITIONS

II–6. Physical and environmental conditions at the facility can affect the performance of physical protection assessment measures. These conditions include camera selection, camera placement, topography, vegetation, and lighting conditions. Failure to accurately assess a sensor alarm limits the ability of the command and control function to direct the response. Additionally, a high rate of nuisance and false alarms might degrade the operator attention and the response to actual malicious acts and alarms. Failing to accurately assess an alarm can reduce the PPS effectiveness.

UNRELIABLE POWER SOURCES

II–7. The purpose of the electrical power system is to provide a reliable power source for physical protection systems and subsystems during normal operation and emergency conditions. Redundancy can prevent individual component failures from leading to 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 that reduce the effectiveness of the PPS.

REFERENCE TO ANNEX II[II–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 III –EVALUATION METHODS FOR NUCLEAR MATERIAL ACCOUNTING AND CONTROL

III–1. This Annex addresses how nuclear material accounting and control elements, including records, physical inventory taking, measurements, and controls, interface with elements of physical protection and can be evaluated to determine the overall effectiveness for the protection of nuclear material and nuclear facilities.

RECORDS

III–2. An effective records system for nuclear material accounting and control provides accurate and complete records that are essential for resolving irregularities involving nuclear material. The records include information about the identity, quantity, type, form 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 evaluation purposes, nuclear material accounting and control records are relied upon for validating late detection of diversion or theft of nuclear material. The reliance upon nuclear material accounting and control records during evaluations of scenarios for the insider threat involving the protracted theft of small quantities of nuclear material over several inventory periods might result in late detection through the comparison of nuclear material type, form, quantities and locations.

In the case of missing nuclear material, whether stolen, lost, diverted, or misused, the nuclear material accounting and control records provide evidence of the nuclear material that is supposed to be in the facility and records can be used to determine what is missing. The inventory list is essential for resolving questions about missing or diverted nuclear material.

PHYSICAL INVENTORY TAKING

III–3. Physical inventory taking confirms the presence of nuclear material and the accuracy of the accounting records, or book inventory. It provides evidence that the facility nuclear material accounting and control system is effective. The frequency of the physical inventory taking depends on the quantities and category of the nuclear material. Conditions and methods for physical inventory taking are described in Ref. [III–1]. All nuclear material has to be measured at the time of the physical inventory taking, or there needs to exist a prior measurement whose integrity has been assured by a tamper indicating device and has been subject to an effective material surveillance programme. Physical inventory taking is an element for consideration during the evaluation and performance testing processes. For evaluation purposes, the frequency of inventory taking can be used to limit the period of insider activity for theft of diversion. For example, if the insider theft strategy is to remove multiple small quantities of nuclear material that is lower than the detection limit radiation detection portal, the number of trips between scheduled inventory periods versus the amount of each attempt is an indication of the PPS effectiveness. If 5 Kgs of U-235 is the target quantity and the inventory period is every two months (60 days) and the facility is operated five days a week, the insider needs to successfully remove 125 grams 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 taking periods and the sensitivity limit of the radiation detection portal to detect lower quantities of nuclear material. This example only outlines the interface between these measures. Other interfaces are presented in paras III–10 to III–15.

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

III–5. A physical inventory taking conducted as part of the evaluation of the nuclear security system may involve 100% of the facility's nuclear material or part of it, depending on the extent of the performance test.

MEASUREMENTS OF NUCLEAR MATERIAL

III–6. The measurements of nuclear material are an important element of the nuclear material accounting and control system. Knowledge of the quantities of the nuclear material helps to deter and detect unauthorized removal. If a container of nuclear material is missing, an investigation and search is conducted. In the case that the missing container is located, a measurement has to be conducted to ensure the appropriate type and quantity of nuclear material is still present in the container. This assumes 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 making it possible to decide whether "found" nuclear material is the same nuclear material that was lost, accurate and precise measurements help to 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 by measurements.

III–7. Measurements can be an effective protection element against the insider threat that needs to be considered during the evaluation and performance testing processes. For evaluation purposes, the frequency of measurement, the location in the process where the measurement is taken, and the accuracy of the measurement are important evaluation considerations. Other interface protection measures for nuclear material accounting and control and physical protection that are applicable during measurements may include detection of unauthorized activity by other personnel (i.e. two-person rule), monitoring of the process using a camera, protection of the measurement equipment and data, and the response to a failed measurement.

III–8. In the example outlined in para. III–4, the theft strategy followed by the insider includes a material acquisition step that is either a single action or multiple actions to obtain the target quantity for theft or diversion. The facility processes and implemented protection measures will determine the nuclear material accounting and control and PPS interface for analysis. One example may include the process to divide and repackage a larger quantity item of nuclear material into smaller containers. Typically, measurements of nuclear material are conducted during this process to establish and maintain accurate records. Depending on the initial state of the material (i.e. powder or pellets), the beginning value will agree with the total of the smaller final values (assuming minimal process loss) within a defined limit of error. The insider strategy considers the measurement protection measures during the nuclear material acquisition step as well as other interface protection measures. These measures are effective in limiting the amount of nuclear material that can be removed during the repackaging activity, and detection probabilities can be assigned based on the statistical analysis for measurement errors and expert judgment.

NUCLEAR MATERIAL CONTROLS

III–9. The purpose of nuclear material control is to preclude the unauthorized use of nuclear material. Controls should be established for authorizing 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 include tamper indicating devices, separation of duties, dual locks, process or item monitoring.

III–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 actions taken by a malicious insider. If a nuclear material accounting and control system is effective, the accounting and control systems together should detect removal or unauthorized activities involving nuclear material.

III–11. Most nuclear material controls provide ‘delayed’ detection of a malicious act. These controls may include passive tamper indication devices and seals, process monitoring, container restraints or tiedowns.

III–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, the observation of the two-person rule, radiation monitoring that alarms when the containment has been breached, and procedural steps or checks to immediately verify that an activity has been properly completed.

III–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 gain or loss of nuclear material is occurring. In process monitoring, statistical models can be a useful tool in determining or detecting 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. Nuclear material accounting and control and PPS interfaces for evaluation may include the actions of the insider adversary to defeat a nuclear material control and the associated PPS measures during an unauthorized removal attempt. An example of this interface may be during the repackaging example described previous, the insider strategy is to divert the nuclear material through either small amounts for each repackaging action or to acquire a container of repacked material prior to it being recorded in the nuclear material accounting and control records system. The insider strategy may consider the defeat of the following protection measures: two-person rule, item control, material surveillance, pre- and post-measurement or item count, as well as other nuclear material accounting and control measures and PPS interface protection measures. These measures are effective in limiting the amount of nuclear material that can be removed during the repackaging activity. The associated detection probabilities 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 judgment.

III–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 for establishing detection values.

REFERENCE TO ANNEX III

[III–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 IV – PATH ANALYSIS METHOD

INTRODUCTION

IV–1. Path analysis proceeds, in a general way, to determine measures of effectiveness of a physical protection system based on comparison of an adversary timeline and one or more response timelines.

IV–2. Path analysis primarily focuses on the measure P_I as a key measure of PPS effectiveness against an adversary attack (other such measures will be discussed in a later section).

IV–3. PI is defined as the probability that the RFs will arrive and deploy in time before the adversary has completed the attack. PI is calculated using an adversary timeline and a response timeline. Figure B.1 depicts the adversary timeline at the top, indicating the adversary task time it takes the adversary to complete all their tasks, and the sensing opportunities along the timeline, which may cause the adversary to be detected. Below the adversary timeline, there is a comparison between the PRT and the adversary task time remaining on the path after first sensing at each possible sensing opportunity.

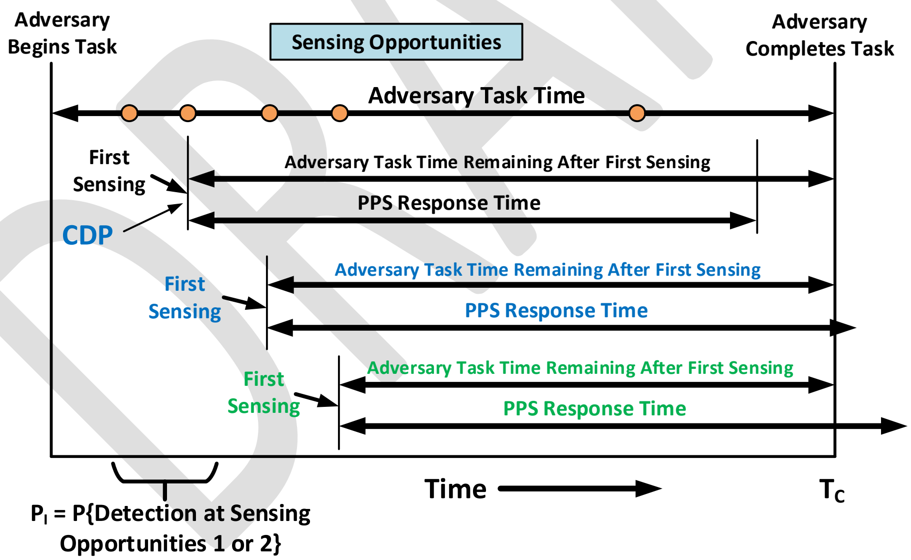


FIG. B.1. Relationship between the adversary timeline and the response timeline

IV–4. If PRT < adversary task time remaining after first sensing, then the corresponding sensing opportunity is considered timely; if this is not the case, then the opportunity is not timely.[6] P_I is equivalent to the probability that the adversary is detected during at least one of the timely sensing opportunities. For the example in Fig. B.1, the first two sensing opportunities are timely, so P_I = P

[6] This model is called ‘timely detection’ and not ‘timely sensing’ because the timing for the beginning of the detection process is the sensing event; hence from a timeline perspective timely detection equates to timely sensing.

(detection at sensing opportunity 1 OR sensing opportunity 2). The CDP is the last sensing opportunity on the adversary timeline that is timely, in this case sensing opportunity 2.

IV–5. The discussion below starts with a definition of adversary and response timelines based on a generalization of a path called an adversary action sequence (AAS). This more general abstraction of a path is used because it accurately describes both insider and outsider attacks and provides a linkage to simulation of an adversary attack plan. The discussion will then present formulas for determining P_I based on the two timelines and will then discuss how path analysis is performed.

ADVERSARY AND RESPONSE TIMELINES

IV–6. The adversary timeline is composed of a sequence of times, each associated with a task that an adversary needs to complete to accomplish their objective of unauthorized removal or sabotage. Each time within the timeline represents how long it would take an adversary to complete that task, given characteristics about the adversary that might be specified within the national threat statement. Thus, the sum of the times represents how much time is required for carrying out all the tasks included in the adversary attack, from the start of the attack in a place where the adversary is not likely to be detected (traditionally termed 'off-site' in evaluation tools) until the last task where their objective is completed.

IV–7. The adversary timeline will depend on the AAS. The most general definition of an AAS is as a time ordered sequence of *n* tasks that the adversary has to complete. An AAS can be thought of as a detailed plan of what a complete adversary team or a single individual would need to accomplish to effect an unauthorized removal of nuclear or other radiological material or sabotage.

IV–8. In carrying out the action sequence there are places on the timeline where sensing may occur. Sensing is defined as the generation of some anomaly that could be evidence that an unauthorized adversary action is under way. The places on the timeline where sensing may occur are called 'sensing opportunities'. Each sensing opportunity has an associated probability of sensing (P_S) and an associated probability of assessment (P_A) which is the probability of a correct assessment conditioned on sensing occurring.

IV–9. Traditionally, it is assumed that each task has an associated sensing opportunity but this not a necessary assumption about AASs. For the discussion below assume that there are N tasks, with times $\tau_1, \tau_2, \ldots \tau_N$ and that there are J sensing opportunities, with probabilities of sensing $P_{S1}, \ldots, P_{Sj}$; J probabilities of assessment $P_{A1}, \ldots, P_{Aj}$; and J probabilities of detection computed as stated in Eq. (1).

$$P_{Dj} = P_{Sj} \times P_{Aj} \tag{1}$$

IV–10. To keep the discussion general, we will assume that there is a time T_{Rj} (time remaining on the adversary timeline after sensing opportunity *j*); the time remaining will depend on the task times, τ_n, in a way that will be discussed later.

IV–11. Once sensing occurs (an alarm is generated or an anomaly is noticed), there are a set of actions that the guard and/or RF will perform to counter the adversary; these actions are depicted on a response timeline. These actions will include 1) assessing the alarm/anomaly to determine if it is indeed due to an unauthorized act, 2) communicating with relevant RFs and 3) deploying those forces to interrupt the adversary before they complete all tasks (see Fig. B.2). The total time from the alarm being generated (at T=0) until sufficient forces arrive to be able to interrupt (in this case, at T_3) is called the PRT.

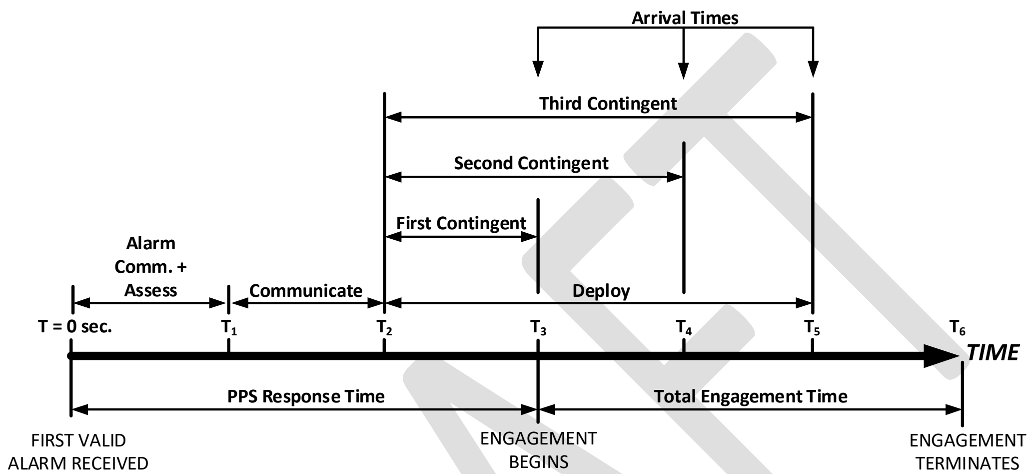


FIG. B.2. Arrival times for the RF

IV–12. In principle, every sensing opportunity may have its own unique response timeline (and associated PRT).

IV–13. It can be noted that in some cases different RFs may arrive at different times; in Fig. B.2, forces show up at different times (T_1, T_2, T_3); the forces that show up at each time are called contingents in this figure even if their arrivals at the same time are not coordinated. Three contingents are shown in Fig. B.2 resulting in values PRT_1 (which is the PRT shown), PRT_2 and PRT_3.

IV–14. From a path analysis perspective, any of the contingent arrival times could be selected within the facility contingency plan as the PRT. Thus, if there are K responding contingents, each sensing opportunity j could have K possible different PRTs. The notation would be PRT_{jk} = the kth PPS response time associated with detection occurring due to sensing at sensing location j[7].

OTHER ASSUMPTIONS AND MATHEMATICAL DEFINITIONS

IV–15. Tasks can be viewed either generally as activities that are to be completed or more specifically as actions against physical protection measures (such as penetrating a wall or defeating a sensor) or as movement from one point to another. There is no requirement, however, that a task be performed in a

[7] A more general model would define PRT_{jkn}, where n is the task on the adversary timeline associated with sensing opportunity j. This case will not be covered here for a number of reasons, but a remark will be made about this topic at the end of this section.

particular place. For example, a task might be to 'learn the combination to the lock' which might occur in any one of a number of places.

IV–16. The action sequence is assumed to be taking the adversary towards successfully completing the attack so that it is presumed that the state (however the adversary's 'state' is defined) at the end of a task is 'closer' in some sense to the objective than the state at the beginning of the task. As an example, the adversary could be physically closer to the target at the end of a transit task than at the beginning.

IV–17. Delays along the AAS may be caused by the need to penetrate barriers or traverse areas but also by armed engagements with guards and RFs.

IV–18. In the discussion below, probabilities are assumed to be point values while delay times and PRTs can be assumed to be either point values or to follow distributions.

IV–19. Probability of Interruption (P_I): the probability that the response arrives in time to defeat the adversary before the latter complete their AAS (we will show the equation for just one contingent so the contingent index *k* will not be shown) (See Eq. 2):

$$P_I = \sum_{j=1}^{J} P_{FDj} \times P\left(T_{Rj} - PRT_j > 0\right) \tag{2}$$

where P_{FDj} = Probability of First Detection at sensing location *j*, defined as Eq. (3):

$$P_{FDj} = P_{Dj} \times \prod_{i=1}^{j} (1 - P_{Di}) \tag{3}$$

Note: The product on the right is assumed to be equal to 1 when j =1, so $P_{FD1} = P_{D1}$.

IV–20. **Timely detection**: When the time remaining, T_{RJ} and PRT_j are point values, those sensing opportunities, j, for which the Time remaining, T_{Rj} exceeds PRT_j are said to be timely meaning that if detection occurs at one of those opportunities interruption will successfully occur before the adversary finishes all of their tasks. When T_{Rj} and PRT_j are point values then sensing opportunity *j* is timely or it is not. If delay times or PRTs follow distributions then sensing opportunity *j* is timely with probability $P\left(T_{Rj} - PRT_j > 0\right)$ and is not timely with probability *1-* $P\left(T_{Rj} - PRT_j > 0\right)$.

IV–21. **Critical detection point**: When the time remaining, T_{Rj} and PRT_j are point values, the last sensing opportunity in the AAS that is timely is the CDP (see Fig. B.1). This point is considered critical in the sense that if detection does not occur before or at this opportunity then the adversary cannot be interrupted. An AAS does not necessarily have any timely sensing opportunities so there may not be a CDP.

IV–22. Remark: It is typically assumed that all of the sensing opportunities before the CDP are also timely. While the Time remaining, T_{Rj}, stays the same or decreases further along the AAS, the PRT_js do not necessarily vary in such a way that all opportunities are timely before the CDP. The only simple sufficient condition for achieving this assumption is that $PRT_j \leq \mathrm{PRT_{CDP}}$ for sensing opportunities before the CDP.[8]

IV–23. If delay times and/or PRTs follow distributions then the selected CDP may or may not actually be timely during a simulation or path analysis. A related issue is that when delays and PRTs are point values, the adversary is assumed to minimize P_D before/at the CDP and minimize delay thereafter. It is not clear how to proceed with choosing defeat methods when delay times and/or PRTs are random variables.

PROGRESSION FROM ANALYSIS OF TIMELINES TO PATH ANALYSIS

IV–24. Path analysis looks at effectiveness of the physical protection system against paths as opposed to AASs. A path is a time ordered sequence of adversary tasks or actions with each adversary action/task being associated with a set of facility locations that the adversary moves through as they perform that action/task. The paths may be defined in a general way by a sequence of elements and areas from an adversary sequence diagram or by a sequence of actions performed by an insider from an adversary action sequence diagram. The same type of metrics, such as P_I, can be calculated for paths as are calculated for AASs.

IV–25. This section will discuss the relationship between paths and AASs starting with adversary action sequences.

IV–26. In principle, it is possible to find the most vulnerable AAS, defined as an AAS that minimizing the one or more metrics over all possible AASs from some starting point outside the facility to the target(s) and then to the end of the path. This is impractical for a number of reasons:

(a) One AAS can differ from another by including different numbers of tasks;

(b) Two AASs can be identical except that the adversary performs a single task against a single physical protection measure (e.g. a fence) using different defeat methods (e.g. cutting through the fence versus climbing over it) or using different tactics such as force, stealth, and deceit;

(c) The performance data for an AAS (P_{Dj}, t_n, T_{Rj}, and PRT_j) will change depending on specifically where the adversaries are located, where they are going and how quickly;

(d) Performance data for an AAS may vary based on the time(s) of day, operational conditions(s), weather condition(s), etc., for which the SA is being performed[9].

IV–27. There are a number of ways of addressing these issues:

(a) Categorize each task in a AAS by a set of locations that the adversary moves through to carry out that task and perform the search for the best AAS only over each set associated with the AAS. To accomplish

[8] $\mathrm{TR_{CDP}} > \mathrm{PRT_{CDP}}$, which means that $T_{Rj} > \mathrm{PRT_{CDP}}$ for all sensing opportunities before the CDP.
[9] In some AASs the tasks cumulatively may extend over long periods such as hours or days, resulting in multiple times, states and weather conditions encountered during the AAS.

this, those AASs that proceed through the same sets of locations would be said to follow the same path. As an example, an adversary path through an ASD might consist of the adversary: penetrating a fence, crossing a protected area (PA), penetrating a door, crossing a building interior, penetrating a certain wall, crossing a vital area and sabotaging a pump. This path ‘includes’ all AASs that go to these locations however defined by the analyst (e.g. penetrating a fence might refer to crossing a perimeter fence anywhere along a the boundary). Thus, a large number of AASs are represented by a set of paths that can be searched to find the one with the lowest P_I, etc.;

(b) Determine conservatively (low) estimates of performance metrics by using minimum probabilities of detection and delay times across defeat methods and operating conditions. These minimum values may be chosen by the analyst but they may also be chosen based on strategies that the adversary might use (such as minimize detection down to a certain task on the AAS and then minimize delay thereafter).

(c) Perform analyses for each of several facility states, where the ‘state’ refers to operational condition(s), weather condition(s), etc., and facility targets.

IV–28. Path analysis, then, includes searching over all paths looking for the one with the lowest P_I, etc. To find the best path, the other two issues need to be addressed. For example, some decision needs to be made about assigning detection and delay times based on all the different defeat methods that the adversary has at each step in the path. Finally, all facility states need to be addressed in some reasonable fashion. These issues will be discussed below.

PATH SEARCHES OVER NETWORKS

IV–29. Path searches are typically performed over a network representing the sets of locations that the adversary would need to pass through to achieve their objectives. Several networks in use are described below. For example, paths can be defined on one type of network called an ASD (see Fig. B.3). In this diagram, the long rectangles represent security areas where an adversary can travel while the squares represent security features that the adversary would need to defeat such as gates (GATs) and Doors (DORs).

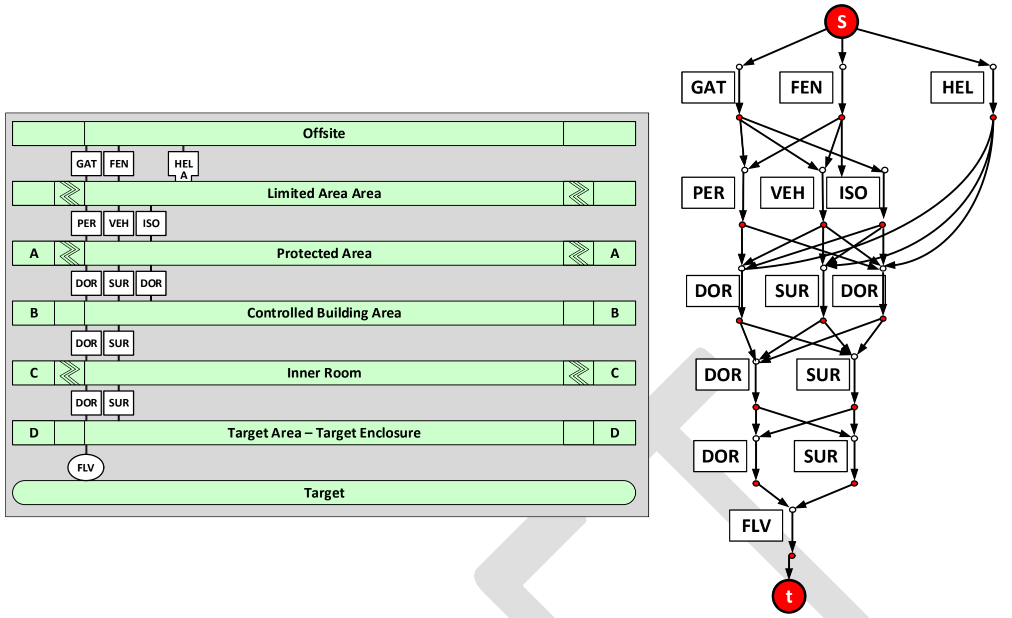


FIG. B.3. Example of an adversary sequence diagram and associated network

IV–30. This ASD could be simplified just to show the boundaries of formal security areas, such as limited access area, protected area, inner and vital areas.[10] The network equivalent of the ASD is shown on the right side of Fig. B.3. Arcs representing the tasks performed at elements such as the personnel portal (PER), vehicle portal (VEH), and isolation zone (ISO) are indicated with thicker arrows. The narrow arrows represent crossing areas, such as the PA between the PER and the surface (SUR). In this model, all P_D and delay times are assigned to the arcs; the nodes merely serve as transition points between adjacent arcs. The red circle with an 's' is the source node where the adversary starts and 't' is the terminal node where the adversary completes their AAS to achieve their objective.

IV–31. Alternatively, the paths through the facility can be represented by movement between nodes of a mesh or grid network as shown in Fig. B.4. Note that the mesh may consist of different types of polygons (such as squares, hexagons, and triangles) and the polygons may be regular (that is with identical sides and angles) or irregular where these sides and angles vary between polygons. The mesh or grid may be two dimensional or three dimensional. Two paths could differ merely by passing through different grid points even though the physical protection measures that are attacked, such as walls and sensors, are identical. Alternative types of networks are visibility graphs, quad trees and Voronoi diagrams; all of these are used in robotic path planning.

[10] In this example, everything within the controlled room boundary, between it and the controlled building area, might be in a vital area.

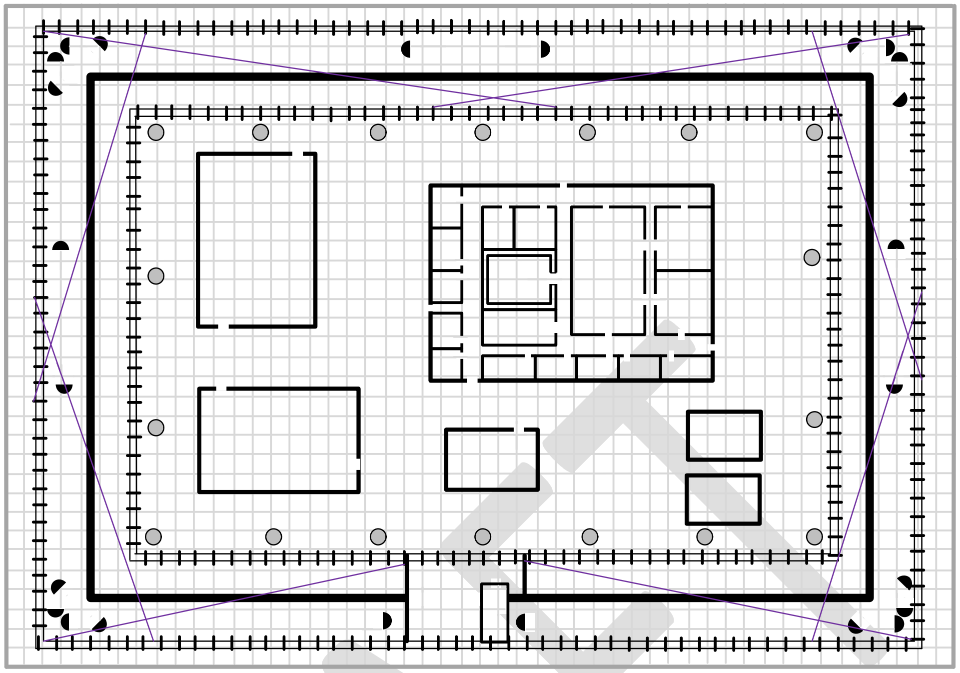


FIG. B.4. *Example of a mesh associated with a facility*

IV–32. Two important issues arise with respect to performing path analysis on these networks:

- How does one ensure that the MVP through the network (e.g. from the defenders' concern about low P_I) is identified?
- How does the analyst deal with mobile elements of the physical protection system, such as guards and RFs that might interact with the adversary on the path?

IV–33. In some cases, shortest path algorithms, such as Dijkstra's or A* methods, can be used to find the MVP. These algorithms can only be used, however, under certain conditions that need to be verified in the underlying model. For example, such algorithms typically require detection probabilities, delay times, and PRTs to be point values (as opposed to following distributions)[11].

IV–34. In other cases, though, such algorithms cannot be proven to work. In such cases, one of several approaches can be taken:

- Have the analyst determine the path;
- Keep the network small enough that an algorithm can review all of the paths by brute force (as has been done with ASDs);
- Perform some global search method that is likely to give the MVP, such as genetic algorithms.

[11] It is possible to sample probabilities and times from distributions *N* times and to solve for MVPs through *N* networks treating the values as if they are point values. This approach comes up with *N* MVPs calculated under slightly different assumptions, which can provide information about how the uncertainty in data affects results. This is different, however, from trying to find the MVP through the network taking those same distributions into account.

DETERMINING WORST CASE PROBABILITIES AND TIMES

IV–35. Even for a single path, there is still the issue of how the adversary performs each task to defeat individual physical protection measures. Several types of decisions come up; for example, if the task is penetrating a fence, does the adversary attempt to climb a fence or cut through it? If they decide to cut through it, what tool(s) might they use, and what delay time against the threat described in the national threat statement would be used? If adversaries use wire cutters to cut through the fence what is the associated probability of detection?

IV–36. There are two main ways of making these decisions:

(a) Use expert judgement: In this case, one or more experts decide what the best defeat methods are and what the associated delay times and probabilities are.

(b) Use information about where the CDP is on the path: In this approach, the analyst selects defeat methods that minimize delay starting at the end of the path until a CDP is found; and then minimizes detection back to the start of the path.

IV–37. As discussed earlier, the CDP can only be defined when detection probabilities and times are point values.

OTHER METRICS BESIDES PROBABILITY OF INTERRUPTION

IV–38. Other performance metrics can be used instead of P_I. Two simple metrics are just cumulative P_D along the entire path (whether that detection is healthy or not) and total delay along the entire path.

IV–39. There are two approaches to attempting to find the path with the lowest P_E:

(a) Software that attempts to find the path with the lowest estimate of P_E based on a combination of path analysis integrated with some sort of combat simulation. Before using such software, it is useful to find out what metric is actually being modelled and to learn about how closely the software can be shown to find one of the most vulnerable paths in terms of that metric.

(b) Use Eq. (4) below, where both P_I and P_N are calculated assuming a given PRT. In this case, P_I comes from a most vulnerable P_I path while P_N is computed using some other tool, such as a combat simulation.

$$P_E = P_I \times P_N \tag{4}$$

IV–40. One complication for determining PRT for this second approach is that, typically, different groups of responders arrive at different times (e.g. on-site forces arrive before off-site forces). An example of this is depicted in Fig. B.2 where RFs arrive in three ‘clumps’ or contingents, each in a slightly different timeframe.

IV–41. Each arrival time leads to a different PRT, based on the sum of the alarm communications and assessment time, response communications time and the deployment time for that contingent of responders. Figure B.2 shows a PRT based on the arrival of the first contingent but the other two contingents could be used as a basis for PRT.

IV–42. The choice of PRT/contingent is chosen by first determining a PRT for each arrival contingent j as PRT_j, $j = 1,\ldots,J$ and then estimating (see Eq. (5)):

$$P_E(PRT_j) = P_I(PRT_j) \times P_N(PRT_j) \tag{5}$$

where $j = 1,\ldots, J$, where j refers to the jth RF contingent

where $P_I(PRT_j)$ is the probability of interruption for the most vulnerable path when PRT_j is assumed. Then the PRT to report is the value PRT_j* which leads to the highest product $P_E(PRT_j)$. Note that the P_N value needs to be determined assuming the adversary is detected at the last possible timely sensing opportunity, namely the CDP.

IV–43. P_N can be calculated using simulations, such as those found in the REF[6].

USE OF SENSING OPPORTUNITIES

IV–44. One of the issues raised with timeline models (see Fig. B.1) is why the adversary timeline shows sensing opportunities and measure response times from sensing opportunities rather than measure from the points on the path where sensing and assessment occur. Figure B.5 addresses that issue.

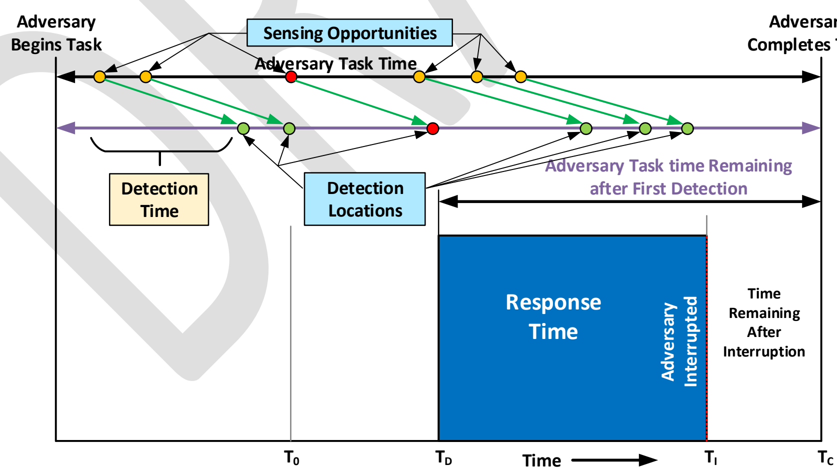


FIG. B.5. Example of a traditional adversary timeline based on sensing opportunities converted in a timeline based on detection locations

IV–45. In Fig. B.5, a second timeline is displayed below the traditional timeline where the sensing opportunities (in green) on the second timeline have been shifted to the right by the amount of time taken to assess the alarm (detection time). These shifted ‘sensing opportunities’ are now labelled as ‘detection locations’ because those are the points on the adversary timeline where assessment is completed. Note that the CDP is the same whether using Fig. B.1 or Fig. B.5 because in Fig. B.5 only the response time is measured after the shifted CDP. The complication here is that the adversary position on the timeline at a particular detection location does not match where the adversary actually was when the corresponding alarm was generated. In the example in Fig. B.5, if sensing occurs at the end of task 3 (the CDP), the detection location is actually depicted in the middle of task 5.

ANNEX V – EXAMPLE OF AN INSIDER ANALYSIS METHOD

V–1. A qualitative based tabletop methodology is one assessment modelling tool that can be used to systematically evaluate system effectiveness of nuclear security through the use of SMEs. The methodology is a scenario based approach based on SME opinion, documented values or a combination of both. The methodology can use either qualitative or quantitative input to document the nuclear security effectiveness against the defined insider threats.

V–2. Evaluating the effectiveness of protective measures involves scenario development and analysis for comprehensive and credible insider scenarios. The effectiveness of the physical protection system against these scenarios is evaluated. If PPS deficiencies are identified, then upgrades will be proposed and analyzed for effectiveness prior to implementation.

V–3. Insiders pose a unique problem since they can choose optimum strategies because they have more opportunity to select the most vulnerable target and the best time to attempt a malicious act. The malicious act can extend over a long period of time to maximize the likelihood of success, and the insider can defeat other operational and safety systems to delay detection and response. For example, insiders may be able to falsify accounting records to repeatedly steal small amounts of NM. Evaluating abrupt theft involves scenario development and analysis for insiders either acting alone or in collusion with another insider. The evaluation generally considers target acquisition followed by removal through the security layers 1 though N as illustrated below.

TABLE C.1. PROBABILITY OF DETECTION FOR EACH SECURITY LAYER

Target Acquisition	Security Layer 1	Security Layer N	Total Pd
P_d (Acquisition)	P_d (Security Layer 1)	P_d (Security Layer N)	P_d(total)

The total probability of detection (P_d) is a function of the P_d at each step or layer of the scenario.

The example below shows 5 layers (layer 1…N) but can have as many as exist in the system being modeled.

Abrupt Theft

V–4. One process for evaluating the PPS against abrupt theft by an insider is described as follows. The process involves developing a list of actions for theft of a selected target, then identify insider strategies and protection measures. The next step is to assign preliminary protection probability and to identify the best insider strategy for theft. The next step is to describe the detailed insider adversary action with specific defeat strategy for that step. The last step is to combine the analysis into a final system effectiveness evaluation table. During the process, the evaluator selects the highest threat insider group(s) for each specific target as a starting point and ensuring that all the insider threat groups and target combinations are evaluated. Many of the details developed for the higher threat groups will also be applicable to the lower threat groups since analyzing all the targets by all insiders for all scenarios is generally not possible.

V–5. It is assumed that the NM targets are contained in drum containers located in a stand-alone locked building, and the nuclear material technician is the insider adversary.

TABLE C.2. HYPOTHETICAL INITIAL INSIDER ACTIONS FOR THEFT

Step	Area	Insider Actions
1	Enter PA	Authorized access
2	Enter Storage Room	Authorized access
3	Inside Storage Room	Acquire Target
4	Storage Room	Remove Target from Storage Room
5	PA	Remove target from PA

V–6. In Steps 1 and 2 the insider uses normal two-person rule authorized actions as far as possible to enter the PA and the Storage Room, so the these two layers can be removed from further analysis.

V–7. In Step 3, once the insider deviates from routine activity, sensing and assessment probability are possible. When the insider does deviate from the routine activity, they will try to minimize detection (and if active “violent” insider, will overtly act to minimize assessment).

V–8. The analyst selects the paths based on the data available and expert opinion (see the TABLE C.3. below). The evaluation process identifies all existing protection measures that may detect or delay each potential separate insider strategy for each step, therefore each step contains several potential insider strategies. Each insider strategy is matched with the existing protection measure encountered using that strategy.

TABLE C.3. HYPOTHETICAL INSIDER STRATEGIES AND PROTECTION MEASURES AT EACH STEP

Step	Area	Actions	Insider Strategies	Existing Protection Measures
3	Inside Storage Building	Acquire Target	Remove from container and hide on person/other	Unauthorized access to target, Two Person Rule
			Falsify shipment to acquire material	NMAC shipment procedure, NMAC records, Two Person Rule
4	Storage Building	Remove target from Storage Building	Hidden on person	Two Person Rule
			Hidden with tools or equipment	Two Person Rule
			Falsify shipment to remove material	NMAC shipment procedure, NMAC records, Guard escort
			Hidden with waste	Separation of Duties; Two Person Rule
5	PA		Hidden on person	NM detection and hand search

Remove target from PA	Hidden with tools or equipment	NM detection and hand search
	Hidden with waste	Vehicle NM detection and hand search
	Falsify shipment	NMAC shipment procedure, NMAC records, Guard escort
	Throw over fence	General observation, Random patrols, 20 m clear zone

NOTE: All insider strategies and protection measures are hypothetical and are used for demonstration purposes only.

V–9. The next step is to assign preliminary "independent" probability of sensing (P_S) and assessment (P_A) values for each protection measure based on the possible insider (defeat) strategies for that step. In this example, preliminary probability of sensing and assessment qualitative values are assigned using expert judgement. These preliminary values are assigned based on facility conditions, PPS and NMAC procedures and compliance, two person rule line of sight conditions, security culture, etc.

Critical note: Assigning the probability of assessment must assume that sensing has occurred. This approach will ensure the proper determination which protection element is deficient and must be improved. In other words, if the sensing is not assumed, the probability of assessment cannot be properly evaluated, nor can the actual conditions and potential improvement be determined.

V–10. 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 protection for that insider strategy as compared to the other strategies in that step. Using this method, see the high-lighted results in TABLE C.4.

TABLE C.4. ASSIGNED PRELIMARY PROTECTION PROBABILITIES AND IDENTIFICATION OF BEST INSIDER STRATEGY FOR THEFT FOR EACH STEP

Step	Area	Actions	Insider Strategies	Existing Protection Measures	P_S	P_A
3	Inside Storage Building	Acquire Target	Remove from container and hide on person/other	Unauthorized access to target, Two Person Rule	M	VH
			Falsify shipment to access target	NMAC shipment procedure, NMAC records, Two Person Rule	M	M
4	Storage Building	Remove target from Storage Building	Hidden on person	Two Person Rule	M	VH
			Hidden with tools or equipment	Two Person Rule	M	H
			Falsify shipment to remove material	NMAC shipment procedure, NMAC records, Guard escort	H	VH
			Hidden with waste	Separation of Duties; Two Person Rule	M	VH
5	PA		Hidden on person	NM detection and hand search	VH	VH

	Remove target from PA	Hidden with tools or equipment	NM detection and hand search	H	VH
		Hidden with waste	Vehicle NM detection and hand search	H	H
		Falsify shipment	NMAC shipment procedure, NMAC records, Guard escort	VH	VH
		Throw over fence	***General observation, Random patrols, 20 m clear zone***	***M***	***L***

P_S = Probability of Sensing, P_A = Probability of Assessment
VL = Very Low, L = Low, M = Moderate, H = High, VH = Very High
NOTE: All probabilities of sensing and assessment are hypothetical and are used for demonstration purposes only.

V–11. The table above reflects that the *potential best combined strategies* to acquire the target with (step 3) falsified shipping papers to open a target container, (step 4) then hide the target with tools or equipment and (step 5) once outside the storage location and at a later time, throw the target over the fence.

V–12. The next step is to develop a *detailed adversary action sequence* (see TABLE C.5.) by describing various insider actions and protection elements to create credible insider theft scenarios by:

- Developing the list of actions and strategies into detailed description
- Determining credibility of insider actions
- Describing specifically how insider accomplishes each step
- Describing protection measures if any

TABLE C.5. DETAILED INSIDER ACTION SEQUENCE DESCIPTION

Step	Step Description
3	*Falsify shipment to access target* – provide detailed description for this strategy to be successful to defeat the protection measures. *NMAC shipment procedure, NMAC records*, Two Person Rule – provide detailed description for these protection measures to either detect insider strategy or to be defeated.
4	*Hidden with tools or equipment* - provide detailed description for this strategy to be successful to defeat the protection measures. Two Person Rule - provide detailed description for protection measure to either detect insider strategy or to be defeated.
5	*Throw over fence* - provide detailed description for this strategy to be successful to defeat the protection measures. *General observation, Random patrols, 20 m clear zone*- provide detailed description for protection measure to either detect insider strategy or to be defeated

NOTE: All insider strategies and protection measures are hypothetical and are used for demonstration purposes only.

— *Note: <u>During the process for detailing the insider actions against the established protection measures in TABLE C.5, the TABLE C.4 assigned preliminary protection probabilities may be revised in TABLE C.6. based on additional input.</u>*

V–13. The next step is to develop TABLE C.6 which evaluates the system effectiveness for this scenario. This is done by analysing each step:

- Within a step, evaluate P_S and P_A individually. Assigning the probability of assessment must assume that sensing has occurred
- Within a step, both P_S and P_A are dependent, therefore, must "sense" the insider action AND assess insider action for the step protection to be effective.
- This process is an intuitive approach, where the weakest link in the chain determined the maximum step protection value or scope.
- Determine the step score using the lowest qualitative value assigned for P_S or P_A

TABLE C.6. SYSTEM EFFECTIVENESS EVALUATION

Step 1 – Select Lowest Value

Step 2 – Select Highest Value

Step	Step Description	P_S	P_A	Step Score
1	*Falsify shipment to access target* – provide detailed description for this strategy to be successful to defeat the protection measures. *NMAC shipment procedure, NMAC records, Two Person Rule* – provide detailed description for these protection measures to either detect insider strategy or to be defeated. *Using expert judgement* – assign P_S and P_A values based on the insider strategy verses the protection measures.	**M**	**M**	**M**
2	*Hidden with tools or equipment* - provide detailed description for this strategy to be successful to defeat the protection measures. *Two Person Rule* - provide detailed description for protection measure to either detect insider strategy or to be defeated. *Using expert judgement* – assign P_S and P_A values based on the insider strategy verses the protection measures.	**M**	H	**M**
3	*Throw over fence* - provide detailed description for this strategy to be successful to defeat the protection measures. *General observation, Random patrols, 20 m clear zone*- provide detailed description for protection measure to either detect insider strategy or to be defeated. *Using expert judgement* – assign P_S and P_A values based on the insider strategy verses the protection measures.	M	**L**	L
	System Effectiveness			**M**

NOTE: All insider strategies and protection measures are hypothetical and are used for demonstration purposes only.

V–14. Is this example, the PPS system effectiveness against the insider for unauthorized removal is "moderate".

V–15. NSS-08 training provides scenario analysis as an example methodology for assessing a facility nuclear security system against the insider threat

V–16. Evaluating collusion between two or more insiders is a difficult process since there are a large number of combinations of potential insiders, each with different access, authority, and knowledge to consider.

V–17. If the national threat statement includes collusion between insiders, then evaluation of the effectiveness of the measures which help prevent collusion (such as compartmentalization and surveillance along with preventive measures) may provide the best approach.

Protracted Theft - Qualitative

V–18. For the evaluation of scenarios involving protracted theft, the P_S and P_A are a function of elapsed time, number of acquisition attempts, and quantity per attempt

- P_S and P_A generally increase as rate of thefts and/or quantity per theft increases
- P_S and P_A are also adjusted by considering the number of cumulative attempts

V–19. For scenarios involving protracted theft from target area (repeated attempts), the following items are considered:

- Small quantity items are easier to remove undetected
- Multiple theft attempts are necessary to obtain a large target quantity of nuclear material
- More protracted theft attempts extend the overall timeline resulting in a longer timeline than for an abrupt theft
- Chances of being detected increases as the number of attempts increases

This same process can be applied to protracted diversion to an unauthorized location within the facility in order to stage the target for a later abrupt theft from the facility

V–20. Using the same method demonstrated in TABLE C.5 to determine system effectiveness, a protracted theft evaluation is described in the sections below.

TABLE C.7. HYPOTHETICAL EXAMPLE OF AN INSIDER PROTRACTED THEFT SCEENARIO ANALYSIS

Nonviolent Insider Protracted Theft of Nuclear Material				
Step	Step Description	P_S	P_A	Step Score
1.	Acquisition Step - The insider removes X g of nuclear material for later retrieval when a goal quantity has been accumulated. The insider repeats this process for a total of 100 assumed attempts over twelve months. Given the number of repeated attempts the P_S and P_A is assumed to be High due to several assumed effective protection measures and material accounting elements.	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 (P_E):		H

V–21. In step 1 the expert group will consider the number of repeated attempts and amount per of nuclear material diverted for each attempt and cumulative amount over time and make some judgment as to the P_S and P_A for that step. The P_S and P_A values are based on actual facility conditions and protection measures and material accounting elements for defeat for each attempt as well as over time.

Protracted Theft – Quantitative Approach

V–22. Figure C.1. below illustrates how a generic scenario probability of detection for physical protection, material control and material accounting activities work together. The timeline is separate for the acquisition stage, the accumulation stage and the exit stage.

V–23. In the Accumulation Profile **-** The material accounting system works independently from the physical protection system. As the insider **acquires** nuclear material (in this case abrupt thefts or series of protracted thefts (small or large) the P_D (where $P_D = P_S \times P_A$) timeline would start. During **accumulation** either through a random inventory, process activity (i.e., process call), or material being identified as being out of place the material accounting system may identify the abnormality.

V–24. During the **exit** of the nuclear material through “layers N” the physical protection system has a P_D at a given value.

V–25. Material accounting system considerations for protracted theft may identify an abnormality but may not identify the cause of the abnormality. NMAC protection measures must consider the elapsed time between attempts, the number of acquisition attempts, and the quantity of material taken per attempt. The ability of NMAC measures to detect theft increases as the cumulative number of attempts, rate of attempts, and quantity of material per theft increases[1]. To evaluate the P_D for protracted theft using a qualitative method, see FIG. C.1.

[1] For more information see A. Sicherman “Evaluating Late Detection, Capability Against Diverse Insider Adversaries”, UCRL—97740, 3 Dec 1987; 7 p; American Nuclear Society Topical Conference; San Diego, CA (USA); 29 Nov - 4 Dec 1987; CONF-8711108--3; Available from NTIS, PC A02/MF A01; 1 as DE88008678

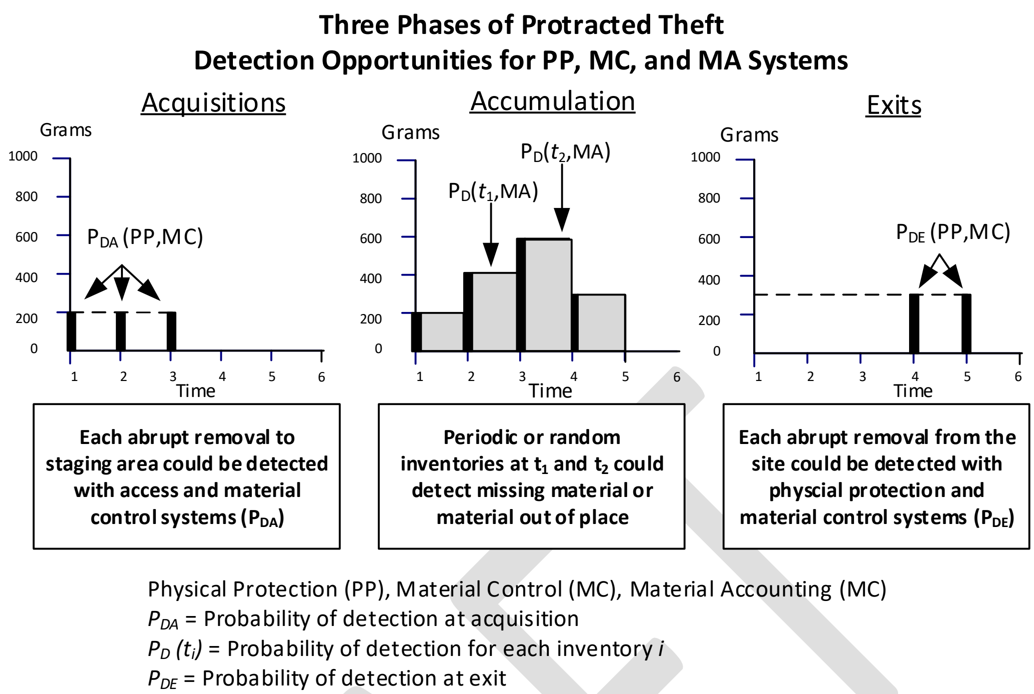


FIG. C.1. Protracted theft of nuclear material detection opportunities

where

Avoidance of sensing during n acquisitions = $1 - (1-P_{DA})^n$

Avoidance of detection during i balance periods = $(1-P_D(t))^i$

Avoidance of detection during m exits = $(1-P_{DE})^m$

where the total protracted theft P_D (see Eq. (6)) would equal:

$$P_{D\ total} = 1 - (1-P_{DA})^n \times (1-P_D(t))^i \times (1-P_{DE})^m \quad (6)$$

Sabotage

V–26. When evaluating sabotage consider not only unauthorized acquisition of material, but also an attack 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 that for abrupt theft. For sabotage, the insider need not leave the facility with nuclear material, so the preventive and protective measures against exiting the facility may not apply. Additional considerations for sabotage include the attack on or compromise of systems or equipment such as cooling pumps, control equipment, valves, etc.