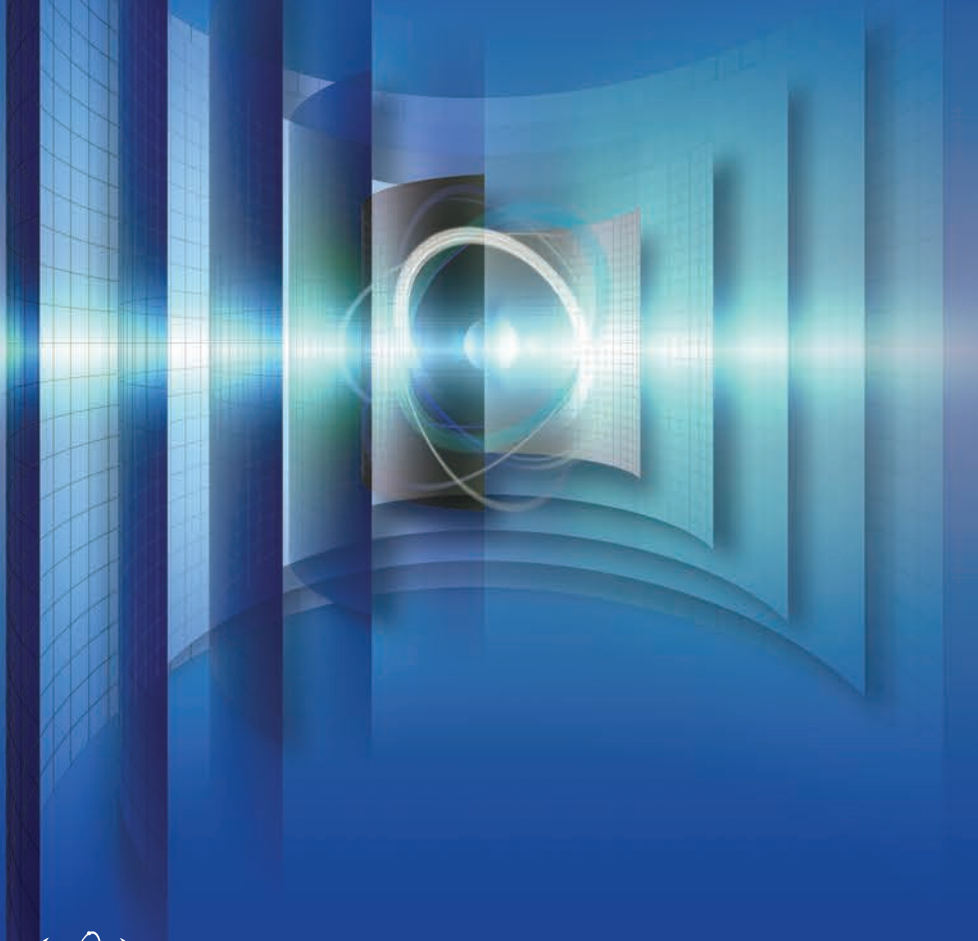
IAEA Nuclear Security Series No. 40-T

Technical Guidance

Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

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

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

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

HANDBOOK ON THE DESIGN OF PHYSICAL PROTECTION SYSTEMS FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES

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

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

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

IAEA NUCLEAR SECURITY SERIES No. 40-T

HANDBOOK ON THE DESIGN OF PHYSICAL PROTECTION SYSTEMS FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
May 2021
STI/PUB/1875

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Handbook on the design of physical protection systems for nuclear material and nuclear facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 40-T | Includes bibliographical references.
Identifiers: IAEAL 21-01412 | ISBN 978–92–0–105419–7 (paperback : alk. paper) | ISBN 978–92–0–100120–7 (pdf) | ISBN 978–92–0–103621–6 (epub) | ISBN 978–92–0–103721–3 (mobipocket)
Subjects: LCSH: Nuclear facilities — Protection. | Radioactive substances — Protection. | Nuclear facilities — Safety measures.
Classification: UDC 621.039.58 | STI/PUB/1875

FOREWORD

by Rafael Mariano Grossi
Director General

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

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

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

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

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

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

EDITORIAL NOTE

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

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.

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 Parties on meeting their obligations under the Convention [3] and its Amendment [4].

1.3. This publication updates the content of a handbook on the physical protection of nuclear materials and nuclear facilities that was issued with restricted distribution.[1] This publication includes information from the International Training Course on the Physical Protection of Nuclear Facilities and Materials, prepared and delivered by Sandia National Laboratories.

OBJECTIVE

1.4. The objective of this publication is to provide comprehensive, detailed guidance for States, competent authorities and operators to assist them in implementing the recommendations in Ref. [1] and the guidance in Ref. [2] for an effective physical protection system (PPS) for nuclear material in use and

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Physical Protection of Nuclear Materials and Facilities, IAEA-TECDOC-1276, IAEA, Vienna (2002).

storage and nuclear facilities. It provides further technical detail on how to design and evaluate a PPS, with respect to the selection and integration of appropriate, effective physical protection measures (including equipment). This publication is intended to serve as a general reference, pointing users to other complementary guidance on specific topics.

SCOPE

1.5. This publication applies to PPSs for nuclear material in use and storage and nuclear facilities against the unauthorized removal of nuclear material and against the sabotage of nuclear material and nuclear facilities. This technical guidance does not address infrastructural aspects of a national nuclear security regime relating to physical protection, such as the legislative and regulatory framework or the institutions and organizations within the State responsible for implementing it. Such aspects are addressed in IAEA Nuclear Security Series Nos 19, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme [5], and 29-G, Developing Regulations and Associated Administrative Measures for Nuclear Security [6]. It also does not address in detail security measures complementary to PPSs, such as computer security measures or nuclear material accounting and control. Such aspects are addressed in other guidance such as IAEA Nuclear Security Series Nos: 17, Computer Security at Nuclear Facilities [7]; 25-G, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities [8]; and 32-T, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement [9].

1.6. The technical guidance in this publication is applicable to all stages in the lifetime of a nuclear facility, but focuses primarily on the design, equipment selection and operational steps of designing, implementing and sustaining a PPS. It addresses equipment and functions of a PPS to provide for prevention of, detection of and response to nuclear security events. It refers, where necessary, to other relevant guidance on specific topics. It also provides some general guidance on the evaluation of a PPS, pending development of detailed specific guidance.

1.7. Although intended for nuclear material and nuclear facilities, the concepts and guidance in this publication can also be applied to radioactive material and associated facilities and activities.

1.8. One of the purposes of nuclear material accounting and control measures is to prevent and protect against insiders who might attempt unauthorized removal or sabotage of nuclear material and nuclear facilities, as discussed in Refs [8, 9]

and in IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [10]. Nuclear material accounting and control comprises both administrative and technical control measures. Technical measures include technologies used for physical protection, such as video surveillance systems and radiation detection alarms. This publication describes the technologies but does not provide specific information on technologies solely used for nuclear material accounting and control, such as tamper indicating devices (see Ref. [9] for more detailed guidance).

1.9. This publication does not include detailed guidance on the following:

(a) Response to a nuclear or radiological emergency that might result from a nuclear security event;
(b) Mitigation or minimization of the radiological consequences of sabotage at a nuclear facility (except to the extent that physical barriers are used to mitigate the consequences of an attack);
(c) Location and recovery of nuclear material out of regulatory control;
(d) Physical protection considerations in the siting of a nuclear facility.

1.10. In addition, this publication does not address security of material in transport, which is covered in IAEA Nuclear Security Series Nos 26-G, Security of Nuclear Material in Transport [11], and 9-G (Rev. 1), Security of Radioactive Material in Transport [12].

STRUCTURE

1.11. Section 2 of this publication provides guidance on key functions and protection measures that normally constitute a PPS. Section 3 describes the process of designing, developing and implementing a PPS. Section 4 provides detailed guidance on physical protection measures, including a range of technology, equipment and supporting procedures used for prevention, detection, delay and response. Section 5 addresses the PPS response, while Section 6 addresses PPS networks and support systems, and Section 7 addresses the introduction of new and emerging technology. Section 8 describes periodic equipment testing and the different types of testing, such as acceptance, operability and functional, maintenance and calibration tests. Section 9 explores PPS evaluation, Section 10 provides an overview of a PPS analysis and Section 11 provides guidance on management systems for nuclear security. The Appendix provides an example of a needs assessment and requirements analysis for adopting a new technology.

2. KEY FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM

2.1. This section describes the key functions of a PPS and how the different physical protection measures and subsystems (as described in Sections 4–6) fit together to create a comprehensive PPS to provide deterrence and to perform the key functions of detection, delay and response to protect against adversaries' attempts to complete unauthorized removal or sabotage. Guidance on key functions of the PPS is provided in Ref. [2].

2.2. A PPS is an integrated system of detection, delay and response measures, and should be effective against both unauthorized removal and sabotage [1]. It should comprise people, procedures and equipment to provide defence in depth, with a graded approach, to address the range of threats identified in the applicable threat statement and to protect against both unauthorized removal and sabotage. Guidance on threat assessment and design basis threat is provided in IAEA Nuclear Security Series No. 10-G (Rev. 1), National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements [13].

2.3. A PPS includes interior and exterior intrusion detection sensors, cameras for assessment, delay measures, access control devices and response measures. A PPS normally has several automated subsystems designed to pass information and video images to a central alarm station (CAS), where they can be used by operators as a basis to respond appropriately. The PPS should also include a secure means for CAS operators to communicate with on-site and off-site response forces and for guards to communicate with each other and the CAS. The PPS integrates all physical protection measures and subsystems, but subsystems may be integrated together within the PPS, for example the intrusion detection system may be integrated with the access control system.

DETERRENCE

2.4. Deterrence is achieved if potential adversaries regard a facility as an unattractive target and decide not to attack it because they estimate that their probability of success is too low or the risks for themselves are too high.

2.5. Sanctions for unauthorized removal or sabotage should be part of the State's legislative or regulatory system [1] to deter an adversary from attempting these acts.

2.6. Maintaining confidentiality of sensitive information about the PPS might deter adversaries by denying them key information that could help them to attempt unauthorized removal or sabotage. An insider might compromise such information, either intentionally or unwittingly, possibly without the knowledge of the operator. A trustworthiness programme might mitigate risks associated with the insider threat. Enforcing the two-person rule for entry into an inner area or vital area can be a deterrent as well as an aid to detecting unauthorized removal or sabotage.

2.7. Other measures that may enhance deterrence at a facility include the following:

(a) A well lit security area with a PPS might provide an impression of high security readiness at a facility and act as a deterrent to a potential adversary. PPS designers can also consider the methodology behind 'crime prevention through environmental design'.[2]
(b) The strategic use of guards and response forces might also contribute to deterrence. For example, a nuclear facility might receive information about a planned peaceful protest on a particular day. Because adversaries could exploit peaceful protests to conceal or divert attention from a malicious act, the operator can deploy extra guards or response forces to act as a deterrent and to provide additional detection, delay and response capabilities.
(c) Random patrols by guards and response forces, both within and outside the limited access areas of a nuclear facility can enhance deterrence. In addition, the use of random searches, hardened guard positions, guard towers and armoured on-site response vehicles can also contribute to deterrence.

2.8. Although measuring deterrence is difficult, thoughtful use of physical protection measures to increase the visibility of guards and response forces, while applying elements of randomness to their actions (including patrols), might deter an adversary. However, the fact that a PPS has not been challenged by an adversary should not be taken as proof that it has deterred such challenges.

DETECTION

2.9. Detection is a process in a PPS that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm [1]. The aim is for detection to occur as early as possible.

[2] See www.cpted.net

2.10. Detection begins with the activation of sensors, or the identification of unauthorized persons or prohibited items through access control measures, or the reporting of suspicious incidents by guards or other personnel. It ends when the initial information has been assessed and determined to be genuinely indicative of malicious activity. Detailed guidance on detection measures, including intrusion alarms, assessment technologies, alarm stations, search systems and access control, is provided in Section 4.

DELAY

2.11. Delay is the function of the PPS that seeks to slow an adversary's progress towards a target, thereby providing more time for effective response [2]. While delay can occur before detection, only delay that occurs after the first detection of an adversary's act will assist with response. Delay is normally provided by physical barriers, but can also be provided or augmented by guards or response forces. All barriers can eventually be defeated, but the delay function is intended to provide time for response measures to be initiated before the adversary completes the malicious act. Detailed guidance on physical barriers is provided in Section 4.

RESPONSE

2.12. Response is the function of the PPS that seeks to interrupt and neutralize an adversary to prevent the completion of any malicious act [2]. Detailed guidance on response is provided in Section 5.

3. DESIGN AND EVALUATION OF A PHYSICAL PROTECTION SYSTEM

3.1. The process for PPS design and evaluation should be systematic and preferably should employ a systems engineering approach. Systems engineering is an approach used to design and build complex systems, and includes processes for defining requirements[3], designing systems and evaluating designs.

[3] In this publication, 'requirements' may include specific written requirements imposed by the relevant competent authority or by the operator to comply with the regulatory requirements.

3.2. The systems engineering approach involves integrated project teams comprising multidisciplinary groups responsible for developing and implementing a design using relevant systems engineering processes.

3.3. These processes are described in detail in international standards (see Refs [14, 15]). For a specific PPS, there may be a requirement to use a specific international standard for the systems engineering process, or standards adopted within the nuclear industry of a State, or regulations specified by the competent authority, or the company constructing or operating the system may be permitted to adopt its own variant.

3.4. This section describes a suggested methodology comprising three phases and using a systems engineering approach:

(a) Phase 1: Identifying the objectives, requirements and specifications for the PPS.
(b) Phase 2: Designing the PPS to meet the objectives, requirements and specifications identified in Phase 1.
(c) Phase 3: Analysing and evaluating the effectiveness of the PPS designed in Phase 2 to meet the objectives, requirements and specifications identified in Phase 1.

3.5. The sequence of the three phases and an overview of the activities in each phase are illustrated in Fig. 1. This is consistent with fig. 2 of Ref. [2], but has been slightly enhanced to explicitly include verification of prescriptive requirements.

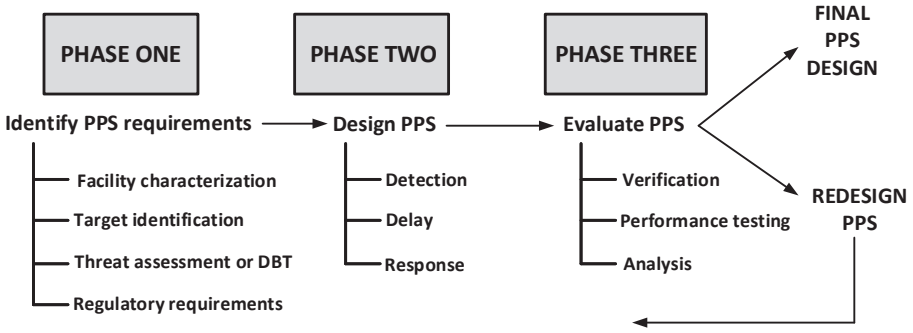


FIG. 1. Process for the design and evaluation of a physical protection system.

3.6. Figure 1 shows an example of a systems engineering process that has been adapted to apply to the design and evaluation of a PPS. The entire process may be applied to a new system, an existing system or to changes to an existing system. The three phases should be iterated as necessary to arrive at an effective PPS design.

IDENTIFYING REQUIREMENTS FOR A PHYSICAL PROTECTION SYSTEM (PHASE 1)

3.7. To begin Phase 1 of the design and evaluation process for a PPS, the designer should first identify the State's legal and regulatory requirements for physical protection. Determining how these requirements are applied at a nuclear facility or to nuclear material includes use of the threat assessment or design basis threat, identification of targets and characterization of the facility.

3.8. Recommendations on the requirements for PPS measures against unauthorized removal of nuclear material and sabotage of nuclear material and nuclear facilities are provided in Ref. [1]. These recommended requirements use a graded approach for unauthorized removal based on the categorization of nuclear material, and for sabotage based on potential consequences and the State's definition of unacceptable radiological consequences and high radiological consequences.

3.9. Other objectives, beyond the scope relating to prevention of unauthorized removal and sabotage as defined in The Convention on the Physical Protection of Nuclear Material [3] and its Amendment [4], may also be identified by States. These can include objectives relating to safety, economics, security of power supply or reputation, and are outside the scope of this publication.

Use of threat information

3.10. A threat statement should be used as a basis for designing and evaluating the PPS [1, 2, 13].

Target identification

3.11. Target identification is used to determine which material and equipment within the facility needs protection and the level of protection needed [2]. This includes identifying the appropriate category of nuclear material needing protection against unauthorized removal and identification of material and equipment needing protection against sabotage.

3.12. The State's threshold levels for unacceptable radiological consequences and high radiological consequences should be used to determine the physical protection requirements for nuclear facilities with identified sabotage targets [1]. The guidance in IAEA Nuclear Security Series No. 16, Identification of Vital Areas at Nuclear Facilities [16], may be used to identify vital areas within a nuclear facility.

3.13. Using a graded approach, each target is required to have an appropriate level of protection, as defined by the State through performance objectives, prescriptive requirements or a combination thereof. Where potential targets are collocated within a defined area or space, that area should be protected in accordance with the more stringent requirements for physical protection, either those against unauthorized removal or those against sabotage [1]. This may have the benefit that substantial detection or delay measures are applied to less attractive targets collocated within that area or building. However, the protection of each target still needs to be considered individually, including particular consideration of the insider threat.

Characterization of the facility

3.14. The PPS should be designed to accommodate the types of operation that will be performed at the facility and to take into account the range of conditions at the facility that could affect it (e.g. environmental conditions or operational conditions).

3.15. One or more operational processes are usually performed at a nuclear facility, and each process may include one or more activities. The processes at nuclear power plants are different from those at nuclear fuel cycle facilities, and therefore the operational activities are different. Paragraphs 3.16–3.19 describe types of information that should be collected about facility activities and processes [2].

3.16. The operating conditions expected at the facility (e.g. normal operation, maintenance, shutdown and emergency conditions) need to be identified and understood. Operational schedules define the activities to be performed at different times during the day and on different days. Information about movements of nuclear material is also needed, including shipping and receiving processes for on-site and off-site movements. Processes and activities relating to safety and nuclear material accounting and control also need to be understood. The interfaces between these different functions, for example between safety and physical protection, should be well understood and characterized.

3.17. Physical and environmental conditions at the facility can affect the performance of physical protection measures, especially those that are outdoors or in high radiation areas. These conditions include topography, vegetation and wildlife, sources of electromagnetic radiation that might interfere with communications systems (e.g. radio or telephone transmitters), and natural seismic disturbances, as well as temperature ranges, precipitation (e.g. rain, snow) and wind (both average and gusting). These factors might affect nuisance alarm rates, the ability of subsystems to sense and assess alarms and/or the ability of guards and response forces to move and perform tasks.

3.18. Facility characterization involves developing a thorough description of the facility, including the boundaries of the facility, the buildings within the facility, building floor plans, structure elevations and normal and emergency access points. Connections between buildings, above and below ground, should also be identified. Details of the construction of walls, ceilings, floors, doors and windows at the nuclear facility boundaries and target locations should be well characterized. Similar information concerning infrastructure, including heating, ventilation, and air-conditioning systems and power distribution systems, and schematics of systems, such as redundant and dependent safety systems in a nuclear reactor, should also be collected.

3.19. Information about the facility can be taken from relevant sources, including facility drawings and process descriptions, safety analysis reports, security and safety plans, construction diagrams, reports of facility reviews, and observations and interviews with personnel. When installing a PPS in an existing facility, information should also include record drawings[4], which may be derived and validated through facility walk downs. This information is needed by PPS designers to understand what needs to be protected and what facility specific constraints (e.g. safety requirements) need to be considered during the design.

DESIGNING A PHYSICAL PROTECTION SYSTEM (PHASE 2)

3.20. The PPS design needs to be such that all security and safety requirements are adequately addressed. During Phase 2, the designer determines how best to combine physical protection measures such as physical barriers, sensors,

[4] Record drawings are the final compiled set of drawings that reflect the facility as built, including all changes made in the specifications and working drawings during the construction process, and show the exact dimensions, geometry and location of all elements of the work completed during construction.

procedures, video surveillance, communication devices and response into a PPS that can satisfy the protection requirements, taking into account other considerations, such as initial and lifecycle costs of the PPS, and potential impacts of the design on nuclear material accounting and control, safety and operations. The overall objective is to ensure that the PPS fulfils the protection requirements by providing an appropriate balance between the functions of detection, delay and response, while also enabling the facility to function effectively. The nuclear facility security plan should reflect the final design of the PPS [2].

General design considerations

3.21. The PPS design should provide for adequate protection while not wasting resources on unnecessary protection measures. When safety, operations and security requirements could conflict with each other, an appropriate balanced approach to risk management should be applied.

3.22. Basic features of the design of a PPS include providing:

(a) Defence in depth, such that the adversary needs to defeat or bypass several protection measures, ideally involving different defeat tactics, in sequence to succeed. This is typically achieved by placing a series of layers of protection around targets, which may include a combination of physical measures (e.g. controls on access to areas through which the target would be reached) and administrative measures (e.g. protection of sensitive information, implementation of a trustworthiness policy). This may involve taking best advantage of the strengths of each physical protection component, and using equipment in combinations that complement the strengths or compensate for the limitations of each other.
(b) Graded approach, which is the use of physical protection requirements proportionate to the potential consequences of the malicious act, taking into account the current evaluation of the threat and the relative attractiveness of the target. For unauthorized removal of nuclear material, this will depend on the nature of the material, and for sabotage of nuclear material or nuclear facilities on the potential consequences if that sabotage were to be successful.
(c) Balanced protection, such that an adversary would encounter comparably effective measures of the PPS in whichever manner unauthorized removal or sabotage is attempted.
(d) Robustness, meaning that the PPS will have a high probability of operating effectively during a wide range of types of adversary attack. This is typically accomplished by incorporating a range of redundant and diverse protection measures in the design.

3.23. In addition to employing the features listed above, it is good practice for the PPS designer to consider designs that can be easily adapted for new and emerging threats, changes in the facility or targets, or changes in legal or regulatory requirements. During the design, consideration can also be given to the ability of the PPS to temporarily protect at the appropriate level a target not normally used or stored in a particular location. For example in the case of an emergency, system failure or other conditions that require the use of alternative or compensatory measures. This might include the temporary installation of the types of system described in Section 4.

3.24. To reduce the insider threat of unauthorized removal of nuclear material and sabotage, a comprehensive approach should include both preventive and protective measures, including those provided by nuclear material accounting and control [8]. More detailed guidance on protecting against insider threats is provided in Ref. [10].

Intrinsic security

3.25. Integrating the features defined in paras 3.22–3.24 as early as possible in the facility lifetime is central to 'intrinsic security' as described in IAEA Nuclear Security Series No. 35-G, Security during the Lifetime of a Nuclear Facility [17], and is likely to lead to more effective and efficient security measures that are more easily sustained or adapted. Adding security measures to a facility after it has been designed and built can result in long term reliance on less cost effective protection measures.

3.26. Intrinsic security includes early consideration of the adaptability of a design (e.g. buying more land than is currently needed to allow for the possibility of more stringent stand-off protection requirements in the future) and consideration of trade-offs between requirements for safety, security, operations and other relevant factors during conceptual design, to identify a design that best addresses requirements in all of these areas. Intrinsic security can also be applied during modifications at an existing facility, although the options might be more limited than for a new facility. Applying security requirements early in partial redesigns and modifications can result in security that is more cost efficient and effective against the defined threats.

EVALUATING THE PHYSICAL PROTECTION SYSTEM DESIGN (PHASE 3)

3.27. During Phase 3, the design of the PPS developed in Phase 2, whether it is new or existing, is evaluated to determine whether it meets the requirements identified in Phase 1. Evaluating the PPS involves three activities referred to in Fig. 1:

(a) Assessments to verify that the PPS meets prescriptive requirements;
(b) Performance testing to determine whether the PPS meets performance requirements;
(c) Analysing data derived from the assessments, performance testing and, for an existing PPS, the results of periodic equipment testing to determine the effectiveness of the PPS in protecting the facility against unauthorized removal of nuclear material or sabotage.

3.28. Evaluation of a PPS should include performance testing [1, 2]. In this publication, testing is divided into periodic equipment testing and performance testing. Periodic equipment testing is used to meet sustainability recommendations for a PPS, while performance testing is used in evaluations of a PPS to ensure it complies with established performance requirements.

3.29. Periodic equipment testing includes acceptance and sustainability testing. Acceptance testing involves testing of equipment and systems, which are newly installed, modified or recently repaired before being brought into service. Acceptance tests determine whether the equipment and systems have been installed and are operating correctly before authorizing their use. Sustainability testing involves maintenance, calibration, operability and functional testing of equipment on an ongoing basis while the PPS is operating. Periodic equipment testing is addressed in Section 8.

3.30. Performance testing involves conducting limited scope and large scale performance tests as part of an evaluation process to determine whether the PPS meets performance requirements against threats defined in the threat assessment or design basis threat. Performance testing is addressed in Section 9.

3.31. PPS evaluation should be appropriate for the stage in the facility's lifetime at which it will be applied [17]. It is good practice to use independent experts to review the PPS before requesting approval from the competent authority for its operation. When using independent experts, protection of sensitive information in compliance with relevant national laws and requirements should be ensured.

3.32. When a PPS is evaluated in conjunction with other systems, such as those for safety, the evaluation should be conducted by an integrated team that includes members with expertise in physical protection, emergency response, operations, safety, nuclear material accounting and control, and other relevant disciplines, and whose trustworthiness has been verified.

OTHER DESIGN CONSIDERATIONS

Physical protection system integration

3.33. A PPS integrates detection, delay and response measures, and should be effective against both unauthorized removal and sabotage [1, 2]. The PPS design should ideally integrate operations, safety, nuclear material accounting and control, physical protection, trustworthiness, and information and computer security in a balanced approach to meet all requirements. The design process should enhance the overall operation of the nuclear facility and help to meet all requirements in the most effective and cost efficient manner. However, the different disciplines have different priorities and perspectives.

Operations

3.34. The operational conditions are aligned with the purpose of the facility. Such conditions that will affect the PPS, and that should be considered in the PPS design phase, include working hours (normally and in particular circumstances), number of people needing access to different parts of the facility, capacity of access control points, and number and types of entrance into a secure area such as a vital area.

Safety

3.35. Effectively managing interfaces between safety and security is an important element of both, to ensure appropriate physical protection of nuclear material and nuclear facilities and health and safety of workers and the public [2]. Physical protection measures should not compromise safety and safety measures should not compromise physical protection. This topic is further addressed in Section 11.

3.36. Close interaction between physical protection and safety specialists is particularly needed in the identification of sabotage targets and protection of these locations. A graded approach should be applied in a manner that does not

compromise safety but allows for effective protection of the targets. The operator should perform target identification analyses:

(a) To determine whether the radioactive inventory at each location within the facility has the potential to result in unacceptable radiological consequences, as determined by the State;
(b) To identify equipment, systems and devices, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences;
(c) To identify computer based instrumentation and control systems important to safety and security.

3.37. Following identification of targets, the PPS should be designed (or modified) to be effective against credible scenarios derived from the applicable threat statement. This process needs to be carried out every time there is a change in the threat assessment or design basis threat, a change in the State's definition of unacceptable radiological consequences or a substantive change in the inventory of the nuclear facility. The process includes identification of vital areas (which contain nuclear material, equipment, systems or devices, the sabotage of which could lead to high radiological consequences), taking into account engineered safety systems that already exist [16].

3.38. Consideration of safety and security requirements at the same time during the design stage of a facility may allow synergies to be exploited effectively. For example, redundancy of equipment or systems, and segregation of such equipment or systems, may provide benefits for both safety and security, whereas providing redundancy without providing for segregation might be beneficial for safety but not for security. The segregation of redundant equipment can provide protection against sabotage by involving more preparation, more equipment and more time for an adversary to complete their actions [10, 18].

3.39. Another example of safety systems that might be designed to also be beneficial to security is continuous air monitors or negative pressure alarms, which provide protection for personnel, but which might also be used to provide alarms indicating a possible attempt at sabotage or unauthorized removal. These systems could be integrated for safety and security by establishing alarm communications (automatic or by procedures) between safety and security personnel if defined conditions occur.

3.40. Basic safety and radiation protection measures such as thick concrete walls or shielding barriers may also be used to increase adversary delay times to target locations.

3.41. Nuclear power plants are specifically designed to withstand extreme external and internal loads such as vibration, heat, overpressure and impact without safety being compromised. IAEA Nuclear Security Series No. 4, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage [18], provides a methodology for assessing the ability of a selected subset of a nuclear power plant's safety related structures, systems and components to withstand a sabotage induced event. This guidance includes assessment of engineered safety aspects for the protection of nuclear power stations against sabotage, including stand-off attacks.

Nuclear material accounting and control

3.42. At the facility level, a robust nuclear material accounting and control system helps to deter and detect unauthorized removal of nuclear material by accounting for material and by applying stringent material controls [8]. The nuclear material accounting and control system should include the capability to receive and assess alarms and to initiate a response if the alarm indicates that nuclear material might have been removed without authorization, or is being used in an unauthorized manner. An effective nuclear material accounting and control system can detect insiders attempting any malicious act involving nuclear material accounting and control records and can support the correct assessment of an irregularity involving nuclear material [8]. The PPS and nuclear material accounting and control system therefore need to function in a coordinated and complementary manner to counter a wide range of threats. Guidance on establishing a nuclear material accounting and control system for nuclear security purposes at a nuclear facility can be used to help operators effectively manage interfaces between the facility PPS and the nuclear material accounting and control system [2, 8, 10].

Information and computer security

3.43. Adversaries wishing to carry out unauthorized removal of nuclear material or sabotage of nuclear material and nuclear facilities might benefit from access to sensitive information. Sensitive information may exist in many forms, including software, the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise physical protection. Before beginning the three phases of designing and evaluating a PPS, operators need to establish internal policies, plans and procedures for protecting the confidentiality, integrity and availability of the sensitive information they hold or handle, in compliance with national security policy and the relevant national laws and requirements on information security. General guidance on information security in a nuclear security context, including an example classification guide to assist in identifying

sensitive information, is provided in IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [19], and Refs [1, 2] provide more specific guidance on the security of sensitive information relating to physical protection.

3.44. Computer security is an important element of PPS design and should be considered in all phases of the PPS design and evaluation. General guidance on computer security for nuclear security is provided in Ref. [7]. IAEA Nuclear Security Series Nos 42-G, Computer Security for Nuclear Security [20], and 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [21], provide more specific guidance on computer security for systems at nuclear facilities.

4. PHYSICAL PROTECTION EQUIPMENT

4.1. A PPS is an integrated set of physical protection measures, including people, procedures and equipment. These measures are implemented and sustained using management systems, as described in Section 11.

4.2. The purpose of a PPS is to prevent and protect against unauthorized removal of nuclear material and sabotage of nuclear material and nuclear facilities [1, 2]. It achieves this using the functions of detection (sensing and assessment), delay and response. These main functions and their interaction are presented in detail in this section.

4.3. A PPS is designed to meet the fundamental principle of defence in depth by creating layered security or concentric security areas centred on identified targets [1, 2]. In this publication, the term ‘security areas’ is used generically to refer to limited access areas, protected areas, inner areas, vital areas and strong rooms within an inner area (see Fig. 2).

4.4. PPS design for a nuclear facility is a complex process. Designers should cooperate at the national level with other designers and experts to coordinate PPS design and equipment selection. Further assistance or advice, if needed, may be obtained through direct cooperation with other States or the IAEA.

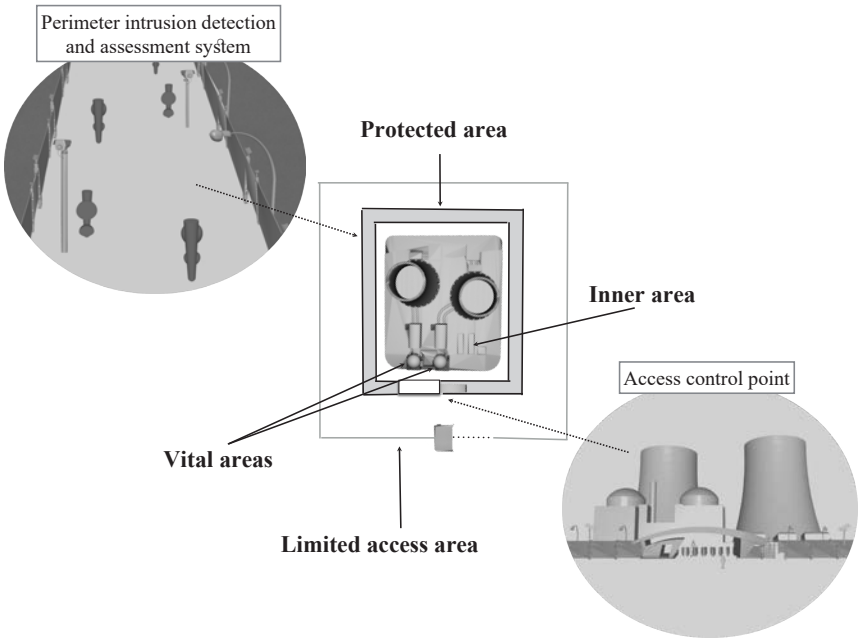


FIG. 2. Types of security area.

DETECTION

4.5. An intrusion detection system is used to generate alarms (sensing) that are assessed by the CAS operator to determine whether they are caused by intrusions of concern for nuclear security. Therefore, the probability of detection is the product of the probability of sensing and the probability of assessment (see Fig. 3). Intrusion detection systems typically include facility exterior and interior intrusion sensors, CCTV, access control measures, alarm communication systems and personnel working together. The intrusion detection system should detect adversaries using their capabilities, as defined in the applicable threat assessment or design basis threat, to attempt or facilitate unauthorized removal or sabotage.

4.6. The designer of an intrusion detection system should have a thorough knowledge of the operational, physical and environmental characteristics of the facility to be protected (see Sections 2 and 3). PPS designers should be thoroughly familiar with the sensing and assessment technologies available, how they work and their limitations.

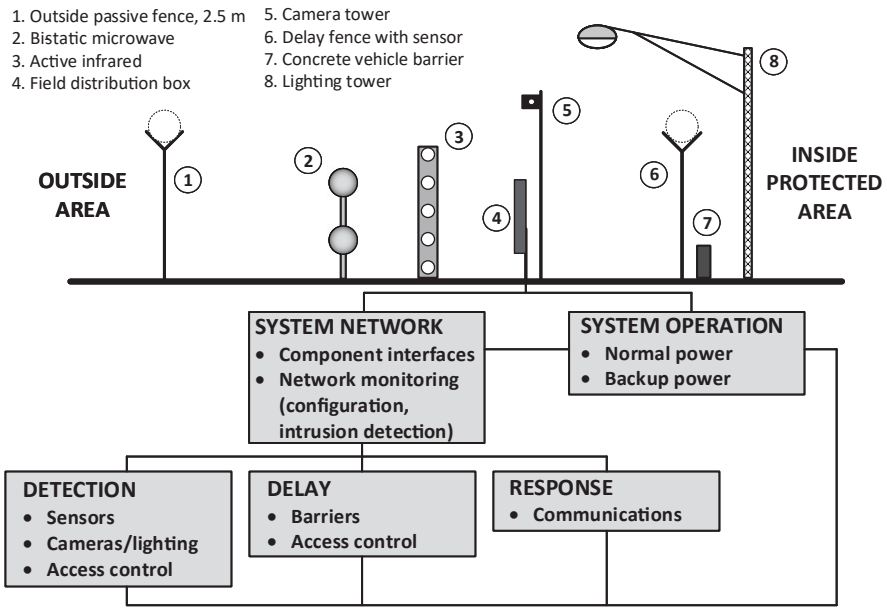


FIG. 3. Typical components of a perimeter intrusion detection system.

Performance characteristics

4.7. The performance of intrusion sensors is described by their fundamental characteristics, including probability of sensing, rates of false and nuisance alarms, and potential to be defeated.

4.8. The probability of sensing depends on the area to be covered and the sensor design, the installation conditions, the sensitivity settings, the weather and other environmental conditions, and the condition of the equipment. It might also depend significantly on the capabilities of the adversary. No sensor is 100% effective, but the probability of a false or nuisance alarm should be as low as possible and the probability of sensing should be as high as possible.

4.9. Conditions will vary for different sensor installations and (although some sensor manufacturers may claim otherwise) a specific probability of detection cannot be assigned to a sensor or set of sensors. The probability of sensing will also vary as equipment ages and conditions change. Therefore, the probability of sensing should be checked by periodic performance tests (see Section 8).

4.10. The nuisance alarm rate is the number of alarms generated over a period of time by occurrences not associated with an intrusion or by planned occurrences such as sensor testing. These occurrences might include environmental factors, such as wind, rain or wildlife, authorized personnel inadvertently causing alarms, or it might result from poor system installation or design. Nuisance alarm rates are usually expressed as an average number of alarms over a period of time (e.g. one nuisance alarm per minute, one per hour, one per day), and might differ greatly between different sensors and installations. Nuisance alarms generated by the equipment itself are termed false alarms (e.g. those caused by poor design or component failure) and are not addressed further in this section. Controlling and maintaining the environment around the sensor can help to minimize nuisance alarms and therefore contribute to the overall effectiveness of the PPS.

4.11. Nuisance alarms are usually further classified by source. Common sources of nuisance alarms for exterior sensors are movement of vegetation, wildlife and weather conditions (e.g. wind, rain, snow, fog, lightning). Other sources of nuisance alarms include ground vibration, electromagnetic interference, radiation and chemicals, and acoustic, thermal and optical effects.

4.12. Identifying and understanding causes of nuisance alarms is important to reducing them. Nuisance alarms can be reduced by three approaches: eliminating the cause of such alarms; reducing the sensitivity of the sensor; or using technologies that can filter out nuisance alarms.

4.13. The first approach, of reducing the causes of nuisance alarms, might include such measures as diverting runoff of rainfall to avoid a sensor bed or installing fencing to reduce vegetation blowing through the area. Some causes of nuisance alarms might be reduced by changing management procedures, for example masking alarms in an area during times when authorized personnel are present.

4.14. The second approach is to reduce the sensitivity of individual sensors. However, care is needed with this approach to ensure that the reduced sensitivity does not unacceptably lower the probability of sensing a real intrusion attempt.

4.15. The third approach is to use technologies designed to filter out some nuisance alarms, for example dual technology sensors, in which two different sensors employing different technologies are used in an AND gate logic configuration. The AND gate produces an alarm only if both sensors are activated, and so nuisance alarms of types commonly encountered with either one of the technologies are less likely. For example, a passive infrared sensor could be placed with a monostatic microwave sensor in the same housing. In this mode,

each sensor could be set at high sensitivity without causing the nuisance alarms associated with a single sensor type.

4.16. When two sensors are combined with AND logic, the probability of sensing will be lower than the probability of sensing of the individual sensors. For example, microwave detectors have a higher probability of sensing motion directly towards or away from the sensor, and infrared sensors have a higher probability of sensing movement across the field of view. Therefore, the probability of sensing with the combined sensors in a single unit will be lower than if the two sensors were mounted separately, perpendicular to each other with overlapping energy patterns and fields of view. If a higher probability of sensing is needed, separately mounted sensors might be preferable.

4.17. Different types of sensor also have different vulnerabilities that can be exploited. The PPS designer should therefore aim for defence in depth through a comprehensive design using different, but complementary, types of sensor with coverage that overlaps in the particular area of interest, so that it is difficult for an adversary to defeat several sensors, based on different technologies, using the same method. Complementary sensors enhance the overall system performance, expressed in terms of the three fundamental sensor characteristics.

4.18. Consideration should also be given to the availability of the intrusion detection system; that is, the ability of the system to perform its functions whenever needed, under the expected range of weather conditions over the lifetime of the system. This can be addressed with redundant and diverse components, components with longer lifetimes and suitable sensors for the expected weather conditions, and through well designed sustainability programmes, including preventive maintenance (which is addressed in Section 11).

4.19. Exterior sensors often need an unobstructed area around the sensor to allow the sensor to work and to provide additional visual evidence to help to assess the causes of sensor alarms. Designers of an exterior intrusion detection system should aim to have uniform detection conditions along the entire length of the perimeter, which is typically achieved by keeping a clear zone parallel to the perimeter fences. The clear zone is intended to keep people, animals and vehicles out of the detection zone and is usually cleared of all vegetation and above ground structures, including overhead utility lines. In areas where the primary sensor cannot be deployed properly, such as a gate, an alternative sensor (e.g. active infrared) can be used to cover the gap.

Environmental conditions

4.20. Many environmental conditions can produce various types of 'noise' in the energy ranges that intrusion sensors are designed to sense. These sources of noise can degrade sensor performance and might cause the sensor to generate an alarm even when an adversary is not present. Paragraphs 4.21–4.28 describe factors that can degrade a sensor's performance and how the effects can be mitigated.

4.21. General environmental factors that can degrade sensor performance include electromagnetic energy, ionizing radiation, certain chemicals, and acoustic, thermal, optical, seismic and meteorological conditions. These factors influence the selection of appropriate sensor technology and might call for specific mitigation measures.

4.22. Since interior sensors generally have less electrical shielding than exterior sensors, sources of electromagnetic energy can particularly affect the performance of certain types of sensor system and increase the occurrence of nuisance alarms. These sensors might also be located in interior spaces in close proximity to numerous forms of electromagnetic energy. Such sources can include lighting, power distribution equipment, transmission lines and radiofrequency transmissions (including from remote controllers). The construction of the building or room to be monitored by an interior intrusion sensor will play an important role in determining the nature of the electromagnetic energy that is present. If the structure is made primarily of wood or concrete, neither of which provides electromagnetic shielding, then a high background of electromagnetic energy generated by external sources is possible. The effects of stray electromagnetic energy can be minimized by providing electromagnetic shielding of all system components (including all data transmission links) and ensuring that all such components are adequately electrically grounded.

4.23. Ionizing radiation can damage some of the components within most types of sensor, particularly semiconductor components, fibre optic cables and camera lenses. Degradation of sensor performance can be reduced by appropriate design and choice of components. In particular, neutron radiation will degrade the performance of semiconductor devices and integrated circuits, the degree of degradation depending primarily on the total radiation exposure, so in areas of high radiation levels the frequency of sensor replacement might be high.

4.24. Chemical environments in some parts of nuclear facilities can negatively affect sensors (and other electronic components with functions relating to nuclear security). Exposure of electronic processing boards to corrosive substances,

especially in conjunction with high levels of humidity, can lead to chemical residues being deposited on circuitry and significant corrosion of the components. This can reduce the performance and reliability of the sensor components. Sensor electronics should be protected to reduce the adverse effects of exposure to corrosive substances. New combinations of materials are emerging in response to the demand for miniaturization, and the effect of corrosion on these materials might be different from that on older materials. Sensor maintenance and testing should therefore be designed to ensure effectiveness of the sensors in the actual environment in which they are used.

4.25. Acoustic energy is generated by many sources, and energy generated by outside sources can be transmitted into an area to be protected. Forms of acoustic energy that can affect the performance of interior intrusion sensors include noise from meteorological phenomena, from ventilation, air-conditioning and heating equipment from television and telephone equipment, and from exterior sources such as aircraft, road vehicles and trains.

4.26. Changes in the thermal environment can result in stimuli that affect the performance of interior intrusion sensors. These changes include uneven temperature distributions, which can cause air movement within the area and expansion and contraction of buildings and their contents. Causes of changes in the thermal environment include weather, heating and air-conditioning equipment, machinery that produces heat, interior lighting, chemical and radioactive reactions producing thermal outputs, and fluctuations of sunlight through windows and skylights.

4.27. Sources of optical phenomena that affect interior intrusion sensors include light energy from sunlight, interior lighting, highly reflective surfaces, and infrared and ultraviolet energy from other equipment.

4.28. Sources of seismic interference that can affect sensors include both natural and human made sources. The primary natural source of seismic interference is wind energy, which is transmitted to the ground especially by fences, poles and trees. Examples of human made sources of seismic interference include traffic and heavy industrial machinery.

Sensor classification

4.29. Sensors are either passive or active, and can be installed in a covert or overt manner. Sensors can be of a type that senses intrusion into a volume, along a line or at a point. Sensor applications (i.e. the ways in which they are installed

and used) include buried line, fence associated, free standing, terrain following, boundary penetration, interior motion, object and line of sight.

4.30. Passive sensors respond to some type of energy emitted by an object of interest (e.g. mechanical energy from a human walking on the ground or climbing a fence) or to a change in some natural field of energy caused by the object, such as a change in the local magnetic field caused by the presence of a metal item.

4.31. Active sensors transmit some type of energy and respond to changes in the energy subsequently received (via transmission or reflection) due to the presence or motion of an object of interest, for example an electromagnetic beam that is temporarily blocked by a person or object passing through it.

4.32. Active sensors can be affected by environmental conditions more than passive sensors because they are both transmitting and receiving signals. Passive sensors therefore typically have fewer nuisance alarms than active sensors in the same environment.

4.33. Most sensors are originally designed with features to make them suitable either for covert or for overt use, but if necessary they can usually be modified in their installation to change from covert to overt (e.g. to provide deterrence) or from overt to covert (to mask the technology).

4.34. Covert sensors are hidden from view, for example by burial in the ground or embedding in walls. They are more difficult for an adversary to identify and locate than overt sensors — although active covert sensors can be detected using electronic equipment — and thus can be more effective against an adversary who is not deterred by visible surveillance.

4.35. Overt (visible) sensors are in plain view of an adversary, for example attached to a fence or mounted on another support structure. Visible sensors might deter an adversary. They are typically simpler to install and easier to maintain than covert sensors.

Sensor type

4.36. Volumetric sensors sense intrusion into a volume of space: an alarm is generated when an object is sensed entering the sensor volume. The sensor volume is usually not visible and is intended to be difficult for the adversary to identify precisely. The characteristics of the sensor volume are based upon a number of

factors including sensor wave frequency and shape of the wave based on the antenna configuration (e.g. cable spacing, mounting height, sensitivity, alignment).

4.37. Line sensors sense intrusion along a straight line: an alarm is generated if an object touches or crosses the detection line. The sensing zone of a line detection sensor is usually easy to identify if the alignment of the sensor can be seen (or if the line follows something obvious, such as a fence).

4.38. Point sensors sense at a specific place, usually a specific object: an alarm is generated if someone or something comes close to, touches or moves the object.

Sensor applications

4.39. Sensors can be used outdoors or inside a building. For external use, the environmental conditions need to be considered, and sensors are typically free standing, attached to or focused on fences ('fence associated') or buried lines. Interior applications of sensors are less affected by environmental conditions and might include boundary penetration and interior motion sensing and sensing of proximity to an object. Early warning systems beyond the facility boundary might also use sensors. Depending on the application, sensors might also be line of sight or terrain following.

4.40. Early warning systems may provide the response forces more time to deploy or to engage the potential adversary before reaching the area of interest. These systems typically include long and short range ground surveillance radar, scanning thermal imaging and laser radar. The effective range of these systems varies from hundreds of metres to tens of kilometres, potentially providing extra seconds or minutes for response. Such systems depend on a line of sight between the sensors and the adversary, but they may be installed in areas outside the facility security boundaries that are not within the line of sight of other sensors and assessment systems. In such applications, the sensors are designed to be covert and totally self-contained. However, such systems pose significant design and operational challenges, which might prevent their effective use. Some of these challenges are described below.

4.41. Early warning systems beyond the facility boundary do not typically provide the level of performance that would be expected for exterior sensors at the facility, such as fence associated sensors. Determining performance requirements and designing systems that can reliably meet them is a challenge, given the nature of these systems and the large areas they potentially need to cover. Performance can

be expected to vary depending on facility specific factors such as environment and topography.

4.42. Line of sight systems should be designed to provide a direct view of the area of interest, and therefore operate most effectively in open areas. In areas where wildlife or vegetation is abundant, the nuisance alarm rate can be high. For some applications to be most effective, such as when using passive infrared sensors, the system itself should normally have range limiting settings and functions, or masking capabilities, to ignore alarms from movement in peripheral areas. Line of sight sensors might need considerable site preparation to level the terrain, or small detection areas, which might result in considerable expense for some facilities.

4.43. Terrain following sensors are capable of sensing adversaries in areas where the uneven topography of the perimeter creates areas that would need significant site preparation of large numbers of sensors to cover with line of sight sensors (see Fig. 4). This type of sensor might or might not be fence associated or buried line. Large terrain variations, such as drainage ditches, can provide places where an adversary can avoid detection, and such variations should be avoided or eliminated.

4.44. Buried line sensors typically sense penetration across the facility boundary. These are normally buried and are not visible (covert sensors). Types of buried line sensor include seismic, magnetic field, ported coaxial cable and fibre optic sensors.

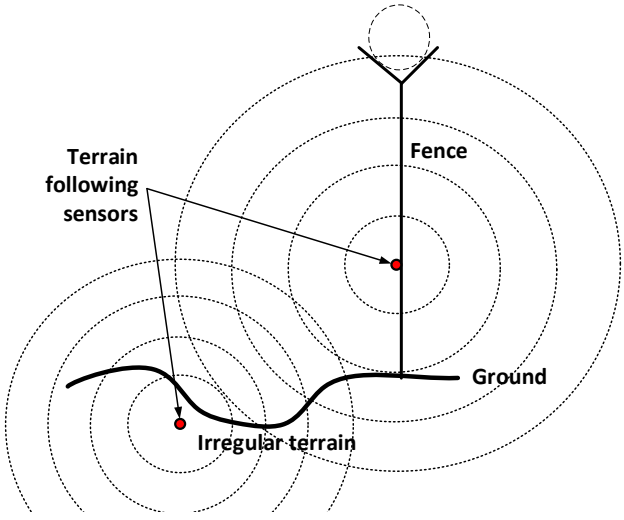


FIG. 4. Terrain following sensor coverage.

4.45. Fence associated sensors can be mounted on a fence or form the structure of the fence, and many such sensors can also be considered terrain following. Examples of sensors mounted on fences include fibre optic cables, capacitance sensors and vibration sensors. Sensors that can form the structure of the fence include strain sensitive sensors.

4.46. Free standing sensors are used for perimeters and sometimes for areas within the facility. Technologies include active and passive infrared laser, bistatic and monostatic microwave and video motion sensors.

4.47. Boundary penetration sensors are used to sense penetration of the boundaries of buildings, including the ceilings and floors of rooms as well as walls and wall openings (e.g. doors, windows, vents). Technologies employed include electromechanical, vibration, glass break, infrasonic and capacitance proximity sensors.

4.48. Interior motion sensors are used to sense movement within an indoor space. Technologies include infrared and microwave sensors.

4.49. Object sensors (also called proximity sensors) are used for a specific target within the facility. Technologies include pressure, weight, electric field, capacitance, video motion and electromechanical sensors.

Exterior sensors

4.50. Each nuclear facility has a unique combination of environmental conditions that can affect the selection of exterior sensors. These conditions include: the physical environment, which will influence the selection of types of sensor for perimeter sensor systems; the natural and industrial environments, which will influence the rate of nuisance alarms; and the topography of the perimeter, which determines the shape and size of the space available for detection, specifically the width and terrain of the clear zone. Thus, a PPS designed for one nuclear facility is unlikely to be optimal for another facility.

4.51. Although an understanding of the interaction between intrusion sensors and the environment has increased significantly in recent years, it is good practice to set up an on-site testing area using different possible sensors before choosing a complete system. This can help to confirm the selection of sensors and to refine the design of the final PPS. Testing should be done in all seasons to assess the performance of the sensors in the actual range of environmental conditions the facility will experience.

Fence associated sensors

4.52. Fence vibration sensors respond to mechanical disturbances of the fence, and are intended primarily for sensing an adversary who attempts to climb or cut through the fence. Several kinds of transducer are used to sense the movement or vibration of the fence. Fence vibration sensors respond to any mechanical disturbances of the fence, and therefore nuisance alarms need to be considered, for example due to strong winds (and rain or debris blown by the wind), hail or vibration from nearby traffic and machinery. Good fence construction, including rigid fence posts and tight fence fabric, can help to minimize the occurrence of nuisance alarms.

4.53. Some configurations of fence vibration sensors use strain sensitive cables. These sensors are attached to the fences and are designed primarily to sense someone climbing or cutting the fence.

4.54. Taut wire fences are fence associated sensors comprising many parallel horizontal wires with high tensile strength, connected under tension to transducers near the midpoint of the wire span. These transducers respond to deflection of the wire caused by an adversary cutting it, climbing on it to get over the fence or separating wires to climb through the fence. The wire is typically barbed, and the transducers are mechanical switches, strain gauges or piezoelectric elements. Taut wire fences can either be mounted on an existing set of fence posts or installed on an independent row of posts in a free standing mode.

Seismic sensors

4.55. Seismic sensors are passive, covert, buried line, terrain following sensors. They respond to disturbances of the soil caused by an adversary walking, running, jumping or crawling.

4.56. A typical seismic sensor comprises a string of geophones, each with a conducting coil and a permanent magnet. Either the coil or the magnet is fixed in position, and the other is free to vibrate during a seismic disturbance; in either case, an electrical current is generated in the coil. Interference from vibrations further away from the seismic sensors can be reduced by alternating the polarity of the coils in the geophone string.

4.57. The sensitivity of this type of sensor is very dependent on the type of soil in which it is buried, and the optimal burial depth depends on the soil. Shallower burial will typically give a higher probability of sensing but with a narrower

sensing area, whereas a greater depth leads to a lower probability of sensing but a wider sensing area. On-site testing with short test sections and sensors buried at different depths can help to determine the optimal depth. The width of a typical sensing area for walking adversaries is in the range of 1–2 m.

4.58. Seismic sensors tend to lose sensitivity in frozen soil. At facilities where the soil freezes in winter, a seasonal adjustment to pressure and seismic sensors can be made to obtain equivalent sensitivity throughout the year if reduced sensitivity in winter is not acceptable.

4.59. Many sources of seismic noise can affect these sensors and cause nuisance alarms. The primary natural source of nuisance alarms is wind energy, which is transmitted into the ground by fences, poles and trees. Human made seismic sources include vehicles and heavy industrial machinery. With seismic sensors, it is difficult to distinguish lighter vibrations, such as footsteps, close to the sensor from heavier vibrations, such as vehicles, further away. They are more commonly used at borders than at facility perimeters.

Pressure sensors

4.60. A pressure sensor comprises two liquid filled tubes buried in shallow trenches and acts like a seismic sensor by detecting small pressure differentials due to pressure (e.g. footsteps) near the sensor.

Magnetic field sensors

4.61. Magnetic field sensors are passive, fence associated, terrain following volumetric sensors, and can be covert or overt. They respond to changes in the local magnetic field caused by the movement of nearby metallic material. They can sense adversaries and their direction of movement and if they are carrying or wearing metal objects (e.g. weapons).

4.62. This type of sensor comprises a series of wire loops or coils buried in the ground. Movement of metallic material near the loop or coil changes the local magnetic field and induces an electric current. Magnetic field sensors can be susceptible to local electromagnetic disturbances, such as lightning, and it can be difficult to tell whether an adversary caused an alarm with a small weapon close to the sensor or by a large vehicle outside the perimeter.

4.63. This type of sensor can be designed to be used underwater or on land at boundaries for early detection of intrusion into the protected area.

Ported coaxial cable sensors

4.64. Ported coaxial cable sensors are typically active, overt or covert, buried line, terrain following volumetric sensors. They are also known as ‘leaky coax’ or ‘radiating cable’ sensors. This type of sensor creates an electromagnetic field around the cables, which is disturbed when an adversary is close to the sensor.

4.65. The name of this sensor is derived from the construction of the transducer’s coaxial cable, in which the outer conductor does not provide complete shielding for the centre conductor, so that some of the radiated signal ‘leaks’ through the ports of the outer conductor. The sensing volume of such sensors extends significantly above the ground, to a height of 0.5–1 m above the surface and to 1–2 m beyond the width of the cable separation. The sensitivity of this sensor depends on the conductivity of the soil.

4.66. Some ported coaxial cables contain a foil shield with a slot instead of ports: a semiconductive inner jacket allows the two cables to be contained in a single outer jacket. This allows the sensor to be installed more easily using a single trench, without a need to consider the spacing between cables. However, the sensing volume in this case is slightly smaller than for a dual cable system with a wide spacing between the cables.

4.67. Older versions of this technology provided a single alarm when something was sensed somewhere within an area, typically up to 100 m from the cables, and allowed only a single alarm threshold for each such area. Newer versions can provide the location at which something was sensed, to within a few metres, and alarm thresholds can be varied along the length of the cables, allowing sensitivity settings to be matched to the different burial media.

4.68. Metal or water in the detection area can cause two types of problem with these sensors. Moving metal objects and moving water are in particular major sources of nuisance alarms, as they provide many opportunities for sensing. Even standing water can contribute to this problem. The second problem is that fixed metal objects and standing water distort the radiated field, possibly in such a way as to create areas in which the sensing is not effective. These sensors should therefore only be used where metal objects, utility lines, fences and poles, underground water lines and electrical cables can be excluded from the sensing volume.

Fibre optic sensors

4.69. Fibre optic sensors are passive or active, buried line or fence associated, terrain following line sensors, and can be covert or overt. Transparent fibres in a fibre optic cable guide light from one end to the other, and are surrounded by a cladding material. The cladding is designed so that light is refracted back towards the centre of the fibre core, and therefore fibre optic cables do not need to be straight. The light diffraction (speckle) pattern and the light intensity at the end of the fibre optic cable are a function of the shape of the fibre over its entire length. A very small change in the shape of the fibre can be sensed using sophisticated sensors and computer signal processing at the far end, up to 100 m or more away.

4.70. Fibre optic continuity sensors can be used to sense penetration of a structural boundary, such as breaking through walls or ceilings. Fibre optic microbend sensors may be applied as vibration or pressure sensors.

4.71. A single mode fibre can also be used as a sensor by splitting the light from the source and sending it in both directions around a loop. If the fibre is disturbed, the two light beams come back in different phases, the change in phasing indicating the amount of disturbance. A single strand of fibre optic cable, buried in the ground at the depth of a few centimetres, can therefore very effectively give an alarm when an adversary steps on the ground above the fibre. To increase the likelihood that an adversary will step above the fibre, it is usually woven into a grid and buried just beneath the surface.

4.72. For fence mounted applications, fibre optic cables can be either mounted on the fence as a type of fence vibration sensor or woven into a mesh that can be installed on a fence to create a fence associated sensor. Such mesh fences usually use some type of continuity sensor to indicate an adversary cutting through the fence. The upper portion of the fence is usually configured so the fibre will be distorted if an adversary attempts to climb over the fence, causing an alarm.

4.73. Sources of nuisance alarms for microbend fibre optic sensors are similar to those for vibration sensors: vibrations caused by external sources such as rotating machinery, low flying aircraft or trains or large vehicles passing nearby. Some nuisance alarms can be avoided by adjusting the sensitivity of the sensor, or filtered out by frequency filtering, event counting or event timing.

Sonar sensors

4.74. Sonar acoustic sensors are active, covert, free standing, terrain following volumetric sensors. A sonar sensor system typically uses acoustic sensors and can be designed for protection of water areas adjoining facilities by sensing and tracking adversaries or objects penetrating into the controlled or protected area. Sonar sensors provide reliable sensing of underwater objects, even under unfavourable marine conditions. Several such systems can be used with overlapping detection zones as part of the overall PPS.

4.75. Sonar works by emitting pulsed hydro-acoustic signals and receiving the subsequent echo signals, reflected from moving objects underwater. Antenna module signals are transmitted through the main cable to the hydro-acoustic service device. Sonar can be installed both at the bottom of a body of water and on hydraulic engineering construction moorings, piers or platforms. Configuration type and structure, choice of the main cables laying route and their protection are defined by the design of the PPS and depend on the underwater terrain and operational conditions.

Radar sensors

4.76. Radar sensors are active, overt, free standing, line of sight volumetric sensors. Radar devices are designed to emit a radio signal and sense changes in the reflected signal to sense objects in the area being protected. They are used for monitoring a controlled area, and provide sensing and tracking of adversaries and objects, such as a small boat or a swimmer. Radar sensors can determine the exact location, speed and route of an adversary.

Laser radar sensors

4.77. Laser radar sensors are active, overt, free standing, line of sight volumetric or line sensors. A laser emits a beam of light to scan an area and measures the time taken for the reflected light to return to the transmitter to calculate the distance from the object. The presence of a moving adversary causes this distance to change between scans, and an alarm is generated.

Interior sensors

4.78. Selection of interior sensors should identify the equipment and installation methods that best meet the goals for intrusion detection for a given facility. This should include consideration of the interaction between equipment, environment

and potential adversaries. Interior sensors add a layer of defence in depth against external adversaries and protection against potential malicious acts by insiders who do not have authorized access to the area being protected (e.g. inner or vital areas).

4.79. It is usually easier to identify appropriate interior sensors than exterior sensors, since building environments are usually more predictable, measurable and controllable. However, choosing the optimal system of interior sensors needs knowledge of the susceptibility of different sensors to the likely causes of nuisance alarms in the environment in question. Motion sensors (microwave and infrared) in particular can be installed to provide acceptable coverage using sensitivity adjustments (manual or automatic) and digital temperature compensation to avoid nuisance alarms from the most common sources.

4.80. Optimal performance of an interior intrusion sensing system can be achieved by an appropriate selection of sensor technologies and placement of sensors (see Fig. 5).

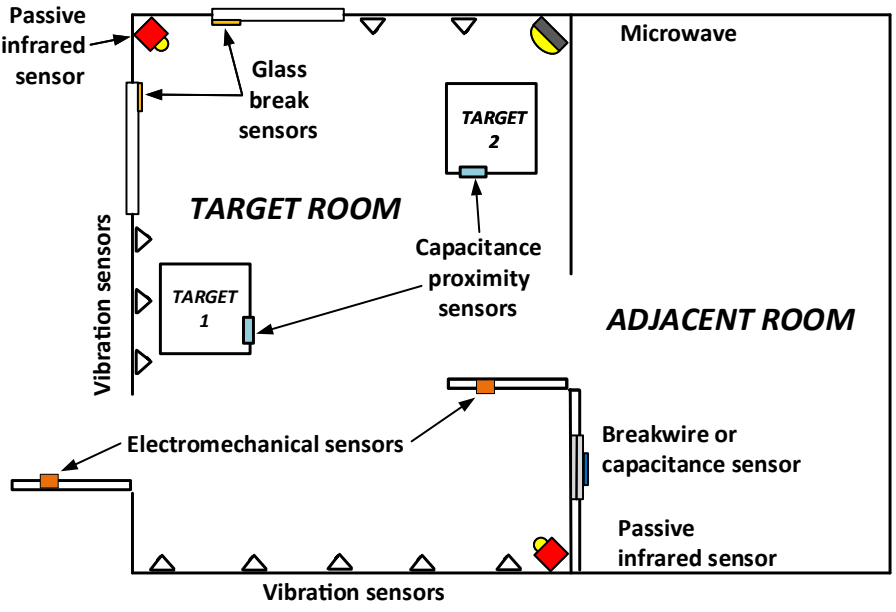


FIG. 5. Placement of interior sensors.

Pressure sensors

4.81. Pressure sensors are passive, covert, object and boundary penetration point sensors. They are often in the form of mats, which can be placed around or underneath an object. Pressure mats contain a series of ribbon switches positioned parallel to each other along the length of the mat. Ribbon switches are constructed from two strips of metal in the form of a ribbon separated by an insulating material, such that when a defined amount of pressure (set depending on the application) is exerted anywhere along the ribbon, the metal strips make electrical contact and initiate an alarm. When using pressure mats in security applications, the mats may be concealed under floor coverings.

Break-wire sensors

4.82. Break-wire (continuity) sensors are passive, covert, boundary penetration line sensors. They are usually attached to, or enclosed in, walls, ceilings, floors or windows to sense penetration. The sensor comprises small electrically conductive wires, and senses the change in current and initiates an alarm if any of the wires are broken. The wires can be formed in any pattern, and therefore a sensor can be designed to protect an area of unusual shape. Break-wire grids and screens can be used to sense penetration, for example through vent openings, floors, walls, ceilings, locked storage cabinets, vaults and skylights. Nuisance alarm rates for this class of sensor are very low, since a wire has to be broken to initiate an alarm, but after each alarm event, the sensor needs to be repaired or replaced. Similarly, continuity sensors based on the breaking of an electrical connection can also use fibre optic cables or printed circuits.

Glass break sensors

4.83. Glass break sensors are passive, overt, boundary penetration line sensors. They employ either shock or acoustic technology, and sense the breaking of the glass in a window. The effectiveness of such sensors depends on characteristics such as the type and thickness of the glass, the distance between the sensor and window, and the presence of any window coverings (e.g. curtains, blinds) or other objects between the glass and the sensor. Shock sensors that are mounted directly on the glass are likely to provide better performance. Nuisance alarms can arise from sources such as thunder, sonic booms, heavy equipment or slamming doors. Vibration glass break sensors can be complemented by additional magnetic contacts to sense the opening of the window without breaking the glass.

4.84. Acoustic glass break sensors are typically mounted on a ceiling or wall within a specified distance of the windows being protected. In order to generate an alarm, most sensors of this type need to sense the initial low frequency sound of impact on the glass followed immediately by the higher frequency sound of the glass breaking. Nuisance alarms can arise from sources of noise of similar frequencies, such as dropping keys on a desk.

4.85. Vibration sensors are passive, overt, boundary penetration line sensors that can be installed on walls, floors and ceilings to detect attempts to penetrate surfaces to gain access to the room. These sensors may differ only slightly from fence vibration sensors by sensing the different frequencies that would be associated with breaking through the surface. These can use fibre optic, piezoelectric or 'jiggle switch' technologies.

Interior and exterior sensors

4.86. Some sensors can be used for both interior and exterior applications, with adjustments in installation to allow for the different environments. Considerations in the installation of such sensors should include the following:

(a) Location (e.g. near the target or at a boundary);
(b) Mounting;
(c) Resistance to defeat through tampering, masking, spoofing or other adversary tactics;
(d) Need for weather proofing (e.g. against water, extreme temperature, dust);
(e) Light levels and variations in them;
(f) Ease of access for maintenance;
(g) Manufacturer's specifications;
(h) Sources of potential nuisance alarms.

Active infrared sensors

4.87. Active infrared sensors are active, overt, line of sight line sensors and can be fence associated, free standing or boundary penetration. The narrow vertical plane in which this sensor operates does not provide any significant volume coverage. These sensors can be used over short ranges for filling gaps in coverage, such as for gates, doors and portals. They can also be used in applications with long ranges of up to about 100 m.

4.88. Active infrared sensors work by transmitting an infrared beam from an LED through a collimating lens and receiving the beam through a collecting lens that

focuses the energy onto a photodiode. The sensor senses the change of the energy of the received beam when an opaque object blocks the beam or changes the reflection characteristics.

4.89. Although single-beam sensors are available for point to point systems, multiple-beam sensors are normally used for nuclear security applications because a single-beam sensor is too easy to defeat or bypass. Figure 6 shows an example point to point system with multiple-beam sensors in two vertical arrays of transmitter (T) and receiver (R) modules (the specific number and configuration of modules depends on the manufacturer). The resulting 'fence' of multiple beams initiates an alarm if any single beam is interrupted. Multiple-beam sensors usually incorporate some type of logic that will initiate an alarm if an adversary attempts to spoof a receiver by aiming another infrared source at it.

4.90. If the 'visibility' between the two arrays is reduced, for example by atmospheric fog, snow, smoke or dust, the system might produce nuisance alarms. Falling objects, small animals or other moving objects could also obstruct the infrared beam sufficiently to cause an alarm.

4.91. Active infrared sensors need a flat ground surface because the beam travels in a straight line: a convex ground surface will block the beam, and a concave surface could allow an adversary to pass under the beam without being sensed. Dual technology sensors can be used to address this limitation.

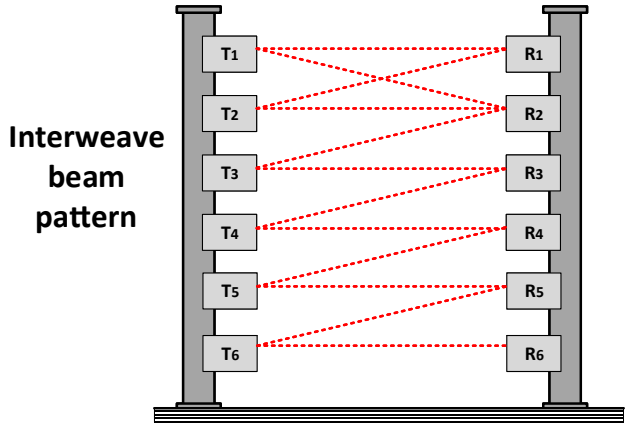


FIG. 6. Active point to point infrared system using multiple beams to create an interweave beam pattern.

Passive infrared sensors

4.92. Passive infrared sensors are passive, overt, line of sight volumetric sensors and can be free standing, and are most commonly used for interior motion detection. They sense changes in thermal energy, caused for example by a human entering the sensor volume. This will typically be an increase in thermal energy because the adversary is warmer than the background; in a high temperature environment, it could also sense an adversary cooler than the background. Special lenses focus the infrared beam onto the detector of the sensor and create a specific field of view: with different lenses, the field of view can be a wide view over a short distance or a narrow long distance view. Wide angle lenses provide volumetric sensing, such as within a room, while narrow view lenses can be used to protect a long narrow area such as a corridor or a perimeter. The lenses also segment the field of view into sensitive and non-sensitive areas.

4.93. Where possible, passive infrared sensors should be mounted so that the motion of an adversary is likely to be across the line of sight, for which the sensitivity is higher. Nuisance alarms could be caused by atmospheric conditions, blowing debris and animals, and sensing might be unreliable during heavy rain. The passive infrared sensor is most sensitive when the background is at a significantly different temperature from an adversary. Sensor ranges can exceed 100 m. Because these are optical devices, the only way to limit the maximum range is to aim the sensor at a solid object, such as the ground, at the end of the desired sensing zone (see Fig. 7).

4.94. The sensor pattern for a typical interior passive infrared sensor is shown in Fig. 8. Subdivision of the field of view into the solid angular segments shown is accomplished with the segmented lens. Such lenses are either Fresnel type, located in front of a pyroelectric sensor, or segmented mirror type, which reflects energy onto the sensor.

4.95. Passive infrared sensors are most sensitive when sensing motion across the field of view, and least sensitive for motion directly towards or away from the sensor (this is the opposite case to that of microwave sensors), as motion across the field of view results in more segments being entered in a shorter distance. This characteristic should be considered in determining where to mount the sensor.

4.96. To reduce nuisance alarms caused by changes in heat emitted by the ground as clouds passed overhead, sensors compare the received thermal energy from two curtain shaped sensing patterns. A human moving into one area causes an

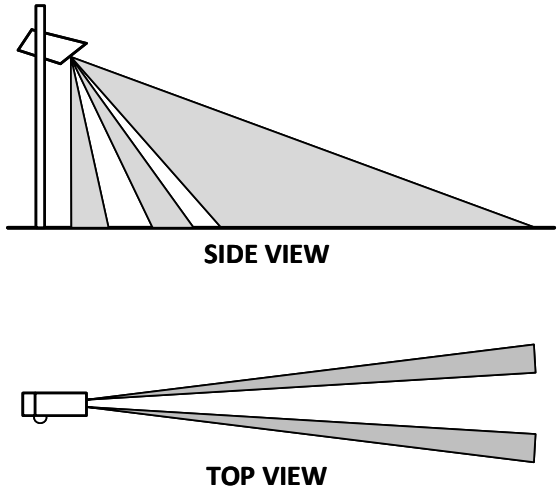


FIG. 7. Passive infrared sensor coverage.

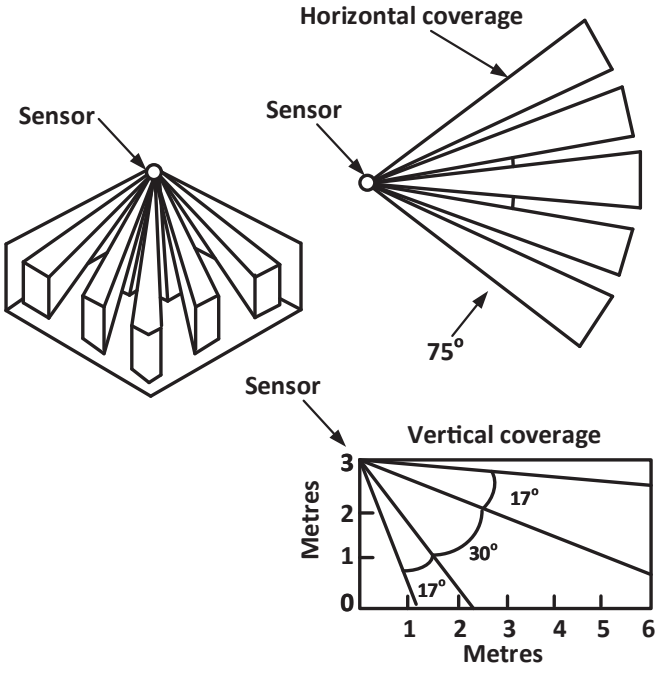


FIG. 8. Passive infrared sensor pattern. (Courtesy of Sandia National Laboratories).

imbalance. Weather changes should affect both areas equally to prevent causing an alarm. Indoor application may only use a single sensor.

4.97. Other sources of nuisance alarms might include insects on the lens and other sources of infrared energy, such as heat sources (e.g. radiators, heaters, hot pipes) or hot surfaces (e.g. sunlight passing through windows can produce locally heated surfaces that can radiate energy in the relevant wavelength). Dual technology sensors can be used to address these limitations.

Electric field or capacitance sensors

4.98. Electric field sensors (including capacitance sensors) are active, overt, terrain following volumetric, line or point sensors, and can be fence associated, free standing or boundary penetration. Interior sensors of this type create a resonant electrical circuit between a protected metal object and a control unit, making them active sensors. The capacitance between the protected metal object and ground becomes a part of the total capacitance of a tuned circuit in an oscillator. The tuned circuit might have a fixed frequency of oscillation or the frequency might vary.

4.99. For perimeter applications, the sensitivity of some electric field sensors can be increased to extend the sensor volume to up to 1 m beyond the wire or plane of wires. However, high sensitivity typically leads to more nuisance alarms, and electric field sensors might be susceptible to lightning, rain and movement of the fence or small animals. Ice storms might cause substantial damage to the wires and the stand-off insulators. Good electrical grounding of electric field sensors can help to reduce nuisance alarms, and other metal objects (e.g. the fence) in the sensor volume should be well grounded, as poor or intermittent grounding will cause nuisance alarms. Because the sensor volume is relatively large and extends beyond the fence plane, electric field sensors are more difficult than other fence associated sensors to defeat by digging under or bridging over the fence.

4.100. Electric field sensors mounted on their own posts will typically provide improved performance because higher sensitivity can be used to obtain a wider sensor volume, since there will be a lower nuisance alarm rate due to movement of the fence.

4.101. This type of sensor may also be used to sense boundary penetration through existing building openings with metal fittings, such as grills, ventilation ducts, window frames and doors.

4.102. For interior applications, electric field proximity sensors can be used for the protection of objects or defined areas within buildings (e.g. safe or sensitive technologies in a work area). For applications where the object to be protected needs to be grounded, the object can be considered the ground plane, and grounding can be achieved by means of a capacitance blanket draped over the object. If the blanket is made large enough to cover the object entirely, any attempts to gain access to it will cause the blanket to move, resulting in a change in capacitance and an alarm. Such sensors can detect capacitance changes as small as a few picofarads.

4.103. The sensitivity of electric field sensors can be affected by changes in relative humidity and the proximity of other metal objects to the protected object. Changes in relative humidity change the dielectric characteristics and the conductivity of the air. If the sensor's sensitivity is set to sense an adversary several metres from the object, this change in conductivity could be sufficient to cause a nuisance alarm. Sensors using a self-balancing circuit adjust automatically to changes in relative humidity and proximity of metal objects to the protected object. Nuisance alarms might nevertheless occur if the object is in an area of high pedestrian traffic.

Microwave sensors

4.104. Microwave sensors are active, overt, line of sight, free standing or interior motion volumetric sensors. Typically, bistatic microwave sensors are used, with two identical microwave antennas at opposite ends of the sensor zone. One antenna is connected to a microwave transmitter and the other to a microwave receiver. The receiver detects changes in the energy of the direct beam between the antennas and the microwave signals reflected from the ground and other objects. Microwave sensors respond to changes in the vector sum of the received signal caused by objects moving in that portion of the transmitted beam that is within the viewing field of the receiver. A moving adversary thus creates new reflections as they approach the sensor or block the signal, and increase or decrease the received signal depending upon the phase of the signal.

4.105. Considerations when specifying microwave detection criteria include the following:

(a) The ground surface should be flat so that the object is not shielded from the microwave beam, preventing sensing.

(b) To overcome the effects of the area of reduced sensing capability in the first few metres in front of the antennas, antennas for adjacent sensors should overlap to cover this area.
(c) The sensing volume for bistatic microwave sensors is large compared to most other intrusion sensors: the cross-section of the volume may be as large as 4 m wide and 3 m high. Microwave sensors can also be stacked to obtain larger sensing volumes.

4.106. Microwave sensors can tolerate a relatively wide range of environmental conditions without producing nuisance alarms. However, the sensing zone should be kept clear from snow and vegetation. To minimize nuisance alarms due to reflections from surface water (from rain or melting snow), flat surfaces in the sensor zone should have a slope or other means of water drainage. Gravel is also often used to reduce nuisance alarms from standing water.

4.107. Monostatic microwave sensors have the transmitter and receiver in the same unit. Radiofrequency microwave energy is pulsed from the transmitter and the receiver senses changes in the reflected beam. A moving adversary causes the reflected frequency to change slightly and thus causes an alarm. These sensors are ‘range gated’, which means that the operator can set the range beyond which movement will not cause an alarm. The monostatic installations are typically used in a fixed volume (e.g. a corridor) or across gates and portals.

4.108. Detection is based on the Doppler shift between the transmitted and received signal caused by a moving object within the energy field. Monostatic microwave sensors are most sensitive to motion directly towards or away from the sensor because this maximizes the change in microwave frequency. Such sensors should ideally be located so that an adversary’s movement from likely points of entry towards protected objects will be approximately towards or away from the sensor. The shape of the sensing zone is governed by the design of the antenna (see Fig. 9).

4.109. Range gating may be used to limit the distance of effective detection, especially if the sensor is to be used at a location where the microwave energy can penetrate beyond the walls of the area or room being protected. Microwaves will penetrate most types of glass, plaster, gypsum, plywood and other materials typically used in walls. This can cause unwanted interference with sensors. Metal objects, such as large items of furniture, screens or fencing within the protected area, can cause ‘shadow zones’, in which there is incomplete coverage.

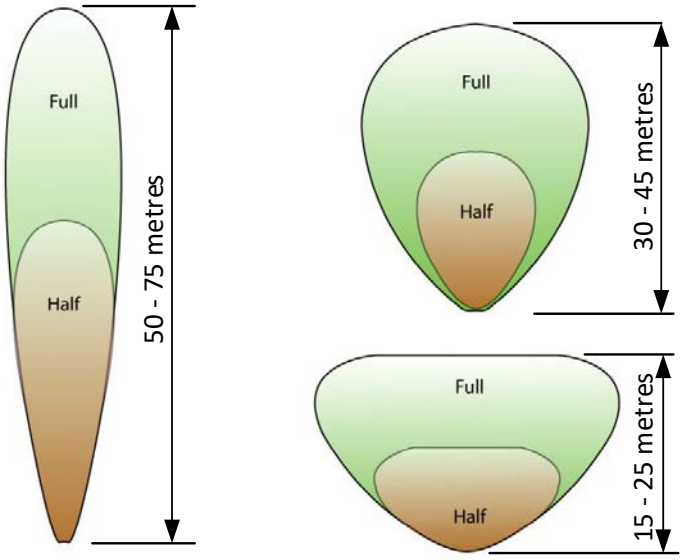


FIG. 9. Typical monostatic microwave detection patterns.

4.110. For interior applications, microwave sensors should ideally be mounted near the ceiling of the area being protected and aimed in the direction of desired coverage, but away from metal objects that might reflect microwave energy and cause nuisance alarms.

Video motion sensors

4.111. Video motion sensors are passive, overt or covert, free standing or interior motion volumetric sensors. These sensors process the video signal from CCTV cameras, which are used in both interior and exterior locations. Such cameras are typically installed on towers, ceilings or walls to view the area of interest, and may be jointly used for sensing, surveillance and alarm assessment and as a video record. Artificial lighting might be needed for daylight cameras in continuous operation.

4.112. Video motion sensors with video analysis capability (hardware modules, video alarm processing hardware and software) can be added to analogue or digital camera systems using daylight cameras, near-infrared cameras, thermal imaging and 360 degree views. Such technology is modular, and can be installed either with the camera or at the CAS.

4.113. Video motion sensors sense a change in the video signal level for some defined portion of the viewed scene. Depending on the application, this portion may be a large rectangle, a set of discrete points or a rectangular grid of points.

4.114. Video motion sensors have a higher probability of sensing movement across the field of view than towards or away from the camera. The background in the detection zone should ideally be a neutral colour, as very light or very dark backgrounds are easier for an adversary to blend into. The probability of sensing might also be reduced during conditions of reduced visibility, such as fog, snow and heavy rain.

4.115. Potential sources of nuisance alarms for video motion sensors used outdoors include movement of unstable camera mounts, changes in light due to, for example, clouds, reflective objects and vehicle headlights, moving objects such as birds and other wildlife, blowing debris and precipitation on or near the camera. Some of the sources of nuisance alarm can be reduced by the use of a screen to limit the camera's field of view.

Vibration sensors

4.116. Vibration sensors are passive, overt line sensors that can be buried line, fence associated or boundary penetration. Interior vibration sensors include glass break sensors. Vibration sensors sense the movement of the surface to which they are attached: an impact on the surface will cause it to vibrate at a specific frequency dependent on its construction and, to a lesser extent, that of the object causing the impact. Vibration sensors are designed to respond to frequencies associated with breaking and entering events, such as forced entry (usually greater than 4 kHz), and to ignore normal building vibrations such as those due to air-conditioning or heating equipment.

4.117. Vibration sensors might generate nuisance alarms if mounted on the walls or structures that are exposed to external vibrations, and their use on structures subject to frequent severe vibrations (e.g. due to rotating machinery) is not advisable. However, if the structures are subject to occasional impacts, vibration sensors might be effective if fitted with a pulse accumulator or count circuit.

Electromechanical sensors

4.118. Electromechanical sensors are active or passive, overt or covert line or point sensors for boundary penetration and object applications. The most common type is a relatively simple switch usually used to sense the opening of doors and

windows. Most switches of this type are magnetic and comprise a switch unit and a magnetic unit. Figure 10 shows a magnetic reed switch and its components in the closed and open positions.

4.119. The switch unit, which contains a magnetic reed switch, is mounted on the stationary part of the door or window. The magnetic unit, which contains a permanent magnet, is mounted on the movable part of the door or window, adjacent to the switch unit when the door or window is closed. The spacing between the switch unit and the magnet unit is adjusted so that the magnetic field from the permanent magnet causes the reed switch to be in the closed (or secure) position. Opening the door or window moves the magnet away, resulting in a decrease in the magnetic field and movement of the switch to the open (or alarm) position.

4.120. An additional bias magnet can be added for adjustment to help prevent defeat: the switch is then referred to as a balanced magnetic switch. Other variations include multiple reed switches and multiple magnets, fusing and voltage breakdown sensing devices, and shielded case construction. Some units incorporate internal electromagnets, which have complex interactions with the movable permanent magnets, increasing the complexity of the unit and making it more difficult to defeat. Some models also have features to make them self-testing.

4.121. A Hall effect switch contains electronic switches instead of mechanical reed switches and needs to be powered. It is intended to provide a higher level of security than balanced magnetic switches. Like other magnetic switches, it comprises a switch unit and a magnetic unit, but operation of the switch is based on Hall effect devices in the switch unit measuring the magnetic field strength

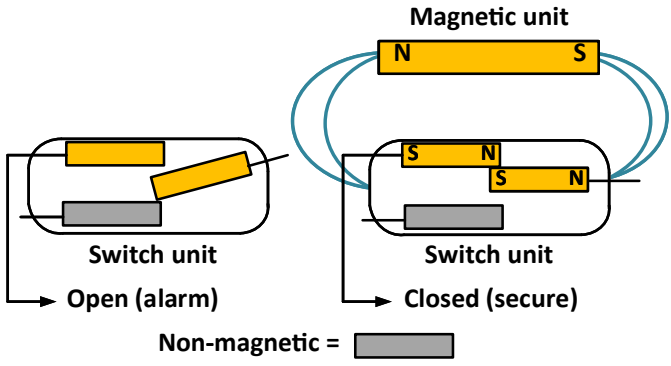


FIG. 10. Magnetic reed switch.

of the magnetic unit. If sufficient changes in the magnetic field occur, an alarm is generated. Both balanced magnetic switches and Hall effect sensors provide better protection against tampering and defeat, including by insiders, than does the simple magnetic switch.

Thermal imaging sensors

4.122. Thermal imaging sensors are passive, covert, line of sight, free standing or interior motion volumetric sensors. Thermal imaging cameras allow recognition and identification of different types of adversary, even under unfavourable meteorological or lighting conditions and at different distances.

Sensor technology summary

4.123. Table 1 summarizes the different intrusion sensor technologies according to the different modes of operation, type of sensor and sensor application.

Alarm assessment

4.124. The final step of the detection process is alarm assessment, which includes the following:

(a) Determining the cause of each sensor alarm;
(b) Deciding whether the alarm is caused by an adversary or is a nuisance alarm (e.g. an innocent alarm due to an environmental event or a false alarm);
(c) If the cause of the alarm is confirmed as an adversary, providing information about the adversary, such as who, what, where, when and how many.

4.125. Alarm assessment is dependent upon trained personnel assisted by appropriate video, lighting and communications technologies.

4.126. Alarms may be assessed using visual evidence from video technologies and/or personnel. Both assessment methods depend upon adequate lighting and appropriate lines of sight. Use of video assessment can reduce the typical assessment time and therefore the overall response time.

4.127. The use of video assessment typically includes output from fixed cameras that allow event recording, instant replay and stop action, and from pan and tilt cameras with manual control or intelligent search functions (e.g. moving automatically to point to the location of sensed movement).

TABLE 1. SENSOR TYPES AND TYPICAL APPLICATIONS

Sensor	Method[a]	Sensor type[b]	Application[c]
Exterior			
Seismic	P	L	BL, TF
Magnetic field	P	V	BL, FA, TF
Ported coax	A	V	BL, TF
Fibre optic	A, P	L	BL, FA, TF
Strain sensitive	P	L	FA
Sonar	A	V	F, TF
Radar	A	L, V	F, LOS
Laser radar	A	L, V	F, LOS
Pressure	P	L	BL, TF
Interior			
Pressure	P	P	BP, O
Break-wire	P	L	BP
Glass break	P	L	BP
Both			
Active infrared	A	L, V	BP, F, FA, LOS
Passive infrared	P	V	F, IM, LOS
Electric field	A	L, P, V	BP, F, FA
Capacitance	A	V	BP, F, FA
Microwave	A	V	F, IM, LOS
Video motion	P	V	F, IM
Vibration	P	L	BL, BP, FA
Electromechanical	A, P	L, P	BP, O
Thermal imaging	P	V	F, IM, LOS

[a] Active (A), passive (P).

[b] Line sensor (L), point sensor (P), volumetric sensor (V).

[c] Buried line (BL), boundary penetration (BP), free standing (F), fence associated (FA), interior motion (IM), line of sight (LOS), object (O), terrain following (TF).

4.128. Assessment by personnel includes using observations from guards, response forces or other personnel, depending on the facility security plan. Assessment by personnel might be needed if the video assessment system is not operable (e.g. due to maintenance or unsuitable weather conditions) or not adequate for the particular situation, or in the absence of such a system. Assessment by personnel relies upon the personnel being in the right location to observe, and the probability of a correct assessment by personnel decreases as the time to arrive at that location increases. Since assessment variables are dependent upon PPS

and facility conditions, the probability of assessment has to be considered when determining the probability of detection.

4.129. Alarm prioritization technologies can assist in the assessment of alarms. When multiple simultaneous alarms occur, the alarm system might have the capability to prioritize alarms automatically in the order of importance for the CAS.

Video technology

4.130. Examples of applications of video technology include the following:

(a) Alarm assessment to provide timely and accurate determination of the threat to the facility. This enables the initiation of an appropriate response if necessary.
(b) Intrusion detection, including the use of video motion sensors and surveillance cameras.
(c) Access control for personnel and vehicles. Face recognition software can be used to support personnel identification. Video technologies can also support remote operation of security equipment (e.g. automatic gates or vehicle stopping equipment).
(d) Detection of prohibited items, including under vehicle surveillance equipment and endoscope inspection cameras.
(e) Situational awareness, to provide information to the response forces on adversary actions and locations during an attack.
(f) Pre-event video provides information from before and during the time when an alarm was initiated, for use in assessment of the alarm.
(g) Post-event video provides information about the adversary and any tools the adversary is carrying and may provide indications of the adversary's target, which can help the response forces to interrupt the adversary.
(h) Recorded video (pre-event and post-event) can be used after a detected event, to support investigations and prosecution.

4.131. To be effective, these different applications need different degrees of video resolution. The video resolution determines the extent to which the detail in an image can be seen, and is dependent on the components of the video system (including the lens, camera, transition system, recording equipment, data compression, the monitor on which the output is viewed). Resolution can be lost at several points in the system (see Fig. 11). The video system should be tested frequently as a system to verify that the combination of components provides the necessary resolution under all operational conditions (e.g. different configurations or bandwidth fluctuations). The type of assessment for which a particular camera

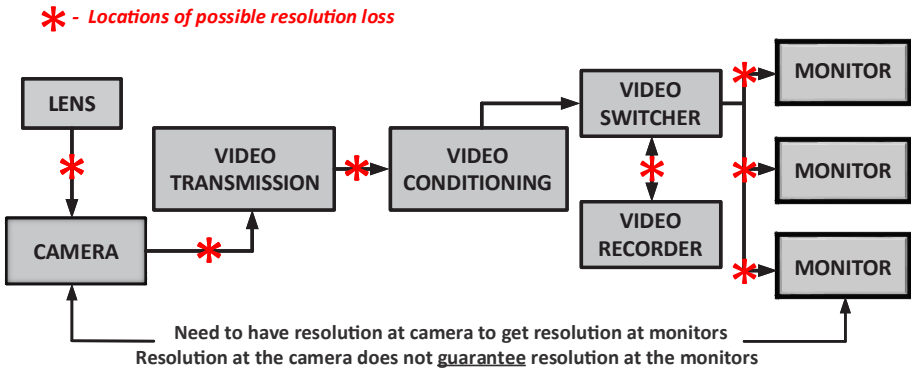


FIG. 11. Camera system diagram illustrating where resolution can be lost.

location is intended to be used should determine the resolution needed, and the system should be selected to provide this resolution.

4.132. Three generic levels of resolution to consider are those for detection, classification and identification, although these levels of resolution also depend on the intended subject for assessment and the level of assessment needed (e.g. classifying an image as human rather than animal needs lower resolution than identifying a specific human).

4.133. The overall resolution of the system should be evaluated by considering the camera, lens, video transmission system, video recording system, compression methods and monitor screen resolution. Commercially available security video systems might offer resolutions as low as 10 pixels/m, but this is normally not sufficient for physical protection purposes. Sufficient video resolution is not only a factor of pixels/m, but is also dependent on factors such as imager sensor size, field of view, background and bandwidth. The resolution needed depends on the purpose. In general, to sense the presence of an object in an area of interest, a resolution of 25 pixels/m is suggested. An increased resolution of about 125 pixels/m enables classification of an object and therefore provides sufficient information to determine what is present by class (animal, blowing debris or person). Identification of a person will most likely need even higher resolution of about 250 pixels/m to be sufficient to uniquely identify an individual based on details of appearance.

Cameras

4.134. The basic function of the camera is to convert an optical image of the physical scene into an electrical (video) signal, suitable for transmission to another location for display. Most cameras use solid state components and have a variety of features to optimize the image produced by the camera. The manufacturer specifies the format and the resolution of the images produced by the camera.

4.135. Cameras should be mounted on a stable tower or mount at a height consistent with the intended use of the system. For example, a face recognition camera may be mounted at head height, whereas a camera used for surveillance of an area may be mounted at a considerable height to provide an extended view. Considerations in installing cameras include the field of view, the objects within the field of view, accessibility for maintenance (e.g. use of collapsible towers) and protection from adversaries, both insider and external and from the sun. For example, cameras can be protected from both insider and external adversaries by placing them between the inner and outer perimeter fences and restricting access to that area to authorized maintenance personnel. Effects from the sun rising and setting can be difficult to mitigate, as the times of these change. Placing cameras higher to view downwards can help to mitigate these effects, but this shortens the length of the sensing zones.

4.136. Using the lens iris control, exposure time and electronic signal amplification, most cameras produce an image of the average brightness of the scene. Bright spots in the camera's field of view increase the average brightness, causing the camera to compensate by reducing the average video signal output. This tends to cause the darker portions of the image to become too dark. The number and intensity of bright and dark areas in the camera's field of view for which the camera can compensate is limited: this is known as the camera's dynamic range.

4.137. Under low light conditions, most cameras automatically compensate for the lack of illumination by increasing some combination of the exposure time (shutter control) and amplifier gain, taking account of the overall brightness level set by the user. Cameras with auto-iris lenses compensate for changing light levels by opening or closing the lens iris. Some digital cameras allow the compensation for illumination level to be programmed by the user. The order in which iris control, shutter control and amplifier gain are used to control illumination can also be prioritized.

4.138. Frame rate is the number of individual frames, or pictures, in each second of video. Shutter speed is the amount of time that each individual frame is exposed. If the shutter speed is too long, the picture in the frame will be blurred. The denominator of the shutter speed should be approximately twice the number of frames per second being recorded.

4.139. Using shutter control for low light compensation causes the shutter to be open for longer exposure times. Long exposure times will lead to blurred images of moving objects while higher amplifier gain on very low light signals will produce grainier images, neither of which is desirable for video based assessment. Camera manufacturers often state camera sensitivity for different test conditions and camera parameter settings, including the minimum illumination level at the camera's imager considered to provide a usable picture. These camera specifications do not take into account the reduction in illumination level caused by the camera lens, so the amount of light that needs to enter the lens to achieve the minimum illumination level at the imager can be significantly higher than the specified level. The illumination and scene conditions during which the camera's sensitivity was determined might also not be documented in the camera's specifications. In addition to the minimum illumination level, the following information is needed:

(a) Condition of the output video (e.g. camera output, gain, exposure time);
(b) Transmittance of the lens (i.e. the percentage of incident light appearing at the front of the lens that passes through on to the imager);
(c) Lens f-number (i.e. the level of light reduction to the imager determined by the lens iris or aperture opening);
(d) Reflectance of the test scene (i.e. the percentage of incident light on a scene reflected back to its source).

4.140. In some cases, the sensitivity claimed by the manufacturer might be unrealistic and indicating better performance than can be achieved in actual installations. Unrealistically high scene reflectance, unacceptably long exposure times and an unfeasibly large lens aperture (low f-number) can all contribute to higher sensitivity being observed in tests than in real conditions. These parameters are also usually determined with the camera viewing a static scene: if the need to effectively observe motion is also considered, the actual camera sensitivity experienced might be significantly lower than that claimed by the manufacturer.

4.141. Camera imagers are sensitive to a specific region of the electromagnetic spectrum. If the output spectrum (colour) of the illumination source and the camera imager's spectral response are not compatible, either more light will be

needed to provide adequate illumination or a different light source will be needed. The physical differences between the imagers will adversely affect the low light performance (sensitivity) of the camera, typically by a factor of two.

4.142. The camera imager needs to be sensitive to the colour of light produced by the lighting source. Lower illumination is needed for a black and white camera than for a colour camera to produce the same level of video output. If a near-infrared energy source is used, a black and white camera can provide a visible video image even if the near-infrared light was not visible to the human eye.

4.143. When using video systems for alarm assessment, more than one camera should ideally be used to assess an alarm. For example, if one perimeter sensor covers a long distance, a number of cameras might be necessary to allow assessment of alarms in the entire detection area. Automatic activation of the cameras in the neighbouring detection zones, especially where sensor coverage overlaps, might also be beneficial.

4.144. Factors affecting the operability of the camera should also be considered and addressed. For example, in severe cold climates, a mechanism can be used to heat the camera housing to maintain a minimum temperature. Measures might also be needed to prevent a buildup of snow and ice, which could affect camera performance.

4.145. Some video alarm assessment systems use a smaller number of cameras but employ pan–tilt mounts and zoom lenses (often referred as pan–tilt–zoom cameras). These cameras can be rapidly redirected to view the area where an alarm occurred, often within a second or less. Older systems were manually controlled, but modern pan–tilt–zoom systems can be programmed with presets that cause the camera to automatically turn to the alarm scene as soon as the alarm is received. This can allow as many as four or five alarm zones to be covered by one camera. However, the speed of reaction is crucial: if the camera reacts too slowly, an adversary could be out of the field of view before the camera is focused on the area of the alarm.

4.146. There are some significant disadvantages associated with the use of this approach. If there are multiple simultaneous alarms within the zones covered by a single pan–tilt–zoom camera, the system cannot record all of these scenes and prioritization is needed to determine which alarm the camera will rotate to view. The use of pan–tilt–zoom cameras also precludes the use of pre-alarm recording, since the camera will unlikely be aimed at the source of an alarm immediately

before the alarm. Finally, the mechanical pan–tilt mount may also need more frequent maintenance and repair.

4.147. A fixed camera should be used in preference to pan–tilt–zoom cameras for immediate detection assessment, but pan–tilt–zoom cameras could be useful for post alarm monitoring of an event or area. They are also useful when tracking an adversary beyond the alarm location.

4.148. Thermal imaging cameras may also be used as part of a CCTV system. These cameras allow detection, recognition and identification of different types of object under unfavourable meteorological and lighting conditions at different distances.

Lenses

4.149. The main parameters for selecting camera lenses are interdependent variables (e.g. format, focal length, field of view, f-number). The choice of values depends upon the designer's objectives, including the manner in which the video system will interface with other security systems. The f-number and iris setting will determine the area that is in focus, also known as the depth of field. For any camera, the assessment zone needs to be in focus, or have a depth of field that allows images of the necessary resolution to be obtained under all lighting conditions.

4.150. Other features can enhance the performance of the lens. Some lenses have automatic iris aperture controls, including neutral density filters in the centre of the lens, which work with the camera circuitry to allow for automatic adjustment of the light levels. This allows for a greater reduction of bright light when the iris aperture is smaller than the neutral density filter. Some lenses have special coatings to either enhance or filter out certain wavelengths of light to optimize the lens performance for specific purposes. For example, some lenses enhance the transmission of near-infrared (wavelengths of 800–1100 nm), which can be used by solid state cameras.

4.151. Lenses should be selected to provide the necessary resolution and field of view. When a video system is being designed for perimeter use, the 'distance and width approximation' may be used to determine the maximum zone length that can be assessed with a particular camera and lens (see Fig. 12). The lower field of view (typically shown at the bottom of the monitor) is normally narrower than the zone width, and the upper field of view is normally wider than the resolution

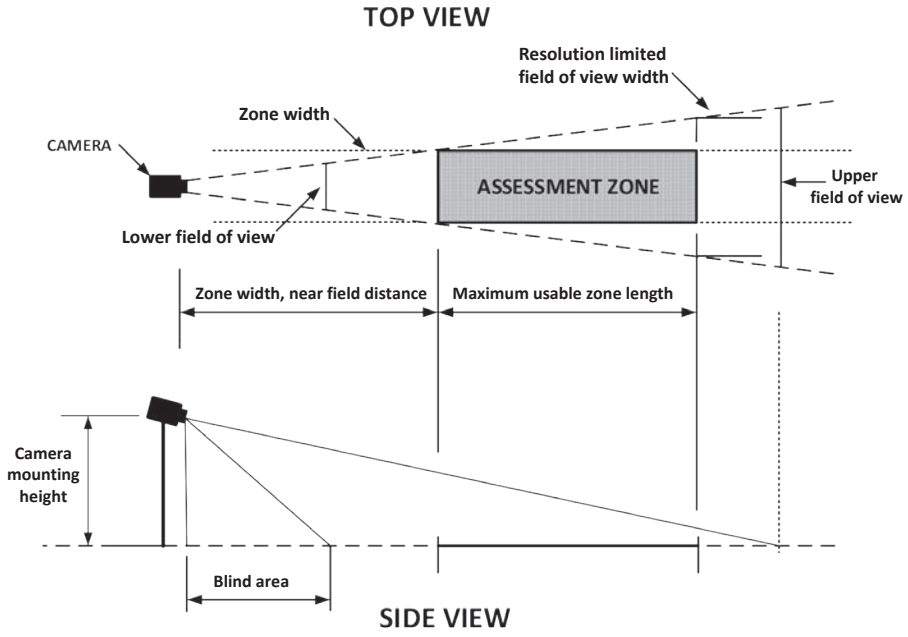


FIG. 12. Perimeter assessment zone geometry.

limited field of view. Between the camera and the lower field of view, the camera cannot see a blind area.

Video transmission system

4.152. The function of a video transmission system is to connect cameras to the CAS video display monitors with no undesirable effects on the video signal. A typical system comprises cameras, wired or wireless transmission systems, processing equipment and storage and display components. For the majority of applications a lighting system will also be needed. Video systems may be analogue, digital or a combination.

4.153. Video transmission from multiple cameras may be networked in several ways, for example:

(a) Coaxial cable (digital and analogue);
(b) Fibre optics (digital and analogue);

(c) Microwave links, optical (infrared) or other wireless systems (digital or analogue);
(d) Network connection (digital).

4.154. Figure 13 shows an analogue system, for which the display monitor should have a resolution closely matched to that of the cameras being used in the assessment system. For digital systems, the display monitor resolution should be at least as high as that of the camera imager.

4.155. A digital system is typically set up using components (cameras, storage devices, display monitors) connected by a network. System designers need to choose an analogue or digital system to obtain the picture quality (including resolution), availability and reliability needed for the application. Security considerations for video transmission networks are addressed in Section 6.

4.156. The capacity of the digital network needs to be considered when designing such a system. The number of cameras and the frame rate and resolution of the displayed images affect the effectiveness of the video system: the more cameras on the network and the higher the frame rate for the cameras, the higher the likelihood that the video will be slow or will 'freeze'. Digital compression techniques can improve network capacity but usually adversely affect the resolution at the display monitor.

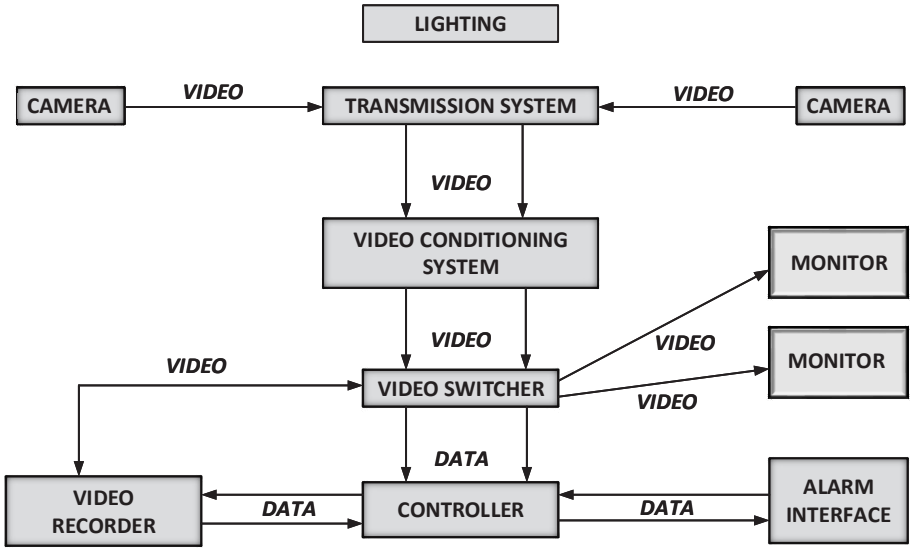


FIG. 13. Analogue components of a video system.

4.157. Hardwired transmission uses either electrical signals carried by copper cable or optical signals carried by fibre optic cables. The use of copper cables (e.g. coaxial) might lead to some degradation of the signal if it is not conditioned with equalizers, isolation transformers or clampers. In comparison, fibre optic cables suffer less from signal loss but might need additional components for analogue–digital conversion of the signal.

4.158. Ground loops, induced noise and surges from lightning can damage electrical equipment but do not occur with fibre optic cables. Fibre optic transmission does not need signal conditioning with equalizers, isolation transformers or clampers, but might need repeaters to provide sufficient signal strength for very long cables.

4.159. Many older analogue video systems use more cameras than there are display monitors in the CAS, so video switching equipment is used to connect multiple video signals to one or more monitoring devices (display monitors, video recorders). The associated alarm sensor system usually interfaces with the switching system in such a way that an alarm in any zone causes the associated camera output to be automatically displayed on a local monitor.

4.160. Types of analogue switching system include the following:

(a) Manual switching by push-button contacts, so the video signal is routed through the switcher with no electronic conditioning or timing.
(b) Sequential switching in which all camera outputs are scanned in sequence, usually with an adjustable scan rate or amount of time each image is displayed.
(c) Alarm activated switching in which the video signal from the camera in the alarm zone is automatically sent to the output regardless of the selected input before alarm activation.
(d) Remote switching, which involves multiple switching, some of which is done remotely before the signals reach the CAS.

4.161. Modern systems use digital multiplex software to manage camera images. A multiplexer is a device that selects one of several analogue or digital input signals and forwards the selected input as a single output signal.

Video recording

4.162. Video recording systems provide historical information for subsequent study, including using instant replay and stop action, to aid assessment and

to provide an audit trail. Video recording systems can use either analogue (i.e. video tape) or digital recorders. Digital recordings can also be used for real time assessment.

4.163. The number of cameras, the number of frames recorded per second (typically in the range 2–30 frames per second) for each individual camera, the resolution of those images and the storage time determine the storage capacity needed for video recordings. The amount of data recorded needs to provide a balance between the needs of the video system for use in assessment and the storage capacity available. For example, high overall video quality supports live playback for real time assessment, high resolution images may allow an adversary to be identified (rather than simply indicating that an adversary is present), and a high frame rate may help to assess the action of an insider, but all need more data to be stored. Video management systems can compress video data for storage and can automatically adjust the quality of the video images between alarm situations (high frame rates and resolution) and normal situations (low frame rates and resolution).

4.164. Digital video recorders can be controlled by a computer system, interacting with the sensor alarm monitoring function of a PPS, so that when a sensor generates an alarm, the recorder can be directed to play back pre- and post-alarm video from the camera covering the area in which the sensor is located.

4.165. The size of stored video files can be reduced by reducing the duration and frame rate of the recording and by compressing the files. To view a compressed recorded image, the file is first decompressed, but the detail in the image from the decompressed file might be degraded compared to the original image before compression. Overall image quality from recorded video data is therefore a function of camera resolution, frame rate, captured image resolution and the amount of compression applied.

4.166. Sufficient video displays should be installed in the CAS to allow effective, rapid assessment without interference from other system controls and outputs.

4.167. The video controller is the main interface between the interconnected PPS and the video system. This controller automatically controls the inputs and outputs of the multiplexer, keeps track of the recorder and displays the scenes on the display monitor. The video controller may be part of the alarm, communication and display software and hardware, which is usually integrated with digital and network recorder systems.

Lighting technology

4.168. Adequate security lighting is needed for areas or structures that form the perimeter of a nuclear facility where intrusion detection systems and assessment of alarms are used. Lighting may also be used to allow assessment of alarms in areas such as vital areas, nuclear material storage areas and inner areas, or areas containing utilities or critical infrastructure for physical protection.

4.169. Security lighting provides illumination for:

(a) CCTV (including video motion sensors) for detection (especially assessment of alarms) and surveillance of adversaries;
(b) Deterrence of adversaries;
(c) Areas of possible concealment;
(d) Access control points (e.g. to allow personnel and vehicle identification and detection of prohibited items);
(e) Guard and response force activities.

4.170. Security lighting helps to protect guards and response forces by reducing the possibilities of concealment by an adversary. When security lighting is poor, additional security posts, patrols, night vision devices or other provisions may be used.

4.171. The contrast between an adversary and the background should be considered when planning a security lighting system. For example, light colours on the lower parts of buildings and structures or on the ground surface might make an adversary wearing dark clothing more easily visible.

4.172. Any proposed lighting system should be planned in conjunction with other security systems, including CCTV and intrusion detection systems. The use of security lighting can also affect operational nuclear safety or conventional health and safety, and these interfaces and the associated priorities need to be understood. Provision should be made to ensure that lighting failures are reported and corrected in a timely manner: some systems provide an alarm when lighting fails.

4.173. Where lighting is not available or cannot be used, a thermal imaging camera can be used. This uses the thermal radiation emitted by objects to produce an image without lighting: all objects emit thermal radiation, which is not visible, and warmer objects (e.g. a human body) appear brighter in the image than cooler objects. The image produced typically looks like a black and white

picture, although some systems apply different colours to the image to represent different temperatures.

4.174. If local environmental laws or policies require that an operator reduce power consumption or use lower light levels, low light cameras, covert infrared illuminators, motion activated lighting systems and LED systems can be considered as low power alternatives.

Types of lighting system

4.175. The type of lighting system should be selected based on the security requirements for the facility. Four basic approaches can be used for security lighting: continuous, standby, movable and emergency.

4.176. Continuous lighting is the most common type of security lighting used. A set of fixed lights is arranged to continuously illuminate a given area during low light conditions with overlapping cones of light. Standby lighting has a similar layout but the lights are normally off during hours of darkness and are either automatically or manually turned on if suspicious activity is suspected by guards or detected by intrusion sensors. If used, standby lighting needs to be carefully managed, and can have undesirable effects (e.g. warning adversaries that their presence has been detected). Movable lighting comprises integrated groups of manually operated, movable lights and generators that can be operated where and when needed, during hours of darkness or otherwise. This type of system is usually used to supplement continuous or standby lighting or as a compensatory measure. Emergency lighting may duplicate any or all of the above systems, but operates when the normal power supply fails or other circumstances make the normal lighting system inoperative. Emergency lighting depends on an alternative uninterruptable power supply, such as installed or portable generators or batteries.

Illumination

4.177. Illumination may be either natural or artificial and is measured in lux. The human eye, when adjusted to low light levels and with good contrast between the subject and the background, can see an adversary at an illumination level of approximately 1 lux, but considerably more illumination is needed to recognize an individual. The human eye typically needs between 5 and 20 minutes to adjust to low light levels, depending on the person’s age, and this should be taken into account when planning a patrol strategy for guards.

4.178. To ensure that sufficient natural illumination is reflected back to the camera during low light conditions and that adversaries are likely to contrast sufficiently with the background, the ground surface of the assessment area should be adequately reflective.

4.179. Illumination and reflection are typically measured using a light meter at a specified distance from the assessment area, usually 15–30 cm above the ground. The average illumination in an area covered by a number of lights is calculated from several measurements at equally spaced locations across the area. This measure is known as 'horizontal scene illumination' or simply 'scene illumination'.

4.180. The average scene illumination should be sufficient to support video assessment and visual assessment by guards and response forces. For example, for an area clear of obstructions, an average scene illumination of 10 lux with a ground surface of 25–35% reflectivity may provide sufficient light for assessment purposes.

4.181. The light-to-dark ratio within an area also influences the ability to make assessments. Figure 14 has a light-to-dark ratio of approximately 20:1 and shows significant blind spots. These are greatly reduced in Fig. 15, which has a light-to-dark ratio of approximately 4:1. Lighting with a light-to-dark ratio of 6:1 or less will typically provide sufficient contrast for assessment purposes. At least 75% of the camera's field of view should ideally have at least the minimum average illumination and an acceptable light-to-dark ratio.

4.182. Since most lighting applications use bulbs that produce visible light, errors can be made in estimating the light needed if the camera imager spectrum, which extends into the infrared part of the spectrum, is not considered.

Lighting layout

4.183. To prevent cameras from pointing directly into a light source, all light fixtures should ideally be located above the camera and out of its field of view (see Fig. 16). To avoid potential effects of backscatter by dust or fog, the light source should not be mounted directly above the camera. A sun shield that extends beyond the front cover glass of a camera enclosure can also help to minimize such effects. Perimeter light poles should be inside the perimeter, so they cannot be used by an adversary to bridge over the perimeter fence.

4.184. Modelling a proposed lighting system can be used to estimate scene illumination levels and light-to-dark ratios. The design of the lighting system

should ideally be physically tested before installation in the final perimeter lighting configuration. This test can be achieved by installing at least five fixtures (for single row installations) and measuring the illumination based on the criteria suggested above.

FIG. 14. Scene with a high light-to-dark ratio of approximately 20:1. (Courtesy of Sandia National Laboratories).

FIG. 15. Scene with a low light-to-dark ratio of approximately 4:1. (Courtesy of Sandia National Laboratories).

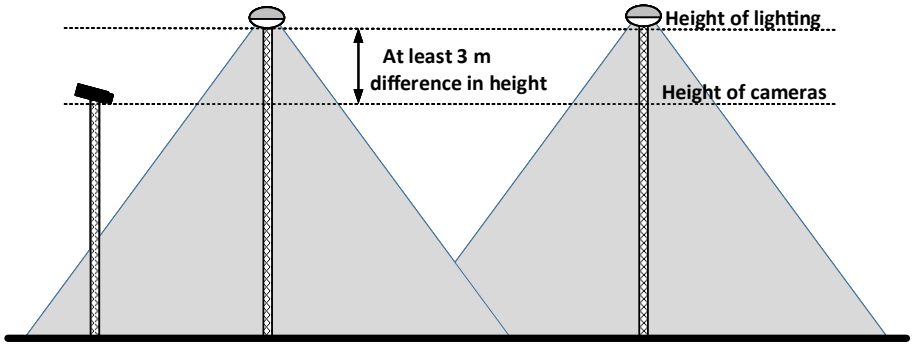


FIG. 16. Suggested height difference between exterior lighting and cameras.

4.185. Adjustment and modification of the entire lighting system after installation is likely to be necessary to achieve the intended performance. For example, camera testing will often show previously unidentified reflections or bright spots that need to be corrected.

4.186. A similar layout of lighting should be considered for interior applications. Normal interior lighting levels allow the use of a video camera with lower sensitivity than is needed for exterior applications. Near-infrared illumination sources can be used internally to provide a measure of covertness for the video surveillance.

Lighting requirements

4.187. Perimeter lighting will need to meet specific requirements depending on whether the perimeter is isolated, semi-isolated or non-isolated. Isolated fenced perimeters are fence lines around the area where the fence is located 30 m or more from the buildings or operating areas. Semi-isolated fenced perimeters are fence lines where approach areas are clear of obstructions for 20–30 m outside the fence. Non-isolated fenced perimeters are fence lines immediately adjacent to operating areas. For example, lighting may be controlled so that guard patrol routes are in relative darkness while the clear zone or area under surveillance is illuminated. The State or operator's safety requirements should be considered when guard patrols are conducted in areas with low light levels (e.g. to avoid tripping hazards).

4.188. Lighting requirements for access control points will be different. Staffed access control points for pedestrians need to have sufficient lighting to enable recognition of individuals and examination of credentials. The requirements

may differ for access points that have automated access control systems. Vehicle entrances may need additional lighting to facilitate searching vehicles and identifying occupants. Less commonly used access points may have the same lighting levels as the surrounding perimeter with the option of increasing the levels when needed. Guard posts at access control points will need interior illumination levels that enable the guards to see approaching vehicles and pedestrians but minimize the extent to which people outside can see into the building.

4.189. Other areas and structures within the facility perimeter may need lighting, such as open areas, storage spaces, working areas, piers, docks and other sensitive areas and structures, each of which may have their own lighting requirements. Open unoccupied areas and outdoor storage spaces (e.g. material storage areas, railroad sidings, parking areas) should normally be illuminated to allow guards on patrol sufficient view of the area. An open area adjacent to a perimeter should normally be illuminated according to the same requirements as the perimeter. Lighting in outdoor storage spaces should provide adequate lighting in aisles, passages and recesses to eliminate dark areas where an adversary could hide.

4.190. Illumination is especially needed for water approaches, piers and docks if these are present at a facility. Searchlights may be used to illuminate an area of interest or for specific reasons as needed. Such lighting should not violate rules and regulations governing use of the sea or inland waterways (i.e. it should not be glaring to pilots).

Lamp types and characteristics

4.191. The choice of lamp type to provide lighting should take account of the characteristics of the assessment system and other security lighting (e.g. if assessment depends on infrared equipment, appropriate lighting is needed). Common lamp types used for security purposes include the following:

(a) Incandescent: Light is emitted from a heated filament inside an evacuated globe.
(b) Fluorescent: Light is generated by an electric arc in a tube filled with low pressure mercury vapour. The vapour emits ultraviolet radiation that is converted to visible light by fluorescent powder on the inner surface of the tube.
(c) High intensity discharge: Light is generated by direct interaction of an arc with a gas. Gases used in high intensity discharge lamps include mercury vapour, metal halides and high and low pressure sodium vapour. Argon is

usually added to aid ignition, and other powders or vapours may be added to improve colour rendition.

(d) LED: Light is generated from a solid state diode. LED lamps usually contain a cluster of LEDs within a suitable housing.

(e) Near-infrared: Light is generated from either LED clusters or incandescent bulbs, and external filters are used to remove the visible light.

Alarm stations

4.192. The function of a CAS (or an alarm monitoring station if a CAS is not necessary) is to provide continuous monitoring of alarms, assessment of alarms based on CCTV, CCTV surveillance, and communication with guards, facility personnel and response forces (see Fig. 17) [1, 2]. In some cases, CAS personnel operate remote access control equipment. A CAS also maintains records used for a number of purposes, including investigation of incidents. For facilities with Category I or Category II nuclear material or the potential for high radiological consequences, as determined by the competent authority, to result from sabotage, the CAS should be located in the protected area, permanently staffed and access to it should be controlled. Although a CAS is not recommended for other nuclear facilities, the term CAS is used in this publication for simplicity to refer to the place at which the above functions are performed.

FIG. 17. Central alarm station. (Courtesy of Sandia National Laboratories).

4.193. A CAS should be designed and operated in a manner similar to a nuclear reactor control room, applying the same approaches to managing human–machine interfaces. Although developed for process manufacturing, the American National Standards Institute and International Society for Automation standard ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries [22], may be considered when designing a CAS for a nuclear facility.

4.194. All physical security systems (including intrusion detection systems, access control systems, CCTV assessment and surveillance systems) should be integrated into the CAS and appropriately managed. The CAS should provide the ability to monitor and assess alarms from all sensors, and be equipped with a dedicated, redundant, secure and diverse network for internal and external voice and data communication. The following recommendations help the CAS perform its functions effectively:

(a) All sensors installed in the facility should transmit their signals directly to the CAS.
(b) If any alarms are not monitored in the CAS, clear procedures should be in place to ensure adequate communication to the CAS for immediate response. This should not be dependent on assessment by facility personnel.
(c) Facility personnel should be able to provide information to the CAS about incidents including unauthorized access, introduction of prohibited items, the activation of safety alarms (e.g. radiation alarms) or any other suspicious incident or activity.

Monitoring of alarms

4.195. The primary tasks of personnel in a CAS include monitoring alarms from sensors, ensuring assessment of all alarms received, and initiating appropriate response actions when necessary. All duties of CAS personnel should be performed in compliance with approved procedures.

Assessment and surveillance

4.196. Alarm assessment should be performed directly from CCTV images and/or indirectly by guards or response forces assessing the cause of the alarm and reporting to the CAS. The CAS should use CCTV and any subsequent alarms to track (i.e. provide surveillance of) the cause of the alarm. The adversary's path and detailed descriptions of their movement, appearance, weapons and actions should be provided to the guards and response force. The use of well positioned CCTV systems equipped with pan–tilt and auto-zoom features can enhance

surveillance capability. Video technology that includes instant replay and stop action features, prerecording and an ergonomic human–machine interface enables real time assessment.

Communication

4.197. Communication systems between the CAS, guards, response forces and facility managers should be dedicated, secure, redundant and diverse, immediate and reliable. CAS personnel should also effectively communicate with, and provide situational awareness to, other organizations such as emergency response organizations and PPS maintenance organizations. CAS communications are used to initiate a response and provide information to personnel assigned command and control functions during a response to nuclear security events.

Access control

4.198. An access control system provides monitoring and control of the movement of people around a facility, and complements other security and emergency management systems.

4.199. Access control systems may be integrated into the CAS as part of a security network or used as an independent, standalone system. In either case, any networked system should be secure.

4.200. Access control systems collect and store data on authorized access through an access control point and unsuccessful attempts to obtain unauthorized access. It can also be configured to display access requests or to provide automated control functions. The intrusion detection system should be integrated with the access control system so that authorized access does not generate nuisance alarms.

4.201. Some access control systems are configured to allow a person to verify remotely whether a person is allowed access to an area and, where appropriate, allow access, for example by remotely releasing the final lock on the door. In these cases, the access control system may display a stored photograph of the individual requesting access and CCTV images of the relevant area. The operator can then determine whether to allow or deny access.

Record keeping

4.202. All notable incidents relating to access control, alarms and video assessments should be recorded and archived for future review. Interconnected

security systems (alarms, cameras, recording systems) should have a time stamp feature so that all elements of the system use the same time reference.

4.203. The ability of the access control system to record where and when an individual has entered and left particular areas of the facility is of value for both security purposes and safety management. For example, access control records may be used to check that all individuals who were in a building are accounted for following an emergency evacuation.

4.204. Automated alarm logs can also be used for the collection and analysis of false and nuisance alarms, and trends can be analysed to support maintenance schedules. Records of alarm and video assessment can also be used for investigations following nuclear security events and emergencies. Written and automated operator records can also be examined to verify that alarm tests were performed with the required frequency and that compensatory measures were initiated when needed. Information acquired at the CAS should be stored in a secure manner.

Human interface

4.205. The CAS should be permanently staffed by authorized personnel whose trustworthiness and aptitude has been verified through careful selection, and who have the appropriate skills and knowledge to undertake the assigned tasks. Measures such as a two-person rule or remote monitoring may be applied in the CAS to reduce the insider threat, and may be required for some CAS functions, such as putting a sensor into access mode (non-secure) or remotely opening a high security door.

4.206. A CAS should be staffed with a sufficient number of personnel to monitor and assess alarms and initiate a response when needed, and to receive and assess information from other sources. During a nuclear security event, CAS personnel should have the capability to communicate details of the incident to the facility management and to advise appropriate facility personnel on any response needed.

4.207. CAS personnel should be familiar with security technologies and extensively trained and tested before being assigned duties. Typically, CAS personnel are guards or response force members, who have the necessary knowledge and understanding of the facility, security operations, procedures and contingency plans. Guidance on contingency plans is given in IAEA Nuclear Security Series No. 39-T, Developing a Nuclear Security Contingency Plan for

Nuclear Facilities [23]. The functions of the CAS and its personnel should be regularly exercised.

Human factors

4.208. A first step in designing the systems within the CAS is to identify the functions that the personnel will need to perform and the interfaces needed to support these functions. Information such as system status, nuclear facility layout, alarm status, and video display and access control information might need to be displayed to support these functions. Careful consideration should be given to when and how such information is displayed to the operator (e.g. always, upon alarm or upon request) and when it should not be displayed, such as when an alarm is associated with a door operated by an authorized person. This might change depending on activities in the facility at different times of the day.

4.209. The alarm assessment process depends crucially on human decisions. A large nuclear facility might have several hundred cameras and sensors to monitor, all of which can generate alarms. The ability to quickly and accurately initiate appropriate action depends on the CAS personnel's ability to interpret the data and make appropriate decisions. The CAS console should be designed to prevent overloading CAS personnel with too much information at once. For larger systems, multiple operators, each with their own station, may be used to effectively monitor and maintain control of the security system, but in such cases the relationships and interactions between the operators and their equipment need careful consideration in planning and design. If a single operator is assigned to the CAS, the system may be designed to monitor the state of health of the person and to alert other appropriate personnel if the operator is incapacitated.

4.210. The layout of hardware and software systems should be considered carefully when designing a CAS. The work area should be comfortable and easy to use for the number of operators expected to be present. The operators should be able to see the necessary equipment, displays and each other, to hear communications and alarm warning indicators and each other, and to operate computer controls and communication equipment.

Layout and design

4.211. The work area of the CAS can be considered as a set of zones, of different accessibility and visibility. All displays and controls should be given adequate space to allow them to be used for their intended function. Primary displays should be clearly visible from the operator's normal working position without

a need for much eye or head movement. The operator should be able to control all of the necessary functions rapidly and accurately. Techniques such as variable letter sizes, shaded backgrounds for contrast and the use of colour to improve the visual presentation of information should be considered.

4.212. The designer should choose input devices (e.g. mouse, keyboard, simple push-button) that are most suitable for the intended function. Communication equipment, such as microphones and telephones, should be within easy reach of operators. The location of support equipment should be chosen based on its importance and frequency of use.

4.213. Additional design considerations include techniques to organize and manage the information displayed to make operator interpretation easier and action more effective. Techniques for managing the equipment in the console include the following:

(a) Audible signals to alert the operator that an alarm has occurred, with different sounds to indicate a different class or priority of alarm.
(b) Colour coding (or a flashing symbol) on the screen for emphasis or to assist in categorizing information (see Fig. 18).
(c) Separate computer monitors for graphic and text displays for different types of data.
(d) Multilayer graphics with links between the layers. For example, a floor plan may indicate there is an alarm in a particular room (see Fig. 19), and selecting the link to that room brings up a display of the room and the sensor producing the alarm.
(e) Text displays with descriptions or dialogue boxes providing additional information (see Fig. 20).

4.214. The alarm management system should be configured to distinguish between and prioritize alarms based on their location (e.g. alarm in a sensitive area before a perimeter alarm) and purpose (e.g. intrusion, system failure, loss of power, unauthorized activity or tampering). This system should provide alarms in the order in which they occurred or, for assessment of multiple simultaneous alarms, according to established priority based on the importance of the asset being protected. Alarms are displayed to the operator in order of decreasing priority, but all alarms are eventually assessed. For example, in a perimeter intrusion detection system, the alarm priority may be established by taking the following into account:

(a) The number of sensors in a given zone generating an alarm;
(b) The time between alarms in the zone;

FIG. 18. Console alarm text screen. (Courtesy of Sandia National Laboratories.)

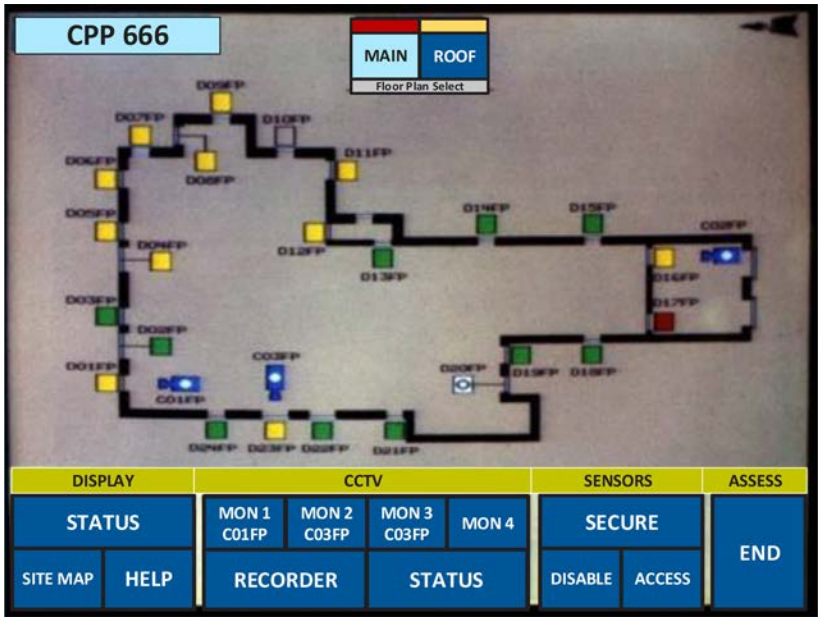


FIG. 19. Facility floor plan map screen. (Courtesy of Sandia National Laboratories.)

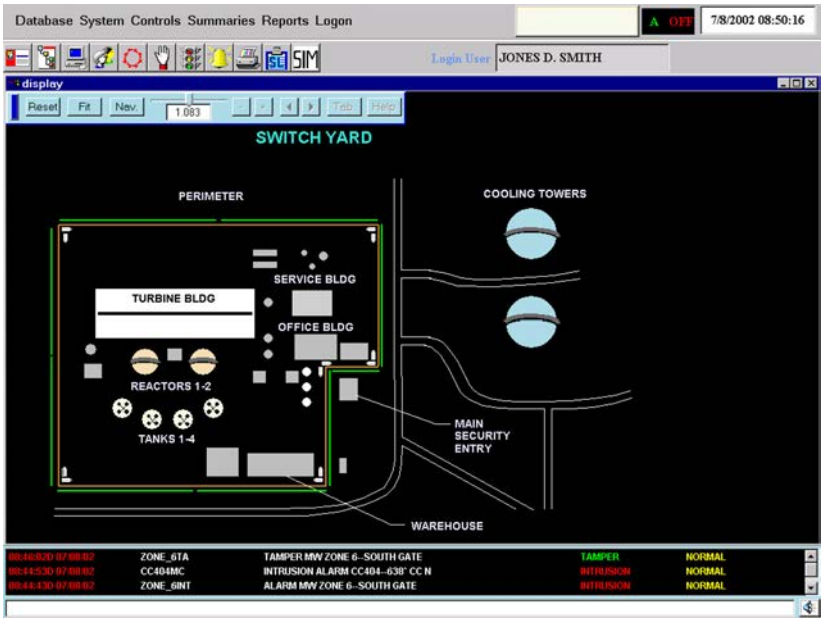


FIG. 20. Floor plan with alarm sensor detail display. (Courtesy of Sandia National Laboratories.)

(c) The order in which the alarms occur in relation to the physical configuration of the sensors;
(d) The presence or absence of alarms in adjacent zones.

4.215. The CAS for facilities with Category I or Category II nuclear material and high radiological consequences facilities should normally be located away from the perimeter boundary inside a hardened structure (e.g. bunker). Consideration should be given to locating the CAS away from the exterior walls of the building in which it is housed to increase its protection against direct assault or stand-off attack. Access to a CAS needs to be strictly controlled. Methods of access control can be manual, for example an operator releases the entry door upon verification of identity by video, or through automated systems. To prevent unauthorized entry by following an authorized individual into the CAS, two interlocking doors covered by CCTV, with enhanced access control, may be used.

4.216. Computer security measures should be applied to the CAS systems, such as controlling access to networked equipment and controlling and detecting access to information [7, 21].

4.217. The CAS should be able to continue to function during scheduled and unscheduled outages, nuclear or radiological emergencies and nuclear security events. Systems associated with the CAS should be redundant, diverse and protected against tampering, to the extent possible. The power supply to the CAS should have at least two independent sources, equipped with uninterruptible power supplies and, when necessary, a backup generator.

4.218. As a CAS is a potential single point of failure for a PPS, it is a good practice to establish a backup station that could take over the CAS's functions if it could not be used. For example, due to hardware or personnel failure, attack on the CAS or the need to evacuate the CAS (e.g. due to fire, earthquake, flood or release of radionuclides). The backup functions should include the monitoring and control of alarms, CCTV and communications. The backup station should be geographically separate from the CAS and in a location that can be accessed when needed, and should be tested regularly.

Voice communications systems

4.219. Reliable voice communication is needed between the CAS, emergency personnel, facility personnel, guards and on-site and off-site response forces. This should include the following:

(a) The ability to communicate at all times and under different conditions (e.g. in both normal and emergency situations);
(b) The ability to use a secure communication method when needed;
(c) The ability to communicate in a timely way with competent authorities and off-site response forces when necessary;
(d) A secondary or alternative method of communication for when the primary method is unavailable.

4.220. Communications systems should be designed to be difficult to compromise, by including multiple modes of communication such as two-way radios, mobile telephones, intercoms and landline telephones. Many voice communication systems operate over a computer network that may use wireless technology to transmit the signals. Security of such networks is addressed in Section 6.

Radio systems

4.221. Guards and response forces commonly use a system of hand-held radios, battery operated and operating at low power. These are easy to use and need little infrastructure, other than an electricity supply to charge the batteries

periodically. A typical radio can operate on any one of several frequencies or channels. The maximum range for reliable communication between two radios is 2–5 km depending on terrain, facility layout and the condition of the radio battery and antenna. More powerful transmitters and more sensitive receivers, commonly called base stations, can be used at alarm stations and fixed posts. Mobile vehicle mounted systems are also used: these can extend the range of reliable communication to more than 20 km. Radio systems used for response force communications usually operate on dedicated channels of a specific frequency, using narrow band frequency modulation and clear voice transmission (i.e. voice transmissions are not encoded or scrambled).

4.222. Clear voice radio systems have disadvantages, particularly their susceptibility to interception, deception (e.g. an adversary monitoring radio communications to learn protocols and sending false messages to disrupt response) and jamming (transmitting signals on the frequency channel of a communications system to mask the desired communications). Encrypted voice radio systems are more secure (e.g. more resistant to interception or the transmission of deceptive messages). Radiofrequency systems are vulnerable to jamming because the jamming signal can be transmitted from a remote location. A communications network can be made more resistant to jamming by using higher powered radios, which need higher powered jamming equipment, more sophisticated radio technologies or multiple communications systems. Encrypted radios by themselves do not prevent jamming, as the encrypted signal can be jammed in the same way as a clear one. More secure radio systems, which are more resistant to jamming, are more complex and expensive, and typically reduce the battery life of radios and suffer from more noise in the communication channel, reducing its effective communication range.

4.223. Depending on the facility configuration, its size and the types of building on the site, radio systems can suffer from a loss of signal, and increasing the signal from hand-held units with a radiofrequency repeater might be necessary. A radiofrequency repeater receives voice transmissions from the hand-held units and transmits them on a separate frequency to all other units within the system. A repeater placed at an elevated location can also increase the range.

4.224. To ensure that guards and response forces can communicate during a nuclear security event, a variety of different communication methods should be available. This may include systems used routinely for other purposes, such as landline telephones and intercoms, as well as systems specifically for emergencies. A diverse set of communication methods can create a system that is robust, reliable and resistant to interception, deception and jamming. Radios

may also be equipped with ‘duress alarms’ that transmit an alarm to alert the CAS that the person operating the device might be transmitting misleading messages under duress.

Search systems

4.225. People, vehicles and materials entering or leaving security areas may be subject to search by guards, dogs and search systems using technologies such as metal, radiation and explosive detectors. Searches on entry are usually to prevent the introduction of prohibited articles. Searches on exiting are primarily to prevent unauthorized removal of nuclear material. If an automated search system or dog raises an alarm, guards may perform a manual search to determine whether the alarm is a nuisance alarm or a valid alarm and, if necessary, initiate a response.

Manual searches

4.226. A manual search is typically a secondary screening technique used to search personnel, packages and vehicles after an initial alarm has been generated. The effectiveness of manual searches by guards depends on their training and procedures: in particular, guards need to be able to identify the types of prohibited item being sought, for example, their likely size, mass and shape. In principle, any item can be searched by hand, from small packages to people, vehicles or large shipping containers.

Vehicle searches

4.227. Because vehicles are difficult to search thoroughly, the operator may require vehicles to remain outside the facility boundary. If vehicles are allowed on the site, an access control portal or ‘vehicle lock’ can be used to isolate a vehicle while it is searched (see Fig. 21).

Metal detection

4.228. Metal detectors are typically used to search personnel at entrances and exits, and can be divided into two broad categories:

(a) Active metal detectors that transmit electromagnetic energy and detect metal by sensing the response of the transmitted field to the presence of the metal object.
(b) Magnetometers that sense local distortions in the Earth’s magnetic field caused by the presence of ferromagnetic materials.

FIG. 21. Vehicle access control portal. (Courtesy of Sandia National Laboratories.)

4.229. Some forms of nuclear material and shielding materials cannot be detected by simple metal detectors, therefore other metal detection technologies, notably pulsed field and continuous wave detectors, are commonly used in portals and hand-held devices.

Metal detection portal

4.230. A steady state sinusoidal signal is applied to the transmitter coil at one side of the detector arch. This coil produces a magnetic field of low strength (typically 50 μT or less). The receiver coils are mounted on the opposite side of the arch so that a person being screened passes between the transmitter and the receiver coils. The signal is detected by the receiver coils and is then analysed. If there is no metal present within the arch, there is no change in the signal over time.

4.231. In a pulsed field metal detector, low inductance transmitter coils produce very short pulses of magnetic energy (as short as 50 μs), 200–400 times per second. During the pulse, the received signal is ignored, but following the end of each pulse, the received signal is analysed for a short time (typically a few tens of milliseconds). If there is no metal present in the portal, the output of the receiver is only the background electromagnetic noise (typically very low). If there is a metal object present, the magnetic pulse induces an eddy current in the metal, which decreases rapidly (as a function of the resistivity of the metal) but persists long enough to be present when the received signal is analysed. The signal is then further amplified and the phase detected, and if the signal exceeds a selected

threshold, an alarm is generated. Detectors based on this technique represent the large majority of metal detection portals in use today.

4.232. For screening individuals passing through search checkpoints, walkthrough portals can be used to screen large numbers of people for metal on both entry and exit.

4.233. Metal detector alarms should also be generated in cases of power line failure, equipment failure or tampering. The environment surrounding a metal detection portal can affect its performance, including the following:

(a) Moving metal objects, such as doors, within a few metres causing nuisance alarms.
(b) Static metal objects, including metal reinforcing rods in the floor, distorting the magnetic field and creating areas of higher or lower sensitivity.
(c) Electrical devices such as radios, X ray devices and computers operating in the vicinity of a metal detector, causing nuisance alarms.
(d) The floor under the metal detector moving when people walk through the area, causing nuisance alarms. Pipes carrying water in a wall or under the floor might also cause the metal pipes to move.

Hand-held metal detectors

4.234. Most hand-held metal detectors are based on continuous wave technology. These detectors generate a steady state magnetic field within the frequency range 100 Hz to 25 kHz. (Early metal detection portals were also based on this technique but these have been largely replaced by pulsed field detectors.)

4.235. Hand-held metal detectors need to be operated very close to the person being scanned. At the normal operational distance from the body, they are highly sensitive and can sense much smaller objects than can be sensed by a portal detector. In particular, they might be more suitable than portal detectors for screening of smaller amounts of metals that might be used to shield nuclear material being removed. The effectiveness of a hand-held metal detector is highly dependent on the technique used by the person doing the screening. Thorough screening following a well designed procedure can be very effective, but it takes a considerable amount of time. Hand-held detectors are therefore mostly used as a secondary method in cases where metal detection portals have generated alarms, and every screening point with a metal detection portal should be equipped with a hand-held metal detector.

Detection of explosives

4.236. X ray absorption or neutron activation and absorption methods are commonly used for detecting explosives in cargo and luggage. Such methods of explosives detection are not used in screening personnel.

4.237. Active and passive approaches have been developed for the trace vapour detection of explosives, typically using ion mobility spectrometry systems and trained dogs. Smaller packages are inspected for explosives using these approaches to sense the trace amounts of explosives on surfaces contaminated by persons who have handled explosives or where explosives have made contact. These methods are also typically appropriate for searching people.

4.238. Low energy millimetre wave technology can be used to search people, and X ray imaging methods can be used to search packages.

4.239. Bulk explosives detection devices measure bulk characteristics of materials to sense the presence of explosives. Such characteristics include the X ray absorption coefficient, the X ray backscatter coefficient, the dielectric constant, gamma or neutron interactions and microwave or infrared emissions. Analysis of measurements of these parameters can provide estimates of the mass, density, nitrogen content and effective atomic number of the material. While none of these characteristics is unique to explosives, they can indicate a high probability of the presence of explosives, and the false alarm rate for bulk detection devices can be low enough to allow for automatic detection of materials that may be explosives. If the system generates an alarm, an operator can carry out secondary screening (assessment) to determine whether explosives are present.

X ray absorption

4.240. In most cases, X ray bulk detectors for explosives are modified versions of scanners used to search packages. These devices therefore usually serve a dual purpose, and the package can be searched for weapons or other prohibited items and screened for explosives simultaneously. Simple single energy transmission X ray scanners do not provide enough information for automated explosives screening and need an operator's interpretation of the image. Dual energy scanners (typically around 100 and 160 keV) measure the ratio of received to transmitted energy at the two energies and, by comparison with known elemental attenuation coefficients, can calculate an effective atomic number for the region scanned. For display purposes, colours are added to the images to indicate materials of low and high atomic number, which can help personnel in interpreting the images.

Computed tomography scanners can extract enough information to calculate the material's mass, density and mass absorption coefficient. Analysis of the backscatter can determine a material's effective atomic number by examining the X ray energy scattered back in the direction of the source (mainly due to Compton backscattering, which is most effective for hydrogen rich materials such as explosives, plastics and food).

Neutron activation and absorption

4.241. Thermal neutron activation detectors and pulsed fast neutron absorption can also be used to detect explosives. Thermal neutron devices can determine the nitrogen content of a material: nuclear absorption of a thermal neutron by ^{14}N generates ^{15}N in an excited state, which is not stable and emits gamma radiation of characteristic frequency. The amount of radiation of this frequency indicates the nitrogen content, and since most explosives are rich in nitrogen, these devices can detect their presence. Pulsed fast neutron devices can approximate the hydrogen, carbon and oxygen composition of the material, which when combined with thermal neutron measurements of nitrogen content can provide a more specific identification of the material. Pulsed fast neutron systems are, however, expensive, large and slow, so systems for large numbers of smaller packages are often based on thermal neutron activation, with systems for searching smaller numbers of vehicles and large shipping containers being based on pulsed fast neutrons.

Trace vapour detection

4.242. Detecting explosive vapours is challenging because the vapour phase concentrations of high explosives can be very low (see Table 2). Vapour pressures are even lower if the explosive is packaged in an oil based gel or solvent.

4.243. In an ion mobility spectrometry system, the molecules in the air sample are first ionized and then passed into a drift region through a shutter that opens periodically for milliseconds at a time, causing 'pulses' of ions. Within the drift region, the ions separate by mass, the lighter progressing more quickly than the heavier. At the end of the drift region, the ions strike a Faraday plate, which records the output current as a function of the time since the ions entered the drift region.

4.244. Detectors using ion mobility spectrometry provide high sensitivity in detecting dynamite, military grade TNT and plastic explosives' compounds. Due to this sensitivity and the relative ease of operation and maintenance, ion mobility spectrometry technology is widely used for detection of explosives. However, it can be difficult to clear explosives residues out of the instrument after the

TABLE 2. VAPOUR PRESSURE OF EXPLOSIVES MOLECULES AT ROOM TEMPERATURE AND ATMOSPHERIC PRESSURE (20°C, 100 kPa)

Explosive	Constituent of	Vapour pressure (ppb)
Ethylene glycol dinitrate (EGDN)	Dynamite	92 000
Nitroglycerine (NG)	Dynamite	340
Dinitrotoluene (DNT)	Military TNT	300
Trinitrotoluene (TNT)	Military TNT	8
Cyclotrimethylenetrinitramine (RDX)	C-4, Semtex	0.006
Pentaerythritol tetranitrate (PETN)	Detasheet, Semtex	0.002

detection of large amounts, as very small remaining traces (e.g. nanograms) of some explosives can still be detected.

4.245. Most commercial explosives detectors are most sensitive when used in surface sampling mode, in which a surface suspected of contamination is swiped with a collection substrate. The substrate is then placed in a heating unit, which desorbs particles of explosives that have been gathered on the substrate and transports them to the detector for analysis.

4.246. For screening individuals passing through sensitive, busy checkpoints, such as airport boarding areas, walkthrough personnel portals have been developed.

4.247. Trained dogs are also used widely to search for explosives. However, dogs need constant retraining to continue to identify even the specific explosives or other materials they are trained to find. Moreover, the reliability of detection is subject to the health and disposition of the dog and the vigilance and skill of the handler. Dogs are usually trained to identify between six and ten odours and can be effective in identifying them for only a limited period each day. Technology based explosive detectors are therefore becoming more widely used as the preferred method for screening personnel for explosives.

X ray imaging and millimetre wave imaging

4.248. Commercially available devices can use low energy backscatter X rays to image materials on the bodies of persons being screened. Such devices can provide an image of prohibited items, including explosives hidden under the clothing, on persons being scanned. They typically subject the person to a very low dose of ionizing radiation. There are privacy concerns associated with imaging a person's body through the clothes. Such privacy concerns could be partially addressed by automated analysis of the produced image that simply indicates to an operator whether additional, manual search of the individual may be needed. Recommendations are provided in IAEA Safety Standards Series No. SSG-55, Radiation Safety of X Ray Generators and Other Radiation Sources Used for Inspection Purposes and for Non-medical Human Imaging [24].

4.249. Millimetre or terahertz wave imaging is another commercially available technology for imaging people, using radiation at frequencies to which most clothing is transparent but that are reflected by the skin. Metals strongly absorb these frequencies, and therefore images can reveal prohibited items such as guns, knives and explosives. Software can be used to modify or anonymize images to address questions of privacy.

4.250. For both X ray backscatter and millimetre wave imaging, secondary screening, typically by manual searches, is needed to confirm indications provided by the technology.

4.251. Screening of vehicles and large cargo containers needs higher energy X rays than those used for small packages. X ray systems with energies of 320 and 630 keV are typically used for vehicle searches. Gamma radiation is also used in some vehicle screening systems, using radionuclides such as ^{137}Cs (using the 661 keV emission from the short lived ^{137m}Ba progeny) and ^{60}Co (1173 and 1333 keV) to provide radiation that is more penetrating even than high energy X ray systems. During screening with these high energy systems, whether X ray or gamma, no occupants should be in the vehicle.

Nuclear material detection

4.252. The purpose of nuclear material detectors is to sense and after appropriate assessment detect the unauthorized removal of nuclear material directly on persons, in packages or in vehicles leaving a security area. There are

two commonly used methods to sense nuclear material, which are applied either in portal or in hand-held configurations:

(a) Passive methods sense the gamma and neutron emissions from nuclear material.
(b) Active methods using neutron activation to sense shielded nuclear material.

4.253. Radiation emitted from nuclear material can be detected using one of several detection materials, including: crystalline or organic scintillators (within a plastic matrix); semiconductors (solid state) that conduct electrically when exposed to radiation; and proportional detectors containing gas that can detect neutrons.

Gamma radiation detection

4.254. Scintillators detect gamma radiation from the radioactive decay of nuclear material: photons are produced when the scintillator material absorbs the ionizing radiation. Typically, the scintillators are crystalline (sodium iodide) or organic (plastic), the latter being used extensively in pedestrian portals.

4.255. A thallium activated sodium iodide (NaI(Tl)) scintillator coupled to a photomultiplier tube is commonly used to detect and identify gamma radiation. Pure sodium iodide crystals scintillate efficiently when cooled to around 77 K but much less efficiently at normal ambient temperatures. The addition of thallium not only increases the efficiency at normal operating temperatures but also causes a shift in the wavelength of the scintillation light so that NaI(Tl) is transparent to its own scintillations. One disadvantage of these systems is that exposure to small amounts of moisture causes the NaI(Tl) to discolour, lowering its transparency to its own scintillation light and preventing reliable detection and identification of gamma radiation. An NaI(Tl) detector can be used to distinguish gamma radiation of different energies, and therefore can be used for distinguishing between radionuclides; but it cannot detect neutrons. However, there are other scintillators, such as lanthanum bromide that might provide slightly better resolution of energies than NaI(Tl).

4.256. Plastic scintillators emit photons when high energy radiation (e.g. X ray, gamma, neutron) are incident on the plastic. The photons do not, however, indicate the energy of the incident radiation that produced the scintillation, and therefore they cannot be used to identify radionuclides. The plastic material is cheaper (per unit area) than the crystalline scintillators described above, but it has lower efficiency. Overall, plastic scintillators can provide more sensitivity at

a lower cost but without any energy resolution. They can also detect neutrons to some extent, and are commonly used for radiation screening of personnel.

4.257. Solid state detectors such as those using high purity germanium and cadmium zinc telluride can indicate the energy of the gamma radiation incident on the crystal. This allows the specific identification of radionuclides because the energy of the gamma radiation emitted is characteristic of the specific decay of a specific radionuclide. This is particularly useful in distinguishing the source of nuisance alarms. For example, a person who has recently had a medical procedure using a radioisotope such as ^{99m}Tc will emit a detectable level of gamma radiation, but a solid state detector can distinguish the gamma energy spectrum from those of radionuclides that the person might have encountered in a nuclear facility. Semiconductor crystals have excellent efficiency (sensitivity per unit area) and good energy resolution, but are more expensive (per unit area) than plastic scintillators. Germanium based detectors also need expensive cooling with liquid nitrogen, whereas cadmium zinc telluride detectors can provide reasonable energy resolution at normal ambient temperatures. Solid state detectors can also detect neutrons to some extent.

Neutron detection

4.258. Neutron detection is particularly useful in detecting nuclear material because some nuclear material (especially plutonium isotopes) emits neutrons that are difficult to shield, and because the neutron background is generally very low. Neutron detectors can therefore be very sensitive, and detecting neutrons can be a reliable indicator of the presence of nuclear material.

4.259. A neutron detector generates an alarm when a statistically significant increase over the normal background reading occurs. The alarm threshold should be selected to be close to the normal background level, but not so close as to cause a large number of nuisance alarms. The reference background level is established by averaging the counts over a number of counting time intervals, and this average is continually updated. Typically in a commercial walkthrough detector, the signal count restarts each time a person leaves the detector and each signal count is compared to the alarm level, taking account of the current average background; an alarm occurs if the signal count exceeds the alarm level.

4.260. Alarms should also be generated if power line failure, equipment failure, excessively high or low background or tampering with the equipment is detected.

Neutron activation detection

4.261. Neutron activation detection is based on directing a beam of neutrons, from a source such as ^{252}Cf, at a target, typically a container that is difficult to search by other means (e.g. cargo containers) to detect the presence of uranium. The source is used to direct a pulse of neutrons at the container — typically for a few seconds — and is then shielded to stop the incident neutrons. Any delayed neutrons emitted by uranium fission fragments are then counted to indicate whether or not nuclear material is present in the container. This search method should be used only for containers.

Nuclear material detection portal

4.262. Radiation detection equipment can be installed in portals to detect nuclear material in vehicles and rail cars (see Figs 22 and 23). Detectors can be mounted on a concrete foundation or on walls, and can be single or stacked to increase the height of the detection zone to cover that of the vehicles. Portals can also be equipped with video monitoring to record the detection process and provide evidence for assessing alarms. Nuclear material can be detected in stationary or moving vehicles.

Hand-held nuclear material detection

4.263. Hand-held detectors can be used to search people, packages and vehicles for a wide range of nuclear material or adjusted for specific types of nuclear material. Hand-held nuclear material detectors are primarily used for secondary screening and for screening very large areas or volumes where a portal detector is not effective. The search procedure and the time needed to conduct it and the benefit of detecting smaller quantities of nuclear material are similar to the benefits and limitations of the hand-held metal detector presented above. Every screening point with a nuclear material detection portal should also be equipped with a hand-held radiation detector.

Shielded nuclear material

4.264. The use of metal detectors in combination with nuclear material detectors is essential to detect shielded nuclear material. The metal detector should be able to detect relatively small quantities of heavy metals, such as lead. Because the resistance of such metals is generally higher than those with lower atomic numbers, they tend to be more difficult to detect. In all cases, the detectors need to operate at very high sensitivity, which will increase the nuisance alarm rate,

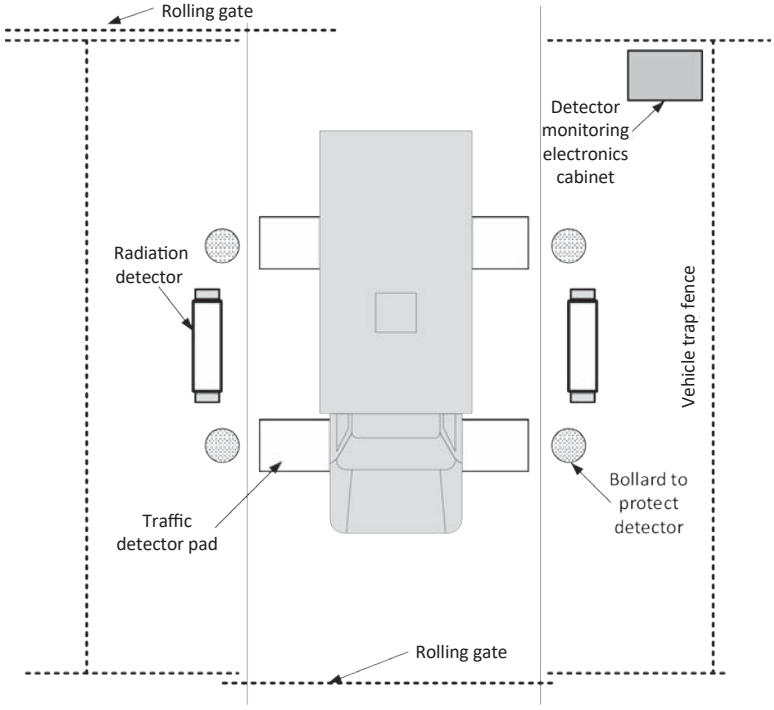


FIG. 22. Vehicle nuclear material portal configuration.

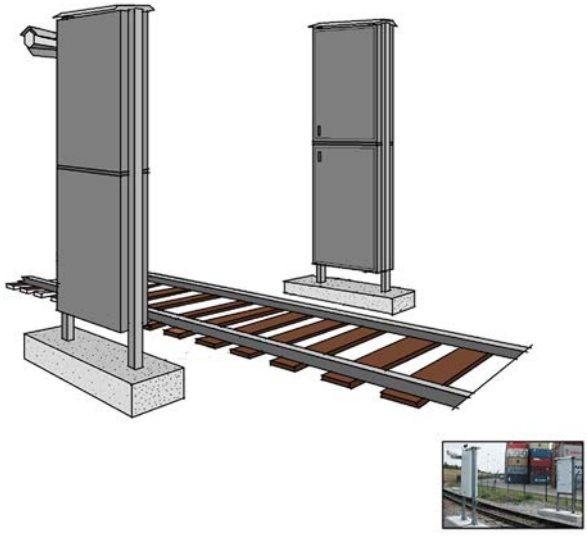


FIG. 23. Rail nuclear material monitor with CCTV.

and therefore an area for personnel to remove metal items from their clothing (e.g. removal of steel toed shoes) might be needed.

Summary of search technologies

4.265. Table 3 summarizes the different search technologies according to the different application and search classification schemes.

ACCESS CONTROL SYSTEMS

4.266. Access control systems are used to prevent or to detect unauthorized entry into security areas (e.g. limited access areas, protected areas, inner areas, vital areas). Such systems should allow only authorized persons and vehicles to enter and exit and support the prevention and detection of unauthorized movement of nuclear material, sensitive information, prohibited items or equipment into or out of security areas. General guidance about access control is given in Ref. [2]. Keys, locks, combinations, passwords and related devices used to control access to security areas and to physical protection equipment should be protected accordingly.

4.267. An access control system can be:

(a) Stand alone: such as a lock on a door.
(b) Interconnected: a group of access control devices controlled locally.
(c) Integrated: an access control system integrated with an intrusion detection system.

4.268. The number of personnel authorized to enter each successive layer of a security area typically decreases due to policies to minimize access to higher security areas. The access control system can and therefore should provide measures of increasing rigour for each successive layer: the number of authorized personnel that need to pass through each access point should be taken into account as well as the security requirements in deciding on the equipment and screening processes that are put in place. Access controls may make use of something a person possesses, such as personnel credentials, the use of something a person knows, such as a personal identification number (PIN), or a unique feature of a person, such as a fingerprint. The access control system should be supervised by guards so that any attempt to defeat or bypass the system is detected and a response is initiated.

TABLE 3. SEARCH SYSTEM CLASSIFICATION AND TYPICAL APPLICATIONS

Search type	Typical items inspected	Portability[a]	Principle of operation[b]	Interaction[c]	Alarm type[d]
Metal detection					
Portal	Personnel	Stationary Built-in	Electro-magnetic	Active Passive	Alarm
Hand-held	Personnel	Mobile	Electro-magnetic	Active	Alarm
Explosive detection					
X ray absorption	Vehicles Cargo containers Hand carried items	Stationary	Display monitor X ray	Active	Interpreted
Neutron activation and neutron absorption	Vehicles Cargo containers Hand carried items	Stationary	Display monitor Radiation	Active	Interpreted
Trace, vapour	Personnel Hand carried items	Stationary Mobile	Gas analysis	Active	Alarm Interpreted
Trained dogs	Personnel Vehicles Cargo containers Hand carried items	Mobile	Explosive odours	Not applicable	Interpreted
Nuclear material detection					
Portal: gamma and neutron	Personnel Vehicles Cargo containers Hand carried items	Stationary Built-in	Radiation	Passive	Alarm

TABLE 3. SEARCH SYSTEM CLASSIFICATION AND TYPICAL APPLICATIONS (cont.)

Search type	Typical items inspected	Portability[a]	Principle of operation[b]	Interaction[c]	Alarm type[d]
Portal: neutron activation	Vehicles Cargo containers	Stationary Stand alone	Radiation	Active	Alarm Interpreted
Hand-held: gamma and neutron	Personnel Vehicles Cargo containers Hand carried items	Mobile	Radiation	Passive	Alarm Interpreted
Combined metal and explosive detection portals					
X ray imaging (low energy backscattering)	Personnel	Stationary	Display monitor X ray	Active	Interpreted
Electromagnetic radiation and millimetre wave imaging	Personnel	Stationary	Display monitor Radiation	Active	Interpreted
Combined metal, nuclear material and explosive detection					
Manual inspection	Personnel Vehicles Cargo containers Hand carried	Stationary Mobile	Display monitor Mirrors Touch	Active	Interpreted

[a] Whether the system is stationary, built-in (combined with other applications), stand alone (not combined with other applications) or mobile (can be moved from location to location).
[b] Type of technology used.
[c] Active or passive interaction with the item being searched.
[d] Audible/visual alarm or interpreted by the operator.

4.269. For access control systems with intrusion detection systems, the requirements for communication paths between servers and access control devices are addressed in Section 6. This type of access control system needs to communicate with the subsystem that senses the state (open or closed) of access

points to be able to record accurately when an individual goes through and that the access point is in the correct state afterwards. The access control system also needs to communicate at some level with the alarm reporting and assessment system. If the two systems are not integrated, there should be at least some level of interaction between the two systems to recognize whether access that has been recorded is authorized or not, and in the latter case initiate an alarm. The two systems may be integrated so long as the system manages alarms and access control messages with the correct prioritization.

4.270. Figure 24 illustrates an example configuration of the components in an access control portal. The order in which search devices are encountered may vary, but all searches need to be completed before a person is allowed into the security area.

Personnel access control

4.271. A personnel access control system verifies the identity and authorization of the person seeking entry to a security area. Authorization is usually based on

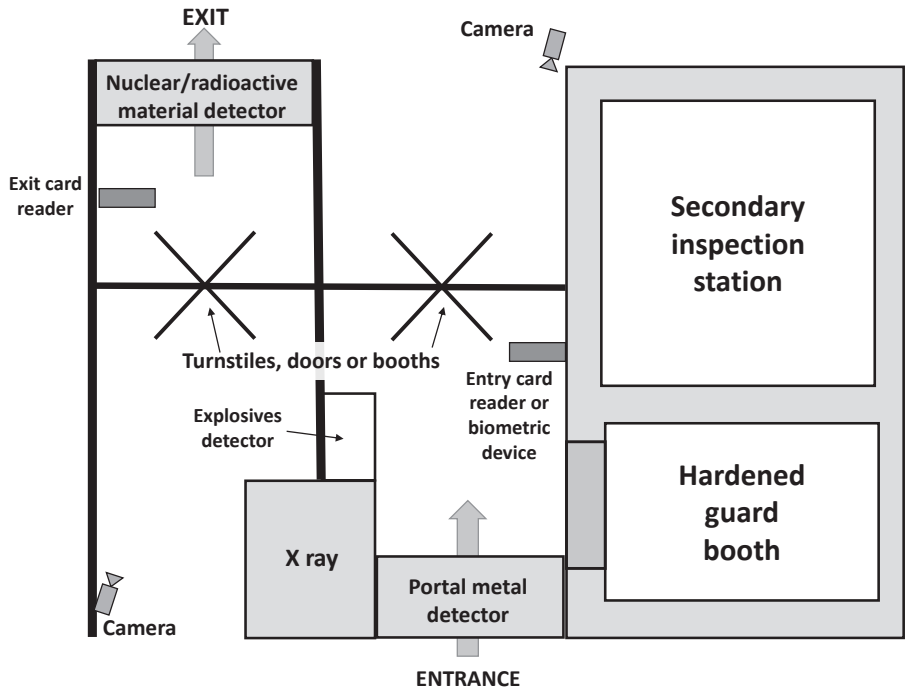


FIG. 24. Example of access control point components.

a need for access to conduct authorized activities. Automated electronic access control systems have an access list, typically an electronic database, containing data on the individuals with authorized access. Such systems should ideally be designed to create time stamped records of all events or alarms generated in the system. Modern access control devices can store the most recent data, so that they can operate in backup mode if networks are interrupted. Paragraphs 4.272–4.295 describe different personnel access control measures.

Credentials

4.272. Access control measures based on something a person possesses (credentials, such as a photo identification badge) usually involve a visual check by a guard. Some badges also contain coded credentials that can be used in automated access control systems. If these badges are used to operate an access control system (e.g. opening a door, turnstile or gate), the badges should be managed and controlled in a similar manner to a lock and key control system (see paras 4.299–4.309).

4.273. The photo identification badge is a common type of credential used for personnel access control but is the least secure. A false photo identification badge can be made, or an individual can alter their appearance to match that found on a stolen badge. Since this type of badge is checked manually, human error by the guard can reduce its effectiveness, especially at times when large numbers of people are entering a facility. These badges typically remain in the possession of the person outside working hours.

4.274. In a badge exchange system, when a person presents a badge the guard compares the presented badge and the individual with the photo on a separate exchange badge held at the access control point. If they match, the guard exchanges the badges and allows entry. The badge is held at the access control point until the person leaves the area, at which time the badges are again exchanged, and the exchange badge worn within the security area never leaves the area. This reduces the risk of a badge being counterfeited, lost or stolen, but it does not prevent human error or a person altering their appearance to match the image on a lost or stolen badge.

4.275. In a stored image system, a guard verifies an individual's identity based on visual characteristics. A securely stored image is displayed on a video or computer monitor and is used for comparison with a real time image of the individual requesting entry. Stored image systems are not based on a unique, measurable characteristic, such as a fingerprint, so they are not considered a form of biometric

verification. However, they are more secure than manual photo identification systems because it is difficult to tamper with the securely stored image.

4.276. A coded credential, which may be in the form of a badge, has information stored in or on it that can be read by an electronic access control system. Commercially available systems that use coded credentials include features such as unique authorization codes, time limited and/or area specific access authorization and recording of every passage through each access point. Examples of such systems include the following:

(a) Magnetic strip encoding is widely used in commercial credit card systems. A strip of magnetic material along one edge of the badge is encoded with data, which is read as the card is moved through a slotted magnetic strip reader or inserted into a reader. Magnetic strip technology is popular because of its relatively low cost and high reliability.
(b) Wiegand signal technology uses a credential code produced by a series of parallel wires with special magnetic properties embedded in a card. The wires are typically arranged in two rows, and encoding is 'fixed' during card manufacture. Cards are swiped through a slotted card reader, similar to the way magnetic strip cards can be read. This technology is widely used in the access control industry.
(c) Barcodes are widely used in the retail trade to automatically identify products at the point of sale, and can be used on coded credentials. The varying widths of the bars and spaces between them establish the code, and the card is read by an optical sensor that scans the barcode and transmits the information to a decoding unit. Barcodes are easily reproduced using a computer printer or copier. Two dimensional barcodes can store more information than one dimensional barcodes.

4.277. Proximity badges can be read without the badge being physically placed into a reader device. The electronic proximity identification badge uses a small radiofrequency transponder (transmitter) and needs to be powered in some way. Passive proximity badges draw power from a radiofrequency signal generated by the reader unit as it reads the badge. Active proximity badges are powered by a long life battery contained in the badges. Active badges have been largely replaced by passive badges. Earlier badges were read only, with a specific code fixed at the time of manufacture, but more modern badges are read–write and programmable, so that the system manager can programme the badge according to the system's needs. Newer systems are password protected and can encrypt data and use encrypted communication between the badge and reader. The system is designed so that the badge can only be read by the reader of the same system.

4.278. The smart card, also known as a chip card, is the size of a standard bank credit card and has an integrated circuit embedded in the card. The card can communicate with a reading device through contacts on the surface of the card or through low power radiofrequency communications (contactless smart card). Smart cards contain a microprocessor that can also be used to include other information, such as financial transactions, personnel training, health care records or property control functions.

Personal identification numbers

4.279. Many access control systems are based on the user entering a memorized PIN to gain entry. In a PIN only system, the user enters the PIN on a keypad to gain entry: the PIN does not uniquely identify the individual if other individuals in the system database have the same PIN. The use of a PIN alone does not provide a high level of security, since an adversary could obtain the PIN by observation or coercion. If the system does not prevent entry of repeated incorrect PINs, then it might be susceptible to defeat.

4.280. A PIN used in combination with one of the credentials listed above provides a more secure system. For example, an individual requesting access would insert their coded credential into the system and then enter a PIN via a keypad. This number can then be compared to the encrypted one stored in the access file for that person, and if the numbers are the same (and the person has the appropriate authority), the person is granted entry. Such a system still has weaknesses, however, as an individual could pass both the PIN and credential to an adversary.

4.281. Systems are typically more secure if PINs are generated randomly for users, rather than allowing the user to generate it. The system should also protect the PIN by encrypting it before transmitting it across a network or storing it.

Biometric identity verification systems

4.282. Biometric identity verification systems use unique physical or physiological biometric characteristics of an individual to verify identity. Commercially available systems use characteristics such as weight, hand or finger geometry, blood vein patterns, fingerprints, face recognition and eye patterns. Factors to be considered in selecting such systems include the extent to which the feature can uniquely identify the individual, the variability of the characteristic in the individual and the difficulty of implementing the system that processes the characteristic. Biometric systems can be used to validate other access

control credentials or as a sole identifier. In the former case, the system uses the first credential to identify the appropriate record (e.g. PIN or radiofrequency identification card), and then the system verifies that the associated biometric data are correct for the individual. When used alone, the entire biometric database might need to be searched by the system until the appropriate record is found, which increases the verification processing time, especially if the database is large. In cases where the laws of a State require anonymity, some systems are designed to prevent reconstruction of a specific person's biometric data (e.g. fingerprints cannot be retrieved).

4.283. For any biometric characteristic, there will be some individuals who cannot be reliably identified in this way and alternative methods need to be available for such cases. If individuals need to wear personal protective equipment when entering a particular area, this equipment might also hinder the use of biometric identification. Workable access control measures may, for example, be designed for personnel wearing gloves or respirators: a person wearing gloves cannot be identified by hand geometry or fingerprints; and a respirator might prevent the use of facial recognition, eye pattern or iris based identification systems.

4.284. Each biometric access control measure has a false acceptance rate (the percentage of times the system allows access to someone without authorization) and false rejection rate (the percentage of times the system denies access to an authorized person). There will also be some failures due to the person's characteristics or actions, such as fingerprints that are unreadable. Selection of biometric access control systems should consider these factors.

4.285. Weight scales can be incorporated into personnel access control systems, whereby the authorized person's weight is recorded on entry for comparison later. If the weight of the individual on subsequent occasions matches the recorded weight (within a specified tolerance), then combined with other access control measures such as cards and PINs there is greater confidence in the identity verification. Weight scales also reduce the risk of individuals passing credentials to others or unauthorized entry of more than one personnel simultaneously.

4.286. Hand geometry systems characterize the shape of the hand, measuring three dimensional features of the hand such as the widths and lengths of fingers and the thickness of the hand. A solid state camera takes pictures of the hand, including a side view to show hand thickness. Infrared illumination and a reflective platen provide a silhouette image of the hand to the camera. The system measures lengths and widths of a number of hand parts and creates a numerical representation (or template) of the hand, which it compares with the hand of an

individual seeking access. If the read image and the stored template match within an allowable tolerance, verification is successful.

4.287. Two finger geometry is a simpler version of such a system used to verify identity in a similar way: in this case, the system measures only the index and middle finger.

4.288. Blood vein patterns, particularly in parts of the hand, are useful characteristics that can be used to identify individuals. Commercially available biometric identity verifiers use the vein patterns in the palm, the fingers and the back of the hand. Near-infrared light can penetrate the skin to sufficient depth to provide clear images of the veins in parts of the hand when used in conjunction with any solid state camera.

4.289. Fingerprint systems typically use ridge endings and bifurcations as the identifying features of the fingerprint, although some systems use the whole print for comparison purposes. All fingerprint identification systems depend upon careful positioning of the finger and accurate analysis and comparison of the print for reliable identification. Modern systems also incorporate a pulse check for added assurance. Direct imaging sensors are available that use solid state devices for acquiring fingerprint images, using capacitive, electric field and thermal methods. Such devices are commonly used in applications such as secure computer login, and use ultrasonic or optical imaging:

(a) The ultrasound method images the lower layers of the skin and so is more robust for 'damaged' fingerprints where the outer surface of the skin is dry or worn. Ultrasound imaging is slower than optical methods because of the raster scan needed by the ultrasonic transducer.
(b) Optical methods use a prism and a solid state camera to capture the fingerprint image. Dry or worn fingerprints are more difficult to image using optical methods, but special coatings can be applied to the optical platens to enhance the image quality by ensuring a good optical coupling between the platen and fingerprint.

4.290. Facial recognition systems use distinguishing characteristics of the face to verify a person's identity. Most systems capture the image of the face using a video camera, although some systems can also capture thermal images using an infrared imager. Distinguishing features are extracted from the image and compared with previously stored records of such features. If the images match within a specified tolerance, identity is verified. Such systems need to be designed carefully to manage reliably variations in the presentation of the face and lighting.

4.291. Eye pattern features, like fingerprints, are effectively unique and identity verification systems are available based on recognition of characteristic patterns in the retina and iris. The unique pattern of blood vessels on the retina of the eye can be assessed optically through the lens of the eye: a circular path about the centre of vision is scanned with a very low intensity light from infrared LEDs, and the intensity of the reflected light from each beam position during the scan indicates the location of the retinal blood vessels.

4.292. Iris based biometric systems use a video camera to image the structure of the iris in the eye. These images are obtained with a camera located at about 25 cm from the iris, so no physical contact between the face and the scanner is needed and there is no artificial light shining into the eyes (the eye is externally illuminated with visible light). For these reasons, iris scan technology is often preferred to the retinal scanner. Possible disadvantages of iris based biometric technology might include false rejection errors for individuals wearing spectacles, the relatively long time needed (4–5 s for practised users, up to 15 s for new users), and the fact that about 2% of the population have an iris colour or structure that cannot be recognized by the system.

Personnel tracking

4.293. Many access control systems provide the capability to track personnel within a facility by recording data read from credentials at entry and monitoring points. The system thereby records the areas visited by an individual and can restrict access to certain locations, generally or at specific times (e.g. outside their working hours). A personnel tracking system helps to protect against procedural violations, such as removing, exchanging or 'passing back' credentials, to detect violations of a two-person rule.

4.294. Personnel tracking data are stored in a permanent log giving details of access by date, area, individual or other parameters. If appropriately recorded, access control records can be used during the investigation of a nuclear security event to identify possible suspects or to ensure that guards are performing their assigned patrol duties correctly. Awareness that a facility has such a tracking system might also deter personnel from unauthorized actions. Requests for authorized access to security areas or systems important to safety or security, whether approved or disapproved, should ideally be reviewed regularly to confirm individuals' continued need for access and to help to identify possible insider threat activity.

Two-person rule for access control

4.295. Some automated access control systems enforce a two-person rule by requiring two sets of credentials or biometric characteristics to be entered into the system before granting authorized access to an area. This might apply, for example, to entry to and exit from a high security area to ensure that a single person does not enter or remain alone in such an area. Two-person rule access controls can also be applied to the opening of cabinets containing security equipment or alarm components, entry to controller processing rooms during maintenance, or for certain CAS personnel functions, such as remotely opening a security door.

Vehicle access control

4.296. Vehicles can be subject to access controls when entering or exiting security areas. In some cases, verification of authorization of the driver and occupants is sufficient and no separate authorization of the vehicle is needed. For higher security areas, a vehicle registration system can be used to allow only authorized vehicles to enter.

4.297. Depending on the facility, vehicle access control methods can be automated or manual. For a small facility, a manual list of authorized vehicles can be used to limit vehicle access to security areas. For large and complex facilities, an automated database of authorized vehicles can be developed and access credentials issued for such vehicles, similar to systems for personnel access control, or automated vehicle identification technology (e.g. by registration plate recognition or an embedded chip in the vehicle) can be used. Image databases can also be used to identify authorized vehicles visually and to determine whether they have been modified compared to the authorized configuration.

Access control in emergency situations

4.298. For an emergency situation, methods should be developed to provide access for emergency personnel. This can include such personnel being escorted by authorized individuals when in security areas. Further guidance on this topic is provided in Ref. [2].

Locks and keys

4.299. Locks are crucial components of a PPS, and provide both access control and delay functions. A physical barrier, such as a door, might be penetrated either by breaking through it or by defeating the locking mechanism. Locks should

be selected to delay an adversary at or as close as possible to the barrier: this might include coupling the locking mechanism into the barrier itself. Locks are commonly categorized by the mechanisms used to withdraw the latching system, which include combination locks, keyed locks and electronic locks.

4.300. Combination locks take the form of either a case lock, mounted on or into a barrier, or a separate padlock. Combination locks are available in multiple-dial, push-button, single-dial and electronic forms. A multiple-dial lock has a number of rotating discs, each with several positions (typically ten, numbered 0–9), and is commonly used on small containers, briefcases and bicycle locks, but can be easily defeated. In a mechanical push-button lock, a sequence of buttons is pressed in turn (and if the sequence is correct) to activate links between a gate and an external knob to permit opening of the lock. This type of lock typically offers relatively few possible combinations, and therefore can be defeated by simply attempting each possible combination until the correct one is discovered. A single-dial combination lock is a mechanical lock with a spin dial, which interacts with several parallel discs or cams. Locks of this type are typically opened by rotating the dial clockwise specific distances (usually in the form of numbered steps) and counter clockwise alternately. The cams typically have an indentation or notch, and when the correct combination is entered, all of the notches align, allowing the latch to fit into them and open the lock. Some single-dial combination locks can be defeated relatively easily, but high security designs are available that are difficult to defeat. Electronic combination locks offer many features unavailable with other types of combination lock: some of these can be defeated as with other combination locks, but they are typically more difficult to defeat.

4.301. Keyed locks can be of warded, wafer (or disc), lever or pin-tumbler type, of which the most common is the pin-tumbler. As in the case of combination locks, a key lock should normally be capable of being set to accept only one from a large number of possible different keys. High security lock cylinders are available, which can allow greater control over keys, by restricting any order to supply or copy keys, blanks or cylinders to people with written authorization, and restricting the manufacture and supply of specific key configurations to specific users. Keyed locks allow the use of master keys, whereby most keys only open one specific lock, but a master key can be used to open any of the locks of that type. Extra controls need to be applied when using such a system because, if a master key is lost or stolen, it can be used to open several different locks at the facility.

4.302. An electronic lock comprises an automatic door closer on a door, an input device, a controlling device and a lock, usually mechanical, which is released or activated when the correct combination is entered or the correct token is presented

to the input device. Such systems can use biometric data badges, magnetic strip cards, proximity cards, smart cards or combination entry. Electronic locks allow the isolation of the part of the lock containing the code from the part that is exposed, can be programmed for use in different ways, and can readily be integrated into alarm systems. In the event of a power failure, an electronic lock system can be designed to 'fail secure', meaning the doors remain locked to personnel on the unprotected side, but exit from the secure side is possible. Many electronic locks are equipped with a case lock in the door, and often a physical key to its cylinder — the emergency override key — which can be used to open the lock during a power outage.

4.303. The facility operator should implement a lock and key control system and assign specific roles and responsibilities for control of all locking devices used at the facility, including locks, keys and other access control measures. Paragraphs 4.304–4.306 describe components of a lock and key control system.

4.304. A lock and key hierarchy should normally be developed, to group locks, keys and other access control devices into groups of measures that are required to provide similar levels of security based on a graded approach. For example, locks, keys and other access control devices used as part of the PPS might be categorized as 'security locks and keys' to distinguish them from 'administrative locks and keys' used elsewhere in the facility.

4.305. Lock and key control measures should be developed for security locks and keys, with appropriate measures proportionate to the potential consequences of their loss or compromise. For example, all keys used to gain access to a vital area should be strictly controlled to ensure they cannot be used by an unauthorized person to gain access; whereas with keys to an administrative office not containing any sensitive materials, the door might have minimal control. Spare security locks, cores, keys, key blanks and credentials (cards and badges) should be stored in a secure location.

4.306. An authorized access list (e.g. identifying personnel authorized to have access to security keys) can be used. Keys and combinations should be issued only to individuals who are authorized users and need to use the security key or combination to carry out their work. A lock and key control system should include procedures for verifying the identity of the individual requesting the keys or combinations and that the individual is authorized to access all areas to which the keys or combinations provide entry.

4.307. An inventory management system should be developed to provide accounting and control for security locks, keys and credentials in use, and spares in storage. Security locks and keys should have a unique characteristic, such as a unique identification number, and a record of all locks, cores, keys, key blanks and credentials should be maintained and stored in a secure location. The records should identify the number of keys for each lock and their locations, and all occasions when a lock was changed, rekeyed or rotated. At a defined frequency, the inventory of all the security locks, keys and other devices should be reviewed and updated. Measures should be established to address the loss or theft of keys, credentials or similar items, such as rekeying, changing of locks or changing of combinations or codes. A notification process should be established for reporting lost or stolen security keys and credentials.

4.308. Automated key control systems are available that control the issuing of keys, track keys until they are returned and conduct automated checks and inventories.

4.309. A combination and PIN management system should be developed to control their issuing to authorize personnel. Records of combinations, PINs and biometric templates should be appropriately secured. Records should be maintained of personnel with authorized knowledge of combinations and PINs, when combinations or PINs were last changed and when they are due to be changed. Combinations and PINs should be changed periodically, when personnel with authorized knowledge no longer need access, or there is evidence the PINs might have been compromised.

Seals or tamper indicating devices

4.310. Seals or tamper indicating devices can be used with locks and alarms as an additional indicator of any unauthorized attempt to open a door or container. If such devices are used, they should be checked periodically for any indication of irregularities. Additional information on tamper indicating devices is provided in Ref. [8].

DELAY

4.311. The delay function, which is provided primarily by barriers, is to increase the time that an adversary needs to complete a malicious act (especially the time after detection and notification of response) by introducing impediments along any path the adversary might choose, with the intention of providing sufficient

time for the response force to react and respond. Barriers also complement access control measures and typically support detection at the perimeter of a security area and can be used to mitigate the consequences of a stand-off attack. Barriers might deter some adversaries and might defeat some attempts to carry out malicious acts. Occasionally, barriers might be provided by natural elements at the site of a facility, such as cliffs, hills or very large distances, but delay should normally be provided by engineered barriers that are carefully planned and positioned in the path of the adversary. In addition to the delay provided by the barrier itself, the distance between the barrier and the protected target might represent an additional delay. The delay provided depends on the nature of the physical obstacles employed and the capabilities of the adversary. Guidance on physical barriers is given in Ref. [2].

4.312. Barriers should be considered in relation to the adversary's goal (normally unauthorized removal or sabotage) and the capabilities of the adversary as defined in the threat assessment or design basis threat. If the goal is unauthorized removal of material, barriers that are penetrated or destroyed by the adversary on entering the facility, will no longer provide delay to leaving the facility. Some barriers, such as emergency exits, might provide some delay against an outsider adversary trying to enter the facility, but for safety reasons need to allow personnel to exit rapidly.

4.313. Table 4 provides an overview of the types of barrier with their associated functions, typical placement, limitations, possible compensatory measures (temporary measures that may be used if the barrier fails) and means to ensure the integrity of the barrier.

4.314. Multiple and different barrier designs can be used to create a delay defence in depth approach to aid alarm assessment and interception of the adversary at predictable locations. Consideration should be given to installing barriers and detection systems adjacent to each other so that the barrier is encountered immediately after the sensor. This arrangement delays the adversary at the point of sensing and increases the probability of accurate assessment resulting in increased detection (see Section 9).

4.315. A balanced barrier design ensures that, to the extent possible, each aspect of a barrier configuration affords an equivalent delay. The following should be considered in the design of a balanced delay system:

(a) Use barriers and other delay measures closest to the target to maximize delay time;

TABLE 4. BARRIER TYPES

Type	Placement	Function	Limitations	Possible compensatory measures	Measures to ensure integrity
Low security barriers	Facility boundaries	Demarcate boundary	No delay	Guard patrol	Visual inspection
Security fences	Facility boundaries Security areas	Demarcate boundary Assist sensing and assessment by delay Might be part of detection system	Limited delay	Guard post	Visual inspection Might have sensors
Vehicle barriers	Usually at security area boundaries	Prevent unauthorized vehicle entry	Barriers are designed for an angle of impact, a maximum weight and speed of a single vehicle Chicanes limit approach speeds	Temporary devices or obstacles	Visual inspection, daily functional test for movable barriers
Structural barriers (buildings)	May be used as the boundary of a security area	Provide delay	No stand-off Some elements might need to be hardened for balance (e.g. installing grills or grates on windows)	Guards Response forces Movable obstacles	Visual inspection Might have sensors

TABLE 4. BARRIER TYPES (cont.)

Type	Placement	Function	Limitations	Possible compensatory measures	Measures to ensure integrity
Turnstiles and doors	At or within security area boundaries	Used to allow authorized entry into a security area	Might be difficult to balance delay with associated fixed barrier	Guards Response forces Movable obstacles	Visual inspection Might have sensors Functionality testing of any active delay systems (e.g. door locking pins)
Boundary penetration barriers	Specific locations	Provide balanced delay	Might be difficult to balance delay with associated barrier	Guards Response forces Movable obstacles	Visual inspection Might have sensors
Specialized barriers (blocks, tie-downs)	Specific locations, to increase delay (e.g. target locations)	Provide balanced delay	Safety/operational impact	Guards Response forces Movable obstacles	Visual inspection
Dispensable barriers	Target locations	Provide delay	Safety Limited use Confined space issues	Guards Manual activation when electronic activation fails	Maintenance and testing

TABLE 4. BARRIER TYPES (cont.)

Type	Placement	Function	Limitations	Possible compensatory measures	Measures to ensure integrity
Marine barriers	Waterway boundaries	Provide delay against attack from waterways	Might be difficult to design and deploy (i.e. tides, current)	Guards Unmanned vehicles	Visual inspection Functionality testing of any active delay systems

(b) Use barriers consisting of different materials that need different methods and tools to defeat;
(c) Locate vehicle barriers at the outermost detection zones;
(d) Limit the adversary's use of vehicles near the target;
(e) Force an adversary on foot to carry tools and weapons (and target material in the case of unauthorized removal);
(f) Prevent the use of a vehicle as a ramming device or fighting position, or to deliver explosives, at the target location;
(g) Use barriers in confined spaces to minimize the adversary's freedom of movement.

Low security barriers

4.316. Low security barriers are typically used at the outermost boundary of a facility and are primarily for safety purposes (e.g. for construction projects) and provide little delay of an adversary. They are frequently used to demarcate boundaries (e.g. to define the area that it is an offence to enter without authorization) and to keep animals out of the detection zone. Typical low security barriers include wooden, fabric and wire fences.

Security fences

4.317. Security fences are installed at the boundaries of security areas. They provide deterrence and some delay, and are often used in conjunction with intrusion detection systems. They can be used to support the functions of sensing and assessment. For example, security fences can be installed in parallel to create a clear zone around a security area. Sensors, lighting and cameras can be installed within the clear zone to create a perimeter intrusion detection system.

4.318. A security fence usually comprises panels, uprights, hardware and foundations. As shown in Figs 25 and 26, typical examples of security fence panels include chain link, welded mesh, expanded metal (normal or flattened), metal palisade, woven metal and reinforced concrete.

4.319. Security fences should be constructed to prevent tunnelling under the fence. This can typically be achieved by extending the foundations into the ground or by concrete grounding.

4.320. Security fence design should take into account the associated detection systems and adversary capabilities. When selecting a fencing material, especially when replacing existing security fences, the effect on guard patrol strategies and

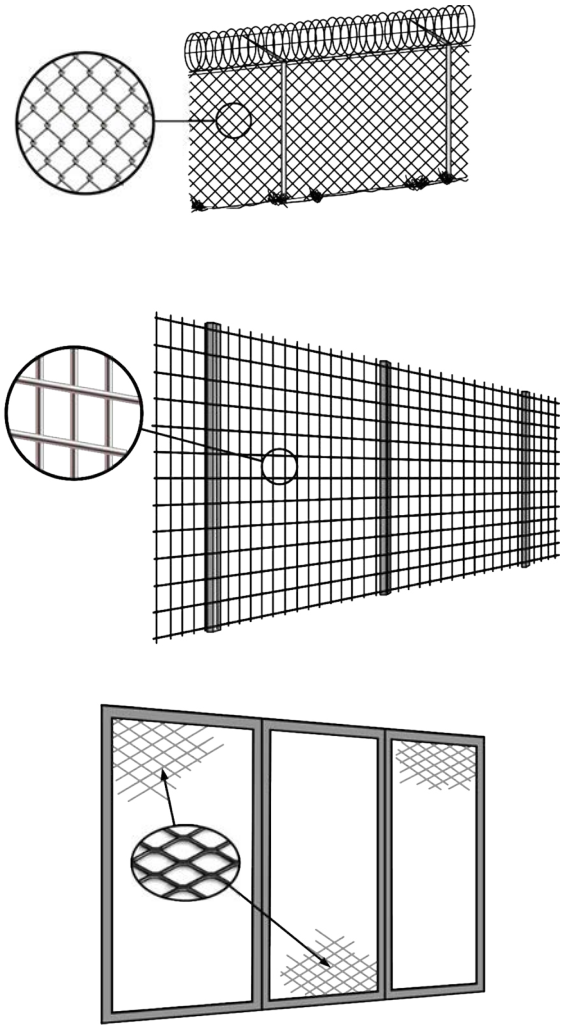


FIG. 25. Typical security fence panels. (Top to bottom) Chain link; welded mesh; and expanded metal.

CCTV coverage will need to be considered, as different fencing materials might change visibility through the fence. For specific purposes, other materials can be used as fencing material (e.g. security glass).

4.321. Security fences might be used as part of the detection system itself. Examples include fences with mounted fibre optic cables, strain sensitive sensors and fence mounted vibration sensors (see Fig. 27).

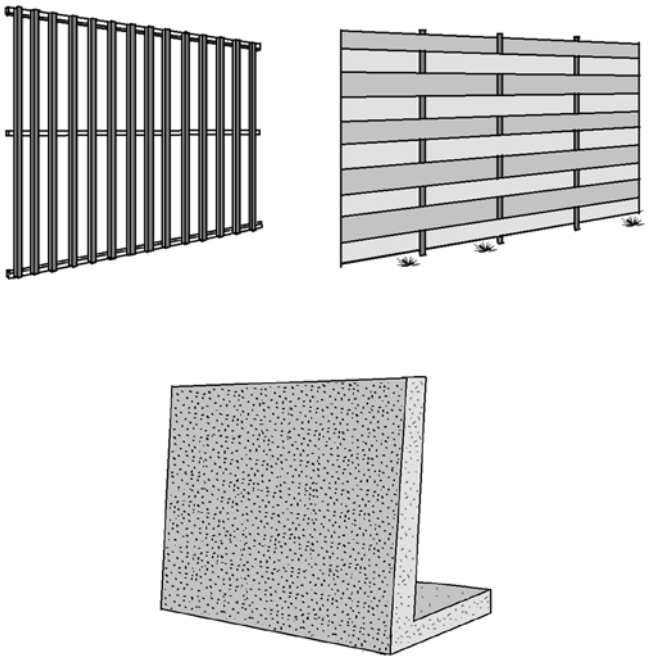


FIG. 26. Typical security fence panels. (Top to bottom) Metal palisade; woven metal; and reinforced concrete.

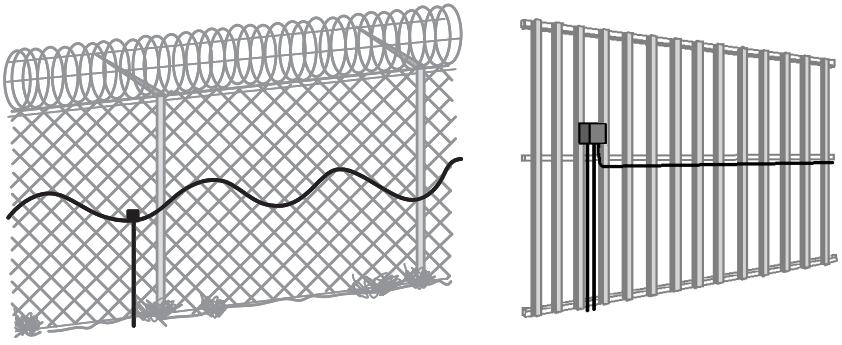


FIG. 27. Security fencing with a vibration sensor cable (left) and a fibre optic cable (right).

4.322. Security fences should be subject to regular visual inspection to ensure that they remain capable of performing their delay function. Typical compensatory measures if this function is temporarily impaired (e.g. when a damaged fence is

being repaired) include the placement of guard posts to provide the detection and delay functions as necessary.

Use of barbed tape coil

4.323. Placing rolls of barbed tape coil on or near fences can enhance their capability to delay adversaries. When added to the top of an existing security fence, it can be an effective addition, as an adversary will need additional tools to be able to climb over the fence (see Fig. 28). If barbed tape coil is used, the facility operator will need to consider the threat assessment or design basis threat, the environmental conditions, possible effects on safety or legal implications, the structural capability of the existing barrier to support the barbed tape coil and the possible effect on maintenance activities (e.g. access to sensors or cameras).

4.324. Another enhancement involves placing barbed tape coil either horizontally on the ground, against the fence or between the fences (see Fig. 29). Placing barbed tape coil between the two perimeter fences can prevent accidental injury to passers-by from outside and inside the facility. When it is placed horizontally, it should be staked to the ground and care should be taken to prevent excessive plant growth or accumulation of debris in the rolls.

Vehicle barriers

4.325. Vehicle barriers are designed to prevent unauthorized access of vehicles to a facility by dissipating the vehicle's kinetic energy. They can either be stationary structures that are built in-line with security fences or movable components deployed at road or rail gates. A vehicle barrier system should be capable of stopping a defined vehicle (consistent with the threat assessment or design basis threat) at a specific distance away from inner and vital areas, regardless of where the attack begins. The stopping capabilities of stationary and movable barriers should be balanced to avoid weak sections in the sequence of vehicle barriers.

4.326. A vehicle barrier is successfully penetrated if a vehicle passes through the barrier and is still functional, or bypasses the barrier because it has been removed, bridged or breached, for example by a previous vehicle.

4.327. Vehicle barriers should be designed with the following considerations:

(a) The threat (using the threat assessment or design basis threat) that the barrier is intended to stop (e.g. type, size and weight of vehicle, impact velocity and angle, other physical characteristics);

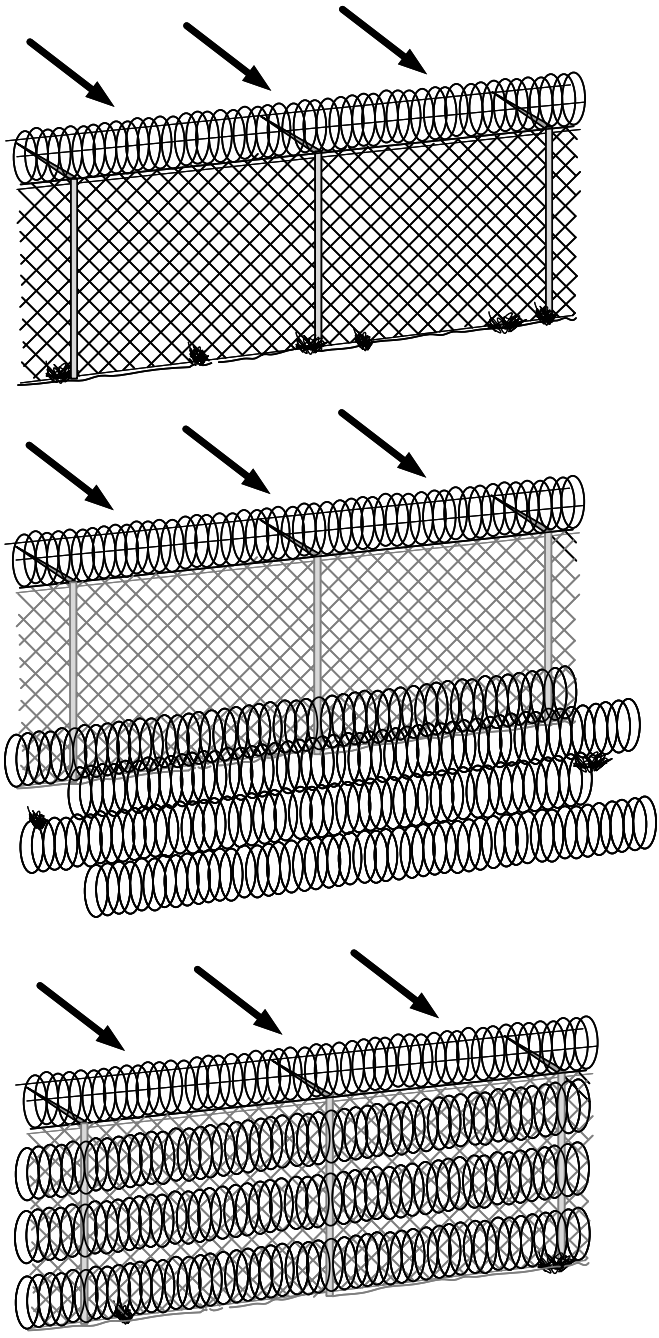


FIG. 28. Security fence with barbed tape coil.

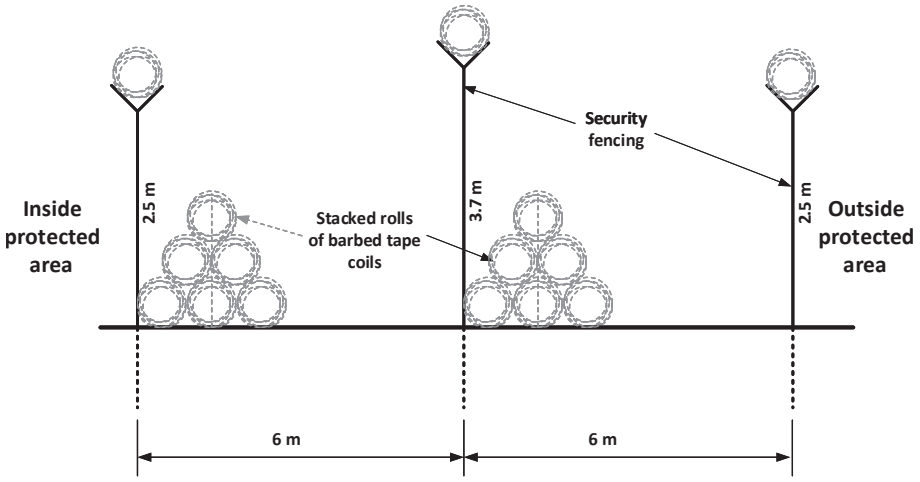


FIG. 29. Security fence configuration with barbed tape coil.

(b) Relevant facility operating conditions, such as the vehicle throughput;
(c) Limitations of vehicle barriers to protect against unusual vehicle types (e.g. small delivery vans, motorcycles, construction vehicles, small all terrain vehicles);
(d) The areas to be protected (to select the optimal locations to install vehicle barriers);
(e) Facility specific considerations such as terrain, road layout in and around controlled areas, potential routes of approach and environmental conditions.

4.328. Barriers should be selected that are best suited to protect against the defined threat, fit the particular situation and environment, and are installed correctly:

(a) Barriers that are installed outside a detection zone should be designed to be difficult for an adversary to defeat. This, together with routine patrols, will make it difficult for an adversary to remove the barriers without detection and a response. For example, large diameter concrete filled pipes sunken deeply into the ground combined with a random patrol would be difficult to remove without detection by the patrol, which could reduce the need for continuous surveillance of an area.
(b) Vehicle barriers that can relatively easily be defeated should be located inside a detection zone to allow detection of any tampering with the barrier.

(c) The height and construction of the vehicle barrier should be chosen to be the most effective against the vehicles anticipated in the threat assessment or design basis threat.

4.329. Most permanent vehicle barriers are designed to stop vehicles through one or more of the following methods:

(a) A vehicle arrestor absorbs most of the vehicle's kinetic energy and applies a low to moderate resistive force to gradually stop the vehicle over a relatively long distance. Examples include a series of weights that successively attach themselves to the vehicle as it moves through the barrier, and cables attached to braking systems to dissipate the vehicle's energy.
(b) A crash cushion absorbs most of a vehicle's kinetic energy and provides a stiff resistive force to stop the vehicle within a reasonable distance. Examples include liquid filled plastic containers and arrays of empty steel barrels backed by strong supports.
(c) An inertia device exchanges momentum and kinetic energy with the vehicle during impact. This device provides a stiff resistive force to stop a vehicle within a reasonable distance. Examples include small concrete shapes and sand filled barrels that are not anchored.
(d) A rigid device provides a high resistive force to stop vehicles in a very short distance. The vehicle dissipates almost all of its own kinetic energy as it deforms during impact. Examples include massive concrete shapes and steel structures that are well anchored. A train derailer is a type of rigid device.

4.330. Vehicle barriers are potentially vulnerable at the access points. Approach roads are often aimed directly towards an access point, making it susceptible to ramming by a vehicle, but the orientation of vehicle barriers and roads can reduce the probability of breaching the barrier. Approach roads constructed with multiple turns and barriers (e.g. chicanes) on each side of the access point area will reduce the approach and departure speed of vehicles.

4.331. The installation of interlocking movable vehicle barriers at access points should be considered. Such a system allows one movable vehicle barrier to be closed and locked before the other is released and opened, so that the area between the vehicle barriers provides a holding area for one vehicle to allow searching before entry or exit. Other methods of achieving a similar effect may be considered (e.g. using vehicles, containers or heavy construction bags as temporary vehicle barriers). Careful placement of the operational controls and the associated hydraulic and electrical systems of a vehicle barrier can help to improve the reliability of such barriers.

4.332. Typical movable vehicle barriers are not designed to stop unauthorized vehicles but to be moved to allow authorized vehicles to enter. The different types include raised bollards, pop-up barriers and raised booms (see Fig. 30).

Structural barriers

4.333. Structural barriers are building components such as concrete walls, floors, ceilings and roofs that can act as delay barriers. Structural barriers can also include interior free standing structures that could also delay an adversary. Structural barriers can also be used for the protection of guards or response personnel.

4.334. Concrete walls, floors, roofs and ceilings are designed to support structural loads and are not normally designed specifically to delay penetration. Conventional wall construction includes wood framing, brick, block or concrete. Concrete walls are built with the strength and thickness of concrete and the size and spacing of reinforcing (rebar) materials to meet structural requirements. However, in order to provide the delay times needed for physical protection, including protection against stand-off attacks, structural barriers might need to be designed to higher standards or with additional reinforcement.

4.335. Specifications for structural barriers should take into account the capabilities of the threats defined in the threat assessment or design basis threat. Typically, penetration methods an adversary might use to defeat a structural barrier include hand, power and thermal tools, explosives and heavy construction and demolition equipment, used alone or in combination.

4.336. If possible, a new facility should be designed and built with inherent features capable of providing large delay times. This not only provides protection against current threats, but also might provide protection against new and emerging threats and capabilities. Alternatively, new structural barriers can be designed and built to provide additional delay, and in some cases, existing structures can be made more robust by adding features to increase delay. Methods to increase the delay provided by structural barriers include the following:

(a) The construction of two or more parallel reinforced concrete walls close to each other. This provides a longer penetration delay time than one wall of thickness equal to the sum of those of the separate walls because penetration of multiple walls needs multiple individual efforts and the transfer of tools from one wall to the next.
(b) The construction of two or more reinforced concrete walls with fill material (e.g. rock) between the walls.

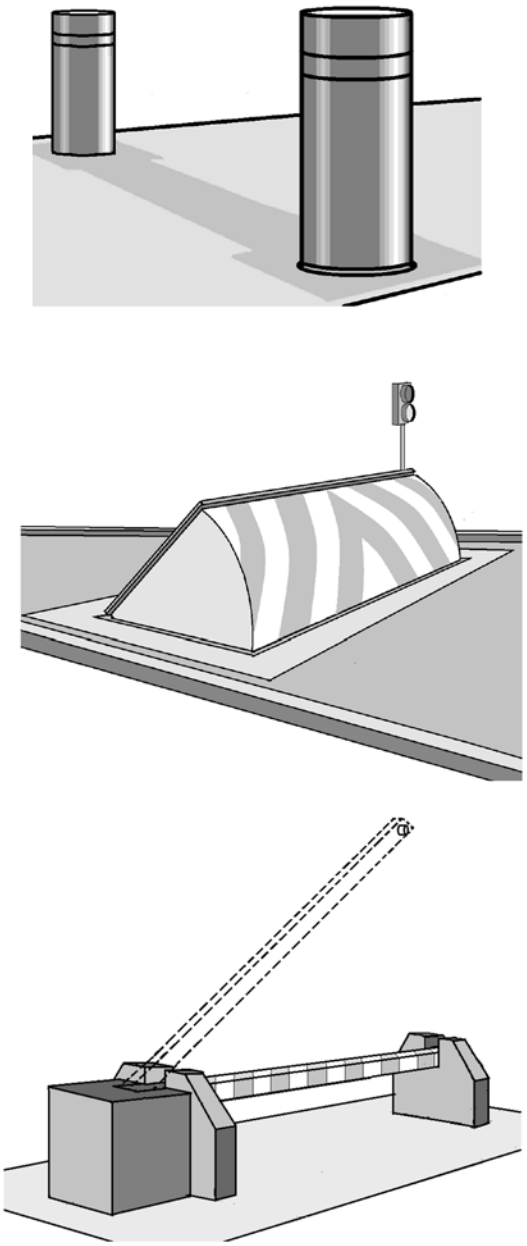


FIG. 30. Movable vehicle barriers. (Top to bottom) Automated or manual raised bollards; pop-up barrier; and movable boom.

(c) The use of multiple materials to construct a composite wall, such as steel plating encasing both sides of the concrete wall. This increases the delay time and the complexity of the task to defeat this barrier.
(d) Roof enhancements, such as membranes with embedded screens, several inches of rigid insulation, reinforced concrete with deformed steel bars and expanded steel mesh, and large rebar in rows or layers in reinforced concrete.
(e) Wall rebar reinforcement in a concrete wall. This can extend the penetration delay time in most designs. Although the concrete might be penetrated by an explosion, the reinforcing material usually remains intact and needs to be removed before entry. Removing the rebar often takes more time than removing the concrete, and therefore using additional rebar, increasing rebar size or decreasing rebar spacing can be advantageous.
(f) Earth cover or other overburden, to delay access to the wall itself.
(g) Barriers placed below the space of the roof. These might be more effective against penetration than barriers in the roof itself, and might be used in some existing structures without major modification. Placing these enhancements below the roof line provides the structure with some protection against direct attack and might create the need for a second separate penetration attempt. The second penetration attempt could also be constrained, as it would take place in a confined area, and might need different tools to complete penetration. The optimum distance below the roof is likely to be approximately 30 cm, and such a distance might further restrict subsequent adversary actions due to it filling with debris. Enhancement materials include quarry screen, expanded steel, bank vault mesh or floor gratings.

4.337. When used as protection for guards and response personnel, barrier design should take into account the barrier's resistance to ballistic and explosive effects or forced entry. If intended for use as a fighting position, the design might include gun ports (or openings) and bulletproof glazing.

Turnstiles and doors

4.338. For a balanced barrier design, the penetration delay time for access points within a sequence of barriers should be equal to the delay time of the surrounding barrier structures. Examples of personnel access points with delay functions at a security area boundary include metal and hardened turnstiles, personnel portals (e.g. a booth with an interlocking door, known as a sally port), and hardened steel grated and barrier doors (see Figs 31–33).

FIG. 31. Metal turnstile (left) and hardened turnstile configuration (right). (Courtesy of Sandia National Laboratories.)

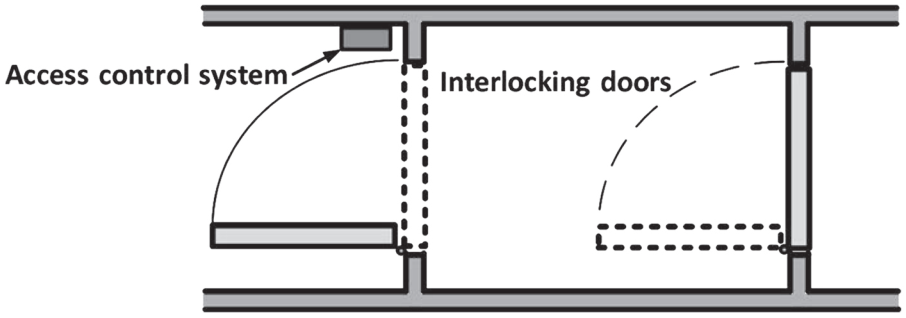


FIG. 32. Personnel portal (sally port) configuration.

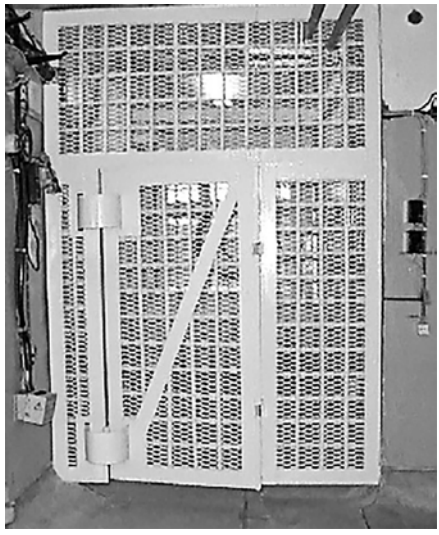


FIG. 33. Hardened steel grated door (may be guarded or unguarded).

4.339. The value of a wall as a barrier should not be reduced by installing standard doors, frames, hinges or other openings. Penetration delay times through access points can be increased by using thicker or composite materials. Explosive and bullet resistant doors and grills with forced entry ratings might offer a substantial increase in resistance to penetration. Doors and their associated frames, hinges, bolts and locks should be strengthened so that they provide the same delay as the floors, walls and ceilings of the structure. For example, high strength vaults for the storage of Category I nuclear material need to have equally high strength vault doors.

4.340. Special consideration should be given to the interaction of safety and security considerations for access points that are part of emergency routes out of a structure and that have delay functions. Measures such as remote lockdown (including temporary blocking of the opening mechanism for emergency doors) in case of an assessed alarm and visual surveillance of the situation might need to be considered. Other solutions might be the installation of interlocking barrier doors or an additional separation device (e.g. hardened turnstiles).

4.341. Since the upgrade and the later hardening of existing access points will be relatively expensive, the number of such access points should be kept to a minimum.

4.342. Standard personnel doors are usually lightweight sheet steel doors, for which penetration times can vary depending on the tools used. Upgrading existing doors might be considered to increase their delay time and balance the overall system of barriers, including strengthening the door face, frame, hinges, exit devices, louvres, glazing and locks, and protecting against penetration attempts with hand, power or thermal tools. The following methods can be used:

(a) Eliminate all unnecessary louvres, external knobs, keyholes and other openings.
(b) Add steel plates to door surfaces.
(c) Add heavy duty hinges to support any added weight.
(d) Add wood cores between door plates to increase delay times for thermal cutting tools.
(e) Weld or bolt a sheet steel strip to the door. This strip should be the same height as the door and at least 5 cm wide with a 2.5 cm overlap onto the adjacent door frame.
(f) Grout the frame with concrete mix at least 45 cm above the frame strike location.
(g) Cut holes in the door frame to allow grouting of both sides of the frame and weld a metal plate over the holes.
(h) Weld the pin top to the hinge.
(i) Use hinges with a stud-in-hole feature.
(j) Prevent removal of the door on the hinge side by using a steel Z-strip bolted or welded to the rear face of the door. If the door hinges are removed and an attempt made to pry the door from its frame, one leg of the Z-strip will come into contact with either the inner frame surface or the rear door stop surface.
(k) Protect panic hardware by adding a hardened steel plate mounted on the inside of a door. The metal plate, to which a drill resistant steel component is fastened, prevents chiselling and wire hooking of the panic bar. This can extend the penetration time considerably if the area between the panic bar and the horizontal leg of the plate is attacked.
(l) Use a single conventional lock with a high security multiple dead bolt system.
(m) Add a second door or grating inside the existing door to balance the delay within the structure.

4.343. At new facilities or when complete door replacement is needed, high security doors with both ballistic protection and forced entry resistance can be fitted to address the threat defined by the threat assessment or design basis threat.

Boundary penetration barriers

4.344. Many boundaries, such as the wall of a building, are designed with openings for windows and utility penetrations. Since these compromise the integrity of the original building wall, barriers are used to make it difficult for an unauthorized person to use the opening to breach the boundary.

4.345. Windows should be upgraded to provide balanced delay, so that they are not the weak link in a barrier system. Standard windows provide no penetration delay to adversaries and need enhancement to provide significant penetration resistance. If a window is operable, the locking mechanism might constitute a weak link that if forced might be opened. Where windows are installed in doors, the metal strips separating the glass from the door are a weak point. The location of the window also affects the upgrading needed: for example, windows close to ground level need more hardening than windows several metres above the ground. The locking mechanism of a window should be located so that it is not readily accessible from outside. The installation of more substantial locking devices or fixed windows might be considered as possible upgrades.

4.346. The strength and weight of the frame material of a window vary widely. Some special window frames contain concealed materials that resist cutting tools, and the attachment of the frame to the structure can be improved by the use of additional or heavier fasteners or by welding the frame fin. However, these enhancements will not affect the delay time through the window unless the glazing materials and protective coverings are also upgraded.

4.347. Standard glass materials are highly frangible. Tempered glass has increased mechanical strength and thermal stress characteristics compared to standard glass. Wire glass is used in fire doors and fire windows and has embedded wire patterns that enhance resistance to penetration. These glazing materials are often upgraded with a protective grill of expanded steel mesh or other forms of metal grill.

4.348. Where a higher level of penetration resistance is needed, thick security glass can be used. Laminated glass is composed of two or more panes of annealed float, sheet or plate glass bonded to a layer (or layers) of plastic. It is more resistant than standard glass to forcible penetration and can be substituted for most glass. However, some types of laminated glass are combustible and their use is restricted by fire regulations. Polycarbonate composite glazing contains a tough core layer of polycarbonate laminated between two outer layers of glass. Composites can be penetrated with hand tools and fire axes, but when the thickest panels are used, the

resistance against forcible entry of steel tools is increased. The impact resistance of polycarbonates approaches the same performance as that of bulletproof glass. Possible further upgrades include the addition of a screen or a bar grid to the interior of the louvre or glazing.

4.349. Utility ports include all types of unattended framed opening other than doors and windows. Nuclear facilities have many such openings, such as ventilation ducts, utility tunnels, crawl spaces, conveyor openings, roof access hatches, exhaust fans and service openings, all of which could be used as a route of entry by an adversary. Such openings at nuclear power plants might also include submerged intake and discharge channels that need to be protected. Utility ports might have covers that can be relatively easily removed so they should be connected to an alarm system and barricaded. Utility ports also often contain grills for safety or ornamental reasons, which can also function as barriers. The penetration resistance of utility ports can be increased by the installation of protective coverings, such as grills, bars, expanded metal mesh or screens. Similarly, grids and grates of steel mesh, expanded metal, bar stock, tubing or bars can be used to reduce the size of the opening in utility ports to prevent human access. Nested ducting or tubing can be used to prevent access to air ducts, culverts or large water lines.

Specialized barriers

4.350. Specialized barriers for specific applications include movable barriers that are placed around areas in which repair and maintenance is taking place or otherwise need to be protected for a limited amount of time (e.g. intermediate storage areas). Massive modular blocks, cargo containers or even parked vehicles can be used to increase delay times of existing barriers, such as in front of the vehicle entrance to a storage location (see Fig. 34).

4.351. Other specialized barriers can provide additional delay directly at locations where unauthorized removal of nuclear material is possible or at locations of sabotage targets. These include high strength storage room doors, double layer steel cages for nuclear material storage and specialized tie-downs (see Figs 35 and 36).

Dispensable barriers

4.352. Dispensable barriers can be active or passive, and can be used to provide additional delay by increasing the time for an adversary to defeat a physical barrier by complicating the task. The dispensable material is normally stored

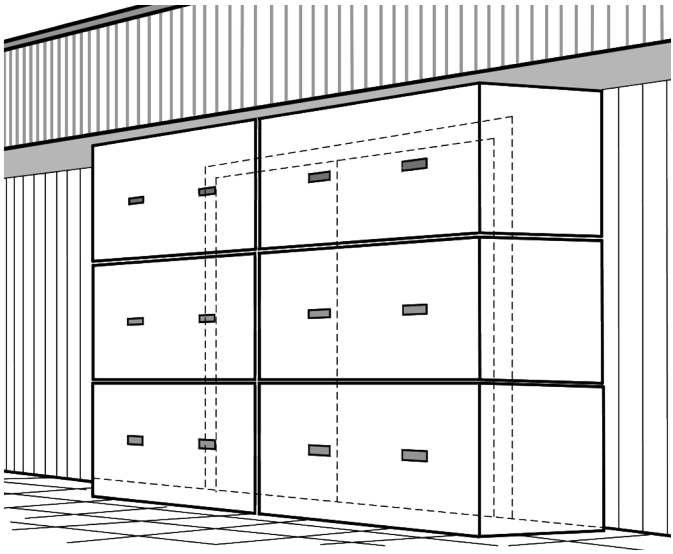


FIG. 34. Massive modular blocks.

in a compact form, and through a chemical or physical reaction expands to fill the opening or space during an attack. Two examples of dispensable barriers are pyrotechnic smoke obscurant and aqueous foam systems.

4.353. Active dispensable barrier systems should be protected against disabling by an adversary or insider and should be designed to avoid accidental activation during other periods (e.g. maintenance). However, they should provide a high level of assurance that the system will activate during an adversary attack (reliability). Consideration might need to be given to safety if such systems are to be activated (correctly or incorrectly) in confined workspaces. A defence in depth measure can include the deployment of a dense obscurant, in combination with concertina or razor wire, and can significantly increase the delay time as compared to the use of razor wire or obscurant alone. Some safety systems may also be usable as dispensable barrier systems. For example, an aqueous foam system for firefighting may also be used as a dispensable barrier system for security, but the manner in which this is done should compromise neither safety nor security.

4.354. Passive dispensable barriers installed in doors or other locations do not depend upon remote or external activation and are relatively simple and inexpensive.

FIG. 35. Double layer steel cage for nuclear material storage. (Courtesy of Sandia National Laboratories.)

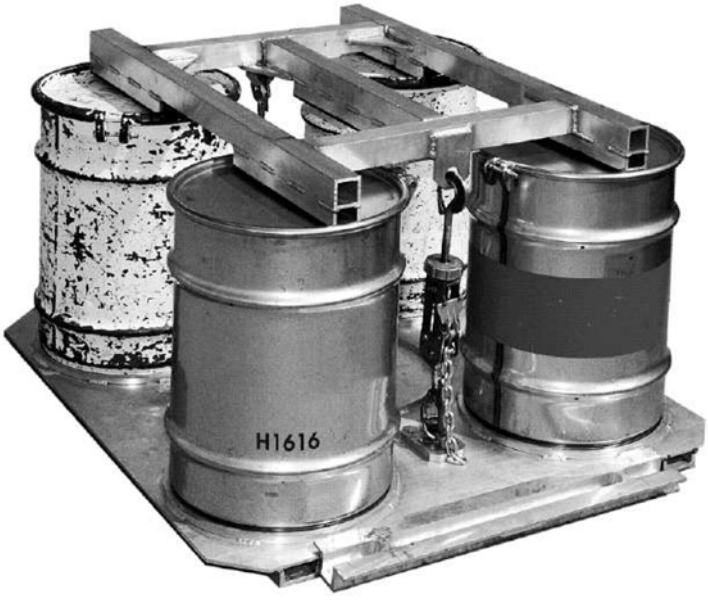


FIG. 36. Specialized tie-down.

4.355. Dispensable barriers should normally be used in conjunction with significant physical barriers to maximize delay on the path to the target location. Dispensable barriers alone provide less benefit in increasing delay times, but might be more effective as barriers against unauthorized removal than sabotage.

4.356. Any use of dispensable barriers, especially activated applications, should be closely coordinated with safety measures during design, installation, maintenance and testing activities to ensure that the safety of personnel is not compromised.

Airborne barriers

4.357. If airborne threats are a credible concern, strategic positioning of poles, cabling or other physical barriers (e.g. barbed tape coil) might restrict some types of airborne vehicle from landing at the facility. Such barriers can be located on the ground or on the roofs of buildings.

Marine barriers

4.358. Marine barriers might be considered where it is necessary to protect against the intrusion of unauthorized water-borne craft. Marine barriers can be permanently fixed or floating. Engineered floating barriers are designed in a modular configuration, constructed of stainless steel beams or reinforced cables, special hinged connections and rigid high density foam encased in polyethylene shells, and modules can be combined in a series to provide the desired length of barrier. Such devices are also used to identify the boundary of the facility in the body of water.

4.359. Engineered floating barriers can be configured in a variety of ways and can be equipped with additional security devices, such as surface barriers, underwater nets and detection devices (see Fig. 37).

4.360. Deployable underwater barriers can be controlled by an electric winch from a remote location or the CAS or manually. These barriers can consist of screens, mesh or other fencing materials.

4.361. Engineered floating barriers are normally installed so that the barrier is fixed to moorings on the shore or to anchors on the bed of the body of water. For a long barrier, multiple intermediate anchoring points might be needed to adequately secure the barrier in place. The installation configuration depends on operating conditions, including the depth of the water, wind directions and tidal conditions.

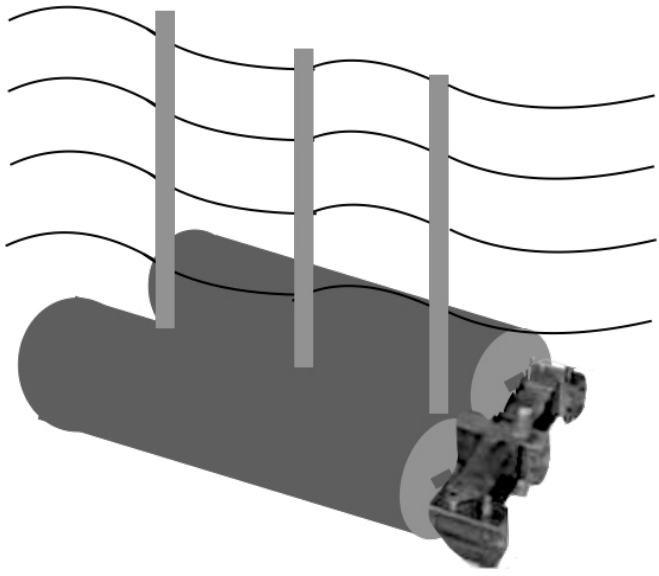


FIG. 37. Double floating barrier configuration with above surface barrier and detection.

Engineered floating barriers can be installed on rivers, lakes, channels, offshore zones and other water areas. Particular attention should be given to anchoring when installing such barriers near or at the cooling water intake or discharge channels, due to the strong currents that might be generated.

4.362. Other marine barriers might consist of fixed structures anchored to the shore, with underwater barriers and detection capabilities (see Fig. 38). Some reinforced concrete sea walls or tsunami walls can also be used as marine barriers.

Role of barriers for stand-off sabotage attacks

4.363. The design of mitigation measures for stand-off sabotage attacks should take into account the robustness of the engineered safety and operational features (e.g. reactor containment, redundancy, physical separation of vital equipment), and fire protection, radiation protection and emergency preparedness and response measures already in place in the facility. Increased guard and response force patrols at potential stand-off locations to deter and disrupt any adversaries might be considered in addition to the use of barriers. When existing measures

FIG. 38. Marine barrier anchored to the shoreline. (Courtesy of the Canadian Nuclear Safety Commission.)

are not sufficient to adequately address stand-off attacks, the following additional protection measures should be considered:

(a) Increasing the stand-off distance by expanding the limited access area or creating larger clear zones outside the perimeter and eliminating areas of concealment.
(b) Installing structures or screens to obscure lines of sight between potential attack locations and targets, thereby reducing the adversary's ability to conduct surveillance, to identify their planned targets and specific vulnerable areas and to provide the response personnel with cover.
(c) Installing physical barriers near to or at targets to mitigate the consequences of a stand-off attack. Barriers can include layers of materials of different densities to make the shockwave from an explosive attack less effective. Multiple barriers spaced out on the outside or inside the structure might cause premature detonation of explosives, forcing adversaries to make multiple accurate attacks. The nature of the threat and State requirements might also affect the placement of the barriers, including the distance of the barriers from the facility.
(d) Modifying layouts and hardening facilities by:
    (i) Constructing or relocating target storage locations underground;
    (ii) Relocating targets within a hardened material storage room within a weaker outer structure that, when attacked, collapses and entombs the inner hardened storage room;
    (iii) Adding a thick overburden of earth to existing or planned facilities.

5. RESPONSE

5.1. Guard duties include activities such as staffing access control points, staffing a CAS, escorting individuals, conducting patrols, assessing alarms, providing timely response and communicating with a CAS or alarm monitoring centre [2]. Response force duties include being prepared to move, communicate and neutralize adversaries as defined in a threat assessment or design basis threat. Response force equipment might include technologies to aid in situational awareness and effective response. This section describes high level considerations regarding equipment, qualification and training.

EQUIPMENT

5.2. Guards and response personnel should be provided with the equipment to perform their routine and response functions. The appropriate equipment for guards and response personnel depends on many factors, including the functions they need to perform, operational and safety requirements of the facility (e.g. use of personal protective equipment), environmental factors and the specific equipment needed to prevent unauthorized removal of nuclear material or sabotage of nuclear material and nuclear facilities.

5.3. In order to fulfil their duties of being able to move (i.e. deploy to an appropriate location), communicate and neutralize an adversary, the response forces' equipment might include vehicles (e.g. hardened vehicles, aircraft, watercraft), communications equipment and weapons.

5.4. Other equipment that might be considered includes technologies that aid in situational awareness, such as a response personnel tracking system and an unmanned aerial system (UAS). Tracking systems allow a tactical commander and response personnel to monitor the locations of the response personnel and vehicles remotely. Technologies such as UAS allow a tactical commander to maintain a real time view of a nuclear security event.

5.5. Consideration should also be given to equipment to protect the response personnel, such as hardened posts and armoured vehicles. Hardened fighting positions can be used to slow adversary forces down, but if they are used, care should be taken to protect such positions against being captured before the responders can reach them. Vehicles such as aircraft or ground vehicles can reduce response time and can be used as stable weapons platforms. If armoured

appropriately, they can also protect off-site responders to some extent against armed adversaries.

QUALIFICATION

5.6. The State should define minimum qualification requirements for those guards and response force personnel that are provided by the operator (as opposed to local law enforcement or military organizations). Operators should ensure that guards and response force personnel (including candidates in training) meet qualifications relating to their health, physical fitness, accuracy and proficiency with firearms, knowledge of procedures and policies, and oral and written communication.

TRAINING

5.7. Training and evaluation should help to ensure that guards and response forces can effectively perform their assigned functions during routine conditions and during a nuclear security event. Results of training and evaluations can be used with other methods to estimate the effectiveness of the response in interrupting and neutralizing adversaries defined in the threat assessment or design basis threat (see also Section 9).

5.8. Training should be based on established requirements, plans and procedures and be conducted in as realistic an environment as possible. This training should use a range of scenarios reflecting adversary capabilities as defined by the threat assessment or design basis threat. Training, tabletop exercises, limited scope and full scope response force exercises and force-on-force exercises (i.e. full scope performance tests) can be used to assess the readiness of the guards and response forces, identify areas needing improvement, and ensure that plans and procedures are appropriate and effective. Training exercises should normally include elements to test the following:

(a) Knowledge of job requirements and procedures;
(b) Response plans (access, denial or containment);
(c) Firearms proficiency, including under reduced light conditions;
(d) Application of less than lethal force;
(e) Adversary tracking.

6. PHYSICAL PROTECTION SYSTEM NETWORKS AND SUPPORT SYSTEMS

PHYSICAL PROTECTION SYSTEM NETWORKS

6.1. Requirements for PPS networks should be identified during the design stage, whenever modifications are planned and when changes to the threat assessment and design basis threat occur. The design of the communication networks, power supply and other support systems should be integrated into the PPS design (see Fig. 39). The PPS should be designed to be resistant to cyberattacks and to provide detection of them (see Refs [10, 17–21] for additional guidance on computer security).

6.2. The integration of PPS networks should be done in a secure manner, taking account of the fact that integration and linking of systems can increase the complexity of the network and might increase the number of ways that an adversary could attempt to compromise the PPS network. Computer security requirements for computer based systems, networks and digital systems should therefore be taken into account from the start of the PPS network design process.

6.3. Computer systems and networks needing protection as recommended in Ref. [1] include those used for the PPS to protect against unauthorized removal of

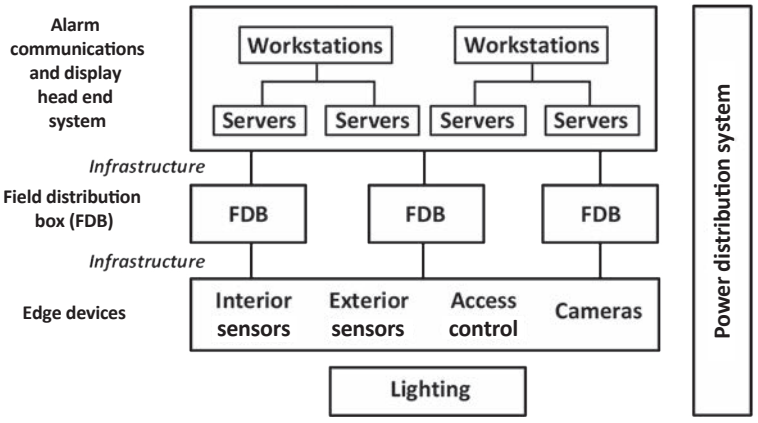


FIG. 39. A typical PPS network and associated devices.

nuclear material or sabotage and those used for nuclear material accounting and control and for safety. Cyberattacks can be aimed at:

(a) Overcoming confidentiality to acquire sensitive information on these systems (see also Section 3);
(b) Compromising the integrity of information on these systems (e.g. altering nuclear material accounting and control records to disguise unauthorized removal of nuclear material);
(c) Denying the availability of a system (e.g. disabling a system important to the PPS or preventing an alarm from reaching the CAS);
(d) Misusing a system function (e.g. unlocking a remotely operated door lock).

6.4. Particular consideration should be given in addressing the security of PPS computers and networks to scenarios in which a system is compromised as a precursor to a physical attack (i.e. as part of a 'blended attack'). In such cases, the cyberattack might occur immediately before the actual attack, but might be carried out much earlier. If compromise of a PPS computer system or network is detected, measures should be taken to determine whether it is intended to alter the system to facilitate a physical attack in the future.

6.5. A wide range of types of computer system are typically used in the PPS of a nuclear facility, including information communications technology systems (which hold and transmit information, including sensitive information), embedded computer systems and instrumentation and control systems (which contain software codes, but whose integrity and availability might be essential for safety). The PPS normally interfaces with operations, nuclear material accounting and control and safety systems, including those for emergency preparedness and response. Guidance is provided for an integrated PPS in Ref. [2] and for the protection of computer based systems in Refs [7, 20], including guidance on establishing an effective computer security programme at nuclear facilities. Guidance on the protection of computer based instrumentation and control systems is given in Ref. [21].

Network design

6.6. PPS network designs vary depending on the size and requirements of the nuclear facility. There are many variables to consider when designing a network to meet current needs and allow for flexibility and growth. Network design should comply with the requirements of the defensive computer security architecture and

the facility's computer security programme [7]. Important considerations to take into account include:

(a) Hierarchy: Designing a hierarchical network allows the designer to break the complex design into smaller and simpler parts. It can also aid in the design of a reliable network infrastructure which might provide a benefit for computer security.
(b) Modularity: By separating the different functions performed by systems on a network into zones, the network can be made easier to design. Modularity might also lead to more stable operation so that failure of one functional area (e.g. a zone or function) will not lead to the total system failure.
(c) Confidentiality: Information relating to the network (e.g. associated databases, files and documentation, change components, simulators) should be protected so that it is not made available or disclosed to unauthorized individuals, entities or processes.
(d) Availability: The network should remain available for use and perform required functions under expected environmental and operational conditions (i.e. normal, abnormal, emergency) for a stated period of time. Abnormal conditions might include hardware or software failures, extreme data traffic loads, unusual data traffic patterns, denial of service events and other unplanned events.
(e) Flexibility: The possibility to modify parts of the network, add new functions, increase future network capacity without going through a major upgrade (e.g. without replacing major hardware devices) or allow for future changes in operations.
(f) Network integrity: Network components should have protective measures to ensure their integrity throughout their service life. Methods to ensure network integrity include design features for controlling physical and logical access to the equipment, detecting unauthorized access to and within the network, and protecting the underlying data.
(g) Complexity: The complexity of the network should be balanced with the protection requirements of the nuclear facility and operations, and maintenance requirements.

6.7. During PPS network design, the needs for both information security and physical protection of communication lines and network nodes should be considered. The system should have means of detecting and registering both explicit and implicit failures of components (e.g. devices, algorithms, signals) [7]. Special attention should be given to the protection measures at computer security zone boundaries (i.e. firewalls, limitation of data traffic) as well as physical and administrative controls.

6.8. The system design should take into account the quality and the operating environment of the components to be installed. Failure modes should be evaluated to understand the potential consequences of failure(s). For example, in a 'tree network' all components attached to a 'branch' might be affected, while the other branches remain unaffected, and installing redundant equipment on the same network branch would simply result in both sets of equipment being affected by the same failure.

6.9. Data communication networks use different architectures to transmit information from one device to another. Network architecture is a method for connecting devices into a single computer network. The type of architecture selected determines the cost, robustness and reliability of the network, and different network architectures can be used to address different needs.

Communication networks

6.10. PPS communication networks and devices should interact with the overall PPS. An automated PPS design should separate critical functions of the PPS, such as perimeter intrusion detection, perimeter monitoring and access control, from other facility networks. The separation of functions will provide an architecture that allows more effective computer security measures.

6.11. An automated facility PPS might include:

(a) Alarm data acquisition and processing system (display and assessment equipment) used to control the intrusion detection system;
(b) Access control system, including automated systems for assigning authentication and identifying authorized personnel;
(c) Video assessment and surveillance;
(d) Communication (voice and data) systems, including to guards and response forces;
(e) Computer and network security components.

6.12. The PPS subsystem devices mentioned above generate, receive and process a range of types of signal (e.g. sensor alarms, video signals for assessment, access control communications, overall system status). For PPS subsystems, all the communication measures can be integrated into a single network or divided across several networks. Integration into a network allows the transfer of information from peripheral devices to computers that perform the function of servers for processing input data.

6.13. Data communication networks might include:

(a) Physical protection devices (e.g. sensors, cameras, alarms);
(b) Peripheral devices interacting with users (e.g. biometrics readers, electromagnetic door locks);
(c) Controllers of devices providing signal processing from several sensors;
(d) Distribution devices (e.g. switchers, routers);
(e) Database servers that process the signals from intermediate distribution devices;
(f) PPS equipment workstations for the CAS, guards and response forces.

6.14. Redundant and diverse data communication paths should be used where possible, and systems are commonly designed so that a secondary system can automatically assume control if the primary system fails. Redundancy provides a more secure communication system by forcing an adversary to defeat or compromise two separate communication paths.

Encryption methods

6.15. Encryption of transmitted data might be used if physical access to PPS communications lines cannot be controlled. However, encryption can cause significant delays in communication as signals are encrypted and decrypted. The risks associated with increased communication times should be evaluated and taken into account while designing the PPS network. Use of encryption should be evaluated during the comprehensive asset inventory undertaken as the basis for a classification of computer systems according to importance [19].

Transmission technology

6.16. The wiring subsystems of a PPS are divided into signal networks and power supply networks. The PPS and lighting subsystems should be operated using an uninterruptible power supply (i.e. alternative or backup power sources are needed at all times).

6.17. PPS data communications can use wire, optical fibre or, exceptionally, wireless links (see Table 5). Wire communication lines are currently the main method of data transfer.

6.18. Wireless signals can be vulnerable to different types of cyberattack, including denial of service (availability) [7]. Any decision to use wireless technology for PPS system communications should be a risk informed decision, and the use

of wireless technology is normally discouraged for those systems requiring the highest security [7].

TABLE 5. TYPES OF CONNECTION FOR COMMUNICATION LINES

Method	Type	Advantages and disadvantages for use in a PPS network
Wire		
Coaxial	Electrical pulses (voltage, e.g. RJ45)	Conventional method Used in television and radio equipment High degree of noise resistance and great mechanical strength
Twisted pair	RS-232 (communication standard) or Category 6 cable	RS-232 has a limited maximum cable length 15 m (standard cable) to 300 m (special cable)
Optical fibre	Light pulses	Not affected by lightning, grounding problems or other sources of electromagnetic radiation 100 times faster than coaxial cable 1000 times faster than twisted pair Transmitter and receiver are required to convert the electrical signal to light and back to an electrical signal Limited bend radius If the fibre runs through a radiation field, potential damage or 'darkening' of the fibre
Multimode	Several rays or modes	Long cable runs might cause signal loss
Single mode	Single ray or mode	Signal transmits over a longer distance than multimode fibre Single mode cable is more expensive than multimode cable
Wireless	Electromagnetic waves, radio, microwave, or infrared (for very short distances) frequencies are used	Solution when no hard lines (wire) options are available Wireless signals are extremely vulnerable to attack Should only be used in very low risk applications Should not be used in a PPS assigned to the highest security level Wireless signals have no clear boundaries

6.19. When considering the use of wireless sensor systems, account should be taken of the possibilities of collisions, signal fade, interference and jamming. Collisions occur when two or more signals are received simultaneously, resulting in neither message being read by the receiver. Signal fading can occur when the path between the transmitter and receiver is too long or is blocked by material that shields the signal, such as large metal objects or structures. Interference occurs when other sources transmitting in the same frequency range overlap the signal sent by the sensor or transmitter unit. Jamming is intentional interference initiated by an adversary so that alarm signals do not reach the receiver. Wireless signals are also susceptible to interception and falsification.

PHYSICAL PROTECTION SYSTEM SUPPORT SYSTEMS

Power and backup systems

6.20. The purpose of the power system is to provide a reliable power source for PPSs and subsystems during normal operation and emergency conditions. Redundancy can prevent individual component failures from leading to failure of the whole system. Depending on requirements, electricity can be supplied by one or a combination of the following methods:

(a) Off-site commercial power supply;
(b) Uninterruptible power supplies and batteries;
(c) Standby generators.

6.21. For the most sensitive facilities, it might be desirable to have two separate off-site power sources to reduce the likelihood of interruption. The off-site power sources should not be collocated to ensure that a single event does not result in power interruption. Other considerations for PPS power sources include the power consumption that needs to be met and compatibility with the power distribution network (e.g. power lines, distribution cabinets, connections, conduits), including loading limitations for all PPS components and subsystems.

6.22. If off-site power to the PPS is lost, an uninterruptible power supply should immediately provide electrical power to support the continued operation of PPS equipment designated as critical, such as sensors, alarms, communication components and surveillance cameras. An uninterruptible power supply, which is normally battery powered, provides temporary electrical supply to the PPS until the automatic transfer of the electrical load from the normal power source to the emergency power source (usually an emergency generator). Audible and visual

indication of any power failure and subsequent restoration should be provided to the CAS, including indication of the status of the emergency generator when available. Perimeter lighting typically does not use the uninterruptible power supply or battery power sources because of its large power usage.

6.23. The uninterruptible power supply and backup generators could provide a route for an adversary to attack PPS systems and so should be subject to protection measures, including computer security. Protection considerations for standby power might include the following:

(a) Installation within a controlled area or hardened building inside the perimeter (in some cases within a vital area);
(b) Installation of sensors to detect tampering and unauthorized access;
(c) Automatic startup upon failure of the primary power;
(d) Routine maintenance testing under load to ensure continuing efficiency and effectiveness;
(e) Routine checks of output voltage to address the initial power surge;
(f) Monitoring of uninterruptible power supply batteries and charging systems, including time to recharge, from the CAS;
(g) Defining the safe load and time for which the PPS equipment can operate on backup power (e.g. adequate fuel storage and supply);
(h) Providing adequate capacity to power the PPS, CAS and backup station;
(i) Providing power to essential PPS equipment to ensure continued operation.

6.24. The capability to switch to a backup network provides redundancy for PPS network equipment operation in case of damage to a network element, and can mitigate the effect of a complete failure of the whole subsystem or its components. Backup networks are more robust if different technologies and equipment (i.e. diversity) are used and no interconnections exist.

Location and protection requirements for stationary equipment

6.25. Maintenance workstations used for PPS equipment and network devices (especially servers) should be located in an access controlled area (e.g. in locked cabinets or rooms with access control and alarms). A two-person rule or other measures can be used for access to network servers and workstations to provide administrative protection of equipment and to ensure configuration management.

Protection considerations of network cables

6.26. All PPS signal cables should be located, wherever possible, within a protected area to restrict access. Where network cables are not located in a secure area and sensitive data is transmitted over these cables, data should be encrypted, signal supervision should be used and the lines should be protected in metal conduits and junction boxes, with welded joints. To increase protection, conduits should ideally be enclosed or buried. Cables will normally be exposed at both terminal locations and are particularly vulnerable to attack at these points.

6.27. The communications lines used for transmitting sensitive information should also be controlled and monitored through computer security measures to ensure that integrity of both the line and signal is maintained and to provide an indication of potential intrusions or component failure [7]. Controls on individual ports should be considered, including shutdown if there is an indication of potential malicious activity.

Tamper protection

6.28. Tamper protection should be incorporated into the hardware and system design, for example by means of sensors to indicate an adversary approaching the equipment or lines. Tamper protection or line supervision should be used for the following:

(a) Electronics and junction box enclosures of sensors, with tamper switches that generate an alarm if opened;
(b) Communication lines for alarms, with line supervision to detect lines that have been cut, disconnected, short circuited or bypassed.

Physical protection system network maintenance and testing

6.29. PPS network devices are continuously exposed to operating conditions that can reduce the life of the components (e.g. weather conditions, mechanical impacts, voltage variations, radiation fields). Periodic preventive maintenance of the physical protection network will increase PPS availability and extend the operational life. PPS network maintenance and testing activities should comply with computer security requirements.

6.30. 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.

6.31. The operator should establish procedures and schedules for the preventive maintenance of PPS network systems based on the type of equipment installed, the conditions under which the equipment operates and the maintenance history of the equipment.

6.32. The life cycle of PPS network components and systems should be managed to ensure that components are replaced before they fail due to ageing or obsolescence, taking account of manufacturers' claimed or historically observed lifetimes. The following activities can facilitate recovery in case of unpredicted failures:

(a) Modular design to allow for rapid replacement and return to service.
(b) Frequent backup of the databases and system configuration.
(c) Documented recovery procedures to return the network to full operability after an outage.
(d) Availability of original or compatible spare parts and equipment. Changes in vendors and suppliers might need monitoring to ensure this availability.

7. NEW AND EMERGING TECHNOLOGIES

7.1. New and emerging technologies need to be evaluated (and, in the case of protective technologies, adopted as appropriate) to address technology development and new and emerging threats. This evaluation can facilitate the adoption of technologies that reduce costs, improve effectiveness, mitigate risk associated with new and emerging threats, and improve overall PPS functionality and capability.

7.2. To be successful, use of new PPS technology should be based on identifying the most appropriate available technology to solve a problem, using the technology within its intended design capabilities, effectively integrating different technologies and only incorporating advanced technologies that are sufficiently mature. Manufacturer's claims about their technology should be considered carefully, including consideration of the suitability and reliability of the technology for the needs and environment of a facility.

7.3. This section provides guidance for evaluating technology needs or gaps in an existing PPS, identifying candidate technologies to address needs or gaps and evaluating them before procurement and implementation. A technology need or gap is a limitation in the currently implemented PPS or a lack of capability to address an existing or future need. Conceptually, the difference between current PPS technologies and new and emerging technologies is simply whether or not a given PPS technology is commonly used at nuclear facilities within a State.

7.4. A State or operator might develop a structured technology management framework to ensure that new and emerging PPS technologies are integrated with existing systems. The objective of such a framework is to identify and develop new and emerging security technologies and to ensure that they will be effective and reliable in the relevant environment, and available for use.

7.5. It is advisable that the management framework:

(a) Identify new and emerging threats and identify how they could affect the facility, and define any new or upgraded security measures needed;
(b) Identify research and development or new technologies that will help address emerging threats and common needs;
(c) Identify technologies that best address a defined need and have undergone sufficient tests and evaluations;
(d) Integrate PPS technologies at a nuclear facility to achieve overall system objectives;
(e) Ensure that the new technology is sufficiently mature for use at a nuclear facility.

7.6. A suggested framework for new and emerging technologies includes formalized processes for conducting needs assessment, tests and evaluation and technology deployment (see Fig. 40). Within the proposed framework, a needs assessment is used to identify areas where technology might address existing gaps or issues, and research and development that could support potential technologies to address future needs and threats. Candidate technologies are then screened to identify those that can be developed into or used in their current state as mature, viable solutions to defined needs. The final stage is to accept mature security technologies that are ready to be used in facilities as needed and that can be integrated with other security technologies.

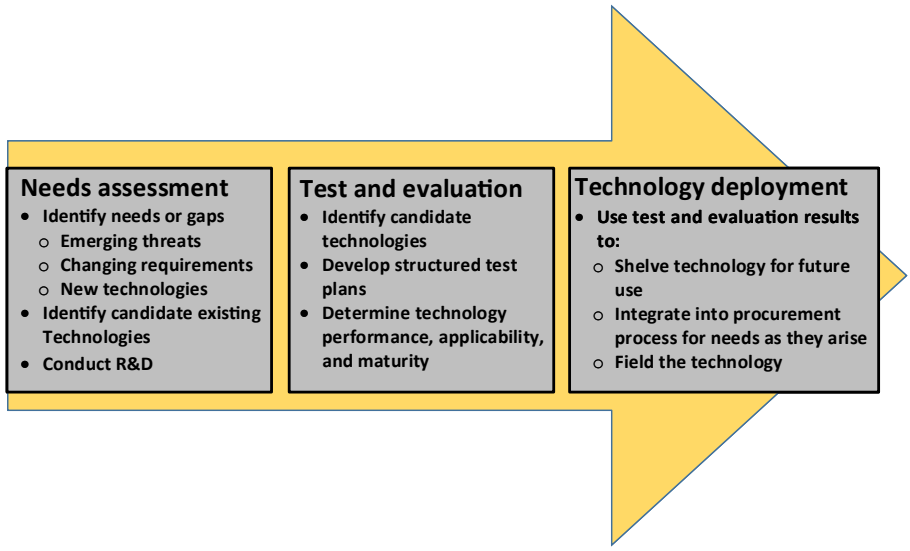


FIG. 40. Proposed technology management framework.

NEEDS ASSESSMENT

7.7. A needs assessment is a systematic process used to determine needs, examine their nature and causes and set priorities for future action to address them (see Fig. 41). It focuses on the goals to be achieved rather than the means to achieve them. The goals might be influenced by many factors, such as changes in the threats, changes in regulatory requirements, changes in operations at a nuclear facility or a desire to increase effectiveness or efficiency of the PPS. The results are used to set priorities and to determine criteria for potential solutions to help decision makers reach sound decisions on how to best allocate available resources.

7.8. The first step in a needs assessment is determining the current state of the existing PPS and the current threat. Issues or concerns are identified from a number of sources, including from assessments or evaluations, from analyses of the performance of a PPS, or from changes in the threat, regulatory requirements or facility operations. Measurable indicators of need should be developed where possible. For example, existing sensors might have a tested sensing probability of 0.75, whereas the desired (or required) performance is a sensing probability of 0.80. Sources of data to analyse the issue in detail should also be identified.

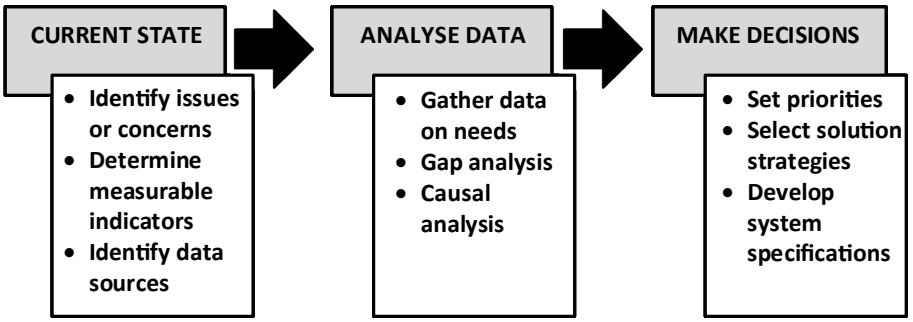


FIG. 41. Needs assessment process.

7.9. Data are then gathered to analyse each identified issue. A gap analysis should be conducted to identify specific areas in any system that needs improvement, and thereby to identify gaps between the current state and the desired state. A causal analysis is a structured analysis to determine what led to the identified issue or gap to help to ensure that any solutions identified will address the actual cause of the issue and not just a symptom. For example, the sensor in the example above might have a low sensing probability due to limitations of the communication between the sensor and the alarm communication and display system and not due to the sensor hardware itself. Replacing the sensor in this case would not address the root cause of the issue.

7.10. The results of the needs assessment analysis phase are documented to provide information that decision makers can use to establish priorities, select strategies and develop specifications for PPS technologies that have the potential to meet the defined needs to be considered in the test and evaluation process.

TESTING AND EVALUATION

7.11. The purpose of testing and evaluation is to provide information to decision makers by verifying and validating performance requirements, assessing how well a technology meets those requirements, and determining whether systems are mature, operationally effective and suitable for the intended use. During the early phases of evaluation of a new technology, testing and evaluation are conducted to demonstrate the feasibility of conceptual approaches, evaluate design risks, identify design alternatives, compare and analyse trade-offs, and estimate the feasibility of meeting operational requirements. As a new technology undergoes design and development, the iterative process of testing gradually moves from

design testing and evaluation, which is chiefly concerned with the attainment of engineering design goals and the verification of technical specifications, to operational testing and evaluation, which focuses on questions of operational effectiveness and suitability to address a defined need.

7.12. Formalized testing and evaluation processes have been developed for hardware, but the processes also need to be applied and adapted to provide effective testing of software. In both cases, the testing and evaluation process needs to be thorough, logical, systematic and iterative, with early testing followed by feedback of well documented and unbiased test and evaluation results to system developers, users and decision makers.

7.13. Most testing and evaluation processes can be summarized in four major steps:

(1) Developing test objectives.
(2) Developing a pre-test plan (including expected results from the tests).
(3) Conducting tests, including:
    (i) Developing detailed test plans;
    (ii) Gathering test data;
    (iii) Analysing test data;
    (iv) Documenting test results.
(4) Conducting and documenting post-test evaluation.

7.14. Test objectives are developed based on the results of the needs analysis and might relate to factors such as performance specifications, user needs, environmental or operational requirements, human interface requirements, mean time between failures, ability to integrate with other systems and ease of maintenance.

7.15. Pre-test analysis of the evaluation objectives is used to determine the types and quantities of data needed, the results expected from the tests and the analytical tools needed to conduct the tests and evaluations. Consideration can also be given during the pre-test analysis to how to design test scenarios, how to set up the test environment, how to record the tests, what resources are needed, the best sequence for the tests and how to estimate test outcomes.

7.16. Conducting the tests involves developing specific test plans, performing the tests, gathering and analysing data and documenting the test results. The tests should be planned and conducted to provide sufficient data to support analysis. The data should then be reviewed for completeness, accuracy and validity before being used for the final step in the process.

7.17. The final step in the process is post-test evaluation, which is the comparison of the measured outcomes (the test data) with the expected outcomes, evaluating the data and applying technical and operational judgement. When the measured outcomes differ from the expected outcomes, the test conditions and procedures should be re-examined to determine whether the performance deviations are real or the result of test conditions. Such deviations might result from inaccurate computer simulations [2], deficiencies in the test equipment or conditions, instrumentation errors or errors in the testing processes. Parameters studied to represent the operational environment, systems performance and logistics support should be carefully chosen, fully described and documented before testing. Modelling and simulation can be used during the data analysis to support the evaluation of performance, effectiveness and suitability.

TECHNOLOGY DEPLOYMENT

7.18. Technology deployment is the process of adding a new or improved technology to an existing system. The aim is to deploy the technology consistent with security requirements within a reasonable time and at the lowest cost. The goals of technology deployment are:

(a) To use the best technology available from all sources, as applicable;
(b) To deploy the technology rapidly after selection;
(c) To refresh the technology, as needed, to maintain an effective PPS throughout the life of the system.

7.19. Technology deployment addresses the following objectives:

(a) To improve and refresh an existing PPS as needed;
(b) To maintain functionality of systems or components of a PPS by updating technologies to prevent obsolescence in an existing system;
(c) To enhance the functionality of systems or components of a PPS by upgrading a technology or adding new technology to enhance the capability of the existing PPS.

8. PERIODIC EQUIPMENT TESTING

TYPES OF TESTING

8.1. Periodic equipment testing includes acceptance and sustainability testing, which includes the following:

(a) Pre-acceptance testing, performed during installation to ensure that all hardware and software components are operational and interacting correctly;
(b) Acceptance testing, performed to demonstrate that installed components or systems have been implemented as designed and will operate as designed;
(c) Operability and functional testing, performed to indicate that physical protection components are working and are functioning as intended;
(d) Maintenance and calibration testing, performed to determine whether the PPS components and subsystems are correctly installed, aligned and calibrated.

8.2. These different types of testing can be performed as separate processes, be combined as part of a comprehensive maintenance and testing process, or support a quality assurance programme as part of an integrated management system (see Section 11). For example, operability and functional testing can be performed once a day on a certain PPS element as a distinct process. At the same time, the same element can undergo operability, functional and calibration testing after maintenance, before acceptance testing, and if the element passes all tests, it is placed back into operation. Paragraphs 8.3–8.16 describe the types of test in greater detail.

Pre-acceptance testing

8.3. Following the installation of new PPSs and subsystems, all physical protection components should undergo pre-acceptance testing to ensure that all hardware and software components are operational and interacting correctly. This process includes point to point testing along the entire network to ensure that all alarm communications are functioning and report to a CAS or other location as needed. The process includes testing of all hardware, software, voice and data communications, lighting, power and backup systems. This testing is typically part of the construction phase of a facility and is conducted before formal transfer from the constructing organization to the operating organization.

Acceptance testing

8.4. The operator should perform acceptance tests to ensure that the PPS measures are fully functional in all aspects of operation and meet design specifications before acceptance. Testing should include all system and subsystem components of the PPS. Acceptance testing is the broadest part of testing, including checking the correct installation of all components and subsystems, and also determining and documenting baselines for performance, operability and function. Acceptance tests are intended to identify any operational and functionality problems that need to be addressed to ensure system operation in accordance with design specifications and requirements. This type of testing is applied to all PPS hardware and software, voice and data communications, lighting, power and backup systems.

8.5. Acceptance testing should be thoroughly planned and documented in an acceptance testing plan that defines the test objectives, scope of testing, approvals for testing, responsibilities, testing approach, fault and data recording, resource specifications and test environment, and describes each planned test. Test plans should be developed to include specifications, a description of the test, initial test conditions, the detailed test procedure, expected results and any special factors. An effective acceptance test plan depends upon design specifications that are clearly defined, measurable and readily tested.

Operability and functional testing

8.6. Operability and functional testing is intended to ensure that PPS measures, components and subsystems function initially upon installation and continue to function and operate correctly. These tests are conducted routinely to determine significant PPS component or subsystem malfunctions or outages. 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. For example, guards might be assigned to periodically ensure the metal detection portal is receiving power and to walk through a metal detection portal to determine whether the metal items they normally carry cause a visual and audible alarm, as they should, or to open a door that has a balanced magnetic switch and confirm that an alarm is generated. Operability and functional tests might also be applied to subsystems. For example, a guard patrolling might be assigned to walk into the area monitored by a volumetric intrusion sensor with CCTV to confirm that an alarm is generated. The CAS personnel would determine whether the alarm is received from the sensor, and whether the appropriate camera was activated and is providing a camera image of sufficient quality to determine that a human set off the alarm.

8.7. Operability and functional tests should normally be performed on a relatively frequent schedule (e.g. from once every shift to once per week as appropriate) to ensure continuous operation of components and subsystems. Any problems identified by operability and functional tests should be promptly corrected or compensatory measures implemented until corrective actions are completed.

8.8. Operability and functional tests can be performed manually by a human tester or using remote or self-testing capabilities. Examples of manual tests include balanced magnetic switch test described above, or a technician inspecting a perimeter after a storm to determine whether sensors or cameras have been damaged or appear to have been moved out of alignment.

8.9. Manual testing of PPS components is strongly preferred. In certain circumstances, however, for example due to staffing limitations or the remoteness of intrusion detection systems, manual testing might not be possible or might be impractical. In such cases, a capability for remote or self-testing might be used, in which the alarm communication and control system itself triggers a test signal. For example, a self-test might begin with the intrusion detection system generating a test trigger to a specific sensor at a random time, and the sensor would be expected to respond with an alarm. The intrusion detection system would subsequently check that the alarm occurred within a specified time of the test trigger, and was cleared by the operator within a specified time. Failure to pass a remote or self-test should produce an alarm message, indicating the possibility of hardware failure or tampering, and this should be investigated. Remote and self-test techniques currently available might identify that the sensor is working, but cannot test the sensor's calibration or alignment, and therefore a remote self-test should supplement, and not replace, manual testing.

Maintenance and calibration testing

8.10. Maintenance and calibration tests are conducted to determine whether the PPS components and subsystems are correctly installed, aligned and calibrated according to specifications. Such testing would also be conducted as part of, or in conjunction with, initial acceptance testing or following maintenance activities. For example, a maintenance or calibration test of a metal or radiation detection portal monitor might involve repeatedly walking through the portal with a specified test source to demonstrate that the detector has an acceptable detection probability for that source. Another example might be a trained technician testing a perimeter sensor by walking, running, jumping, climbing or crawling (as appropriate) in the detection area to demonstrate that the sensor provides the required probability of sensing.

8.11. Well designed maintenance and calibration tests will detect whether component performance has deteriorated over time, whether spare parts appear to be defective or whether a component might have been tampered with. Maintenance and calibration tests should be conducted in a consistent fashion and provide repeatable results to ensure that a device passing the test on one day but failing the next indicates some degradation of the device's performance and not a variation in how the test was conducted. Consistency and repeatability can be achieved by providing a detailed set of procedures and training the tester, or by using an approved testing device that simulates an adversary crossing the sensor (e.g. using a tool to pull the fence fabric with a consistent force to simulate a climber).

On-site testing

8.12. Since facility design and environmental conditions are facility specific, the operator should conduct on-site performance testing to establish and validate the values used in assessments of PPS effectiveness (see Section 9). If the facility is operating, detailed coordination is needed between facility operations and security personnel to ensure that protection measures are maintained during the testing period, including where necessary through previously approved compensatory measures. If a deficiency is identified through testing or a protection element is defeated as part of a test (e.g. a fence is successfully cut through), compensatory measures should be implemented and corrective actions initiated immediately. The compensatory measures should remain in place until corrective actions are completed and evaluated.

USE OF DEDICATED TEST BEDS

8.13. Performance testing on dedicated test beds located at the facility or at another testing location can be used to test 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 might include facilities to test interior and exterior PPS systems and infrastructure to support sensor testing, data gathering and data recording. The test bed might 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.

8.14. A test bed located at a facility provides the possibility of testing and monitoring PPS measures under facility specific environmental and industrial conditions, to better understand how these factors affect performance and nuisance alarm

rates. Such a test bed can also be used to evaluate physical protection components and subsystems before a facility is built. It is advisable that the components or subsystems be monitored and tested to cover all feasible weather conditions.

8.15. A dedicated test bed might also be used to obtain realistic performance data to assess new technologies and to train personnel for operation and maintenance of the PPS. A test bed can be used to identify facility specific maintenance and calibration tests, and for testing the performance of a barrier or intrusion detection system that cannot be tested on the facility itself due to cost or facility considerations such as personnel safety (e.g. in a high radiation or contaminated area).

8.16. Such tests can provide the data needed to develop specific physical barrier delay times. If these tests are documented properly, the results can be used to develop a data library of PPS element attributes (e.g. barrier delay times) to support the use of similar protection measures at other nuclear facilities within the State without the need to repeat testing. Similarly, barrier delay times can be collected for a range of adversary tactics, such as use of hand tools, power tools, explosives and vehicles, as applicable.

9. PHYSICAL PROTECTION SYSTEM EVALUATION

9.1. The purpose of PPS evaluation is to determine whether the PPS meets prescriptive requirements or performance objectives. The methods and sources used to gather, analyse and manage the data used in the evaluation directly influence its validity. All physical protection measures, including the people, plans, procedures and equipment involved, should be included in the evaluation to determine whether the PPS as a whole is effective to meet the defined requirements and objectives. This section provides an overview of methods that can be used to evaluate PPS effectiveness.

9.2. PPS design requirements specified by a State might be of the following types:

(a) A prescriptive regulatory approach where the State identifies specific requirements to fulfil its defined physical protection objectives. A prescriptive requirement is met if the required measures are in place: for example, ‘a 2.4 m chain link fence is required on the boundary of the limited access area.’ Prescriptive requirements might include performance criteria

that are measured in technical terms, not in terms of effectiveness against the threat assessment or design basis threat.

(b) A performance based regulatory approach where a general requirement is specified in terms of the overall objectives of the PPS as a whole against the threat defined in the threat assessment or design basis threat. For example, a performance based requirement could be to prevent theft of Category I nuclear material by a specific adversary equipped with rifles, bulk explosives and a commercial vehicle, or to detect an intrusion into a facility containing a quantity of Category III nuclear material and report to the local police immediately and the competent authority within 24 hours.

(c) A combined prescriptive and performance based regulatory approach, where some requirements might be defined in terms of effectiveness against the threat assessment or design basis threat, and some might be defined in terms of presence or absence of one or more specific measures that the State prescribes (perhaps meeting associated technical criteria). Other requirements might also include a combination of these two aspects.

9.3. Measuring the effectiveness of a PPS designed to meet prescriptive requirements simply involves determining whether or not all of the specific requirements have been fully met. Prescriptive requirements can usually be evaluated by direct observation at the nuclear facility, for example observations of operational plans and procedures, records and logs, personnel training, interviews and observations of the PPS operation.

9.4. Measuring the effectiveness of a PPS designed to meet performance requirements typically involves conducting performance tests, such as exercises [2]. Performance testing is not possible for a facility being designed, so other methods, such as computer simulations, may be used. The evaluation of performance requirements might include both direct comparative reviews and independent testing to validate that each PPS element meets performance requirements and specifications.

9.5. When evaluations indicate that any element of the PPS is deficient or not performing adequately, immediate corrective action including compensatory measures might be needed, along with notification of the competent authority as required. A PPS evaluation can also be used:

(a) To improve the effectiveness of the PPS by identifying efficiencies and deficiencies;

(b) To adjust the PPS capability where it significantly exceeds or does not meet regulatory requirements;

(c) To compare the effectiveness of several PPS design options to support selection of the best option.

9.6. Independent reviews, such as those provided by the IAEA's International Physical Protection Advisory Service, could also be considered to support evaluation of a facility's PPS.

PRESCRIPTIVE VERIFICATION

9.7. Using the prescriptive regulatory approach, the State establishes specific physical protection requirements to meet its defined physical protection objectives for unauthorized removal of each category of nuclear material and for each level of radiological consequences from sabotage [2]. These requirements provide a set of 'baseline' provisions or criteria that the operator is required to apply for each category of material and each level of radiological consequences.

9.8. Prescriptive requirements can generally be evaluated by direct observation, measurement or examination of records, combined with testing of individual PPS elements. Examples of prescriptive requirements include the following:

(a) Specific features (e.g. wall, fence, camera) have to be present.
(b) A physical protection measure has to meet directly measurable parameters (e.g. a minimum wall thickness or fence height).
(c) Physical protection equipment needs to have a certificate or other officially recognized documentation to confirm its specification.
(d) Guards need to have certain qualifications, possess specific types of equipment and be knowledgeable in their use.
(e) A perimeter sensor has to be designed, operated and periodically tested to ensure that it provides at least a defined probability of sensing with at least a minimum level of confidence for a person crawling, walking or running in the detection area.

9.9. An evaluation of a PPS against prescriptive requirements should always be performed before other evaluations, for example if performance based requirements are also to be evaluated.

Prescriptive evaluation methods

9.10. An evaluation of a PPS against prescriptive requirements involves understanding the requirements, gathering information and comparing the

information against the requirements to determine compliance. The following methods are used to acquire the information needed to determine compliance:

(a) Reviews of written material such as plans, procedures, training lesson plans, logs and records.
(b) Interviews with personnel involved in designing, operating, managing and maintaining the PPS. Interviews might also be conducted with facility personnel not directly involved with the PPS to provide a broader understanding of how physical protection measures are implemented in practice.
(c) Direct observations of the organization, practices and systems in place for the PPS and specific measures at facilities.
(d) Using all of the above to perform an objective assessment with regard to the compliance of the PPS against each prescriptive requirement.

PERFORMANCE TESTING

9.11. Performance testing is used to validate the ability of a PPS to meet performance requirements, but it may also be required where a prescribed measure has to meet some technical criterion or specification.

9.12. The choice of which PPS components and measures to test might be based on facility operation, test schedules or a requirement of a competent authority. Specific measures might also be tested based on lessons identified from operational experience, results of previous assessments or nuclear security events, or other information indicating a potential weakness in the PPS.

9.13. Performance tests of individual physical protection measures or a combination of PPS measures can be conducted for a variety of reasons, including:

(a) Tests to determine values for performance indicators (e.g. detection probabilities, delay times) representing how well physical protection measures perform against adversaries with different capabilities, as specified in the threat assessment or design basis threat;
(b) Tests to determine methods by which an adversary might seek to defeat technical measures and subsystems (which might be used to support fault tree analyses).

9.14. Other considerations in developing a programme of performance testing, including exercises, to support PPS evaluation include the following:

(a) Developing a plan to validate compliance with requirements and performance of the PPS. The plan should provide a basis for the design and frequency of the performance testing and criteria for the evaluation. The plan should ensure that the evaluation determines whether criteria are met for reliability, operability, functionality, readiness and performance.
(b) Ensuring that performance tests, including exercises, are conducted periodically and coordinated with external response organizations at a frequency determined by the competent authority.
(c) Integrating other parts of the operating organization (e.g. emergency response, facility personnel, control room staff) into exercises to make them realistic and to test the different disciplines working together during a nuclear security event.
(d) Documenting results of the evaluations, including corrective actions needed and, where appropriate, reporting the results and findings to the competent authority.
(e) Engaging with other operators or organizations to share lessons identified and best practices, including on the process of conducting evaluations and the results.

9.15. The PPS performance testing programme should make use of data from other existing testing conducted by maintenance personnel as part of the quality assurance programme. It is advisable for the performance testing programme to have elements to coordinate the design, planning and conduct of the tests and management of the data derived from the tests, including the following:

(a) Integrating data from other testing, such as in maintenance and training, to identify common test objectives and methods and to make the most effective use of test data;
(b) Ensuring resources are integrated with the facility's operational schedules to minimize disruption;
(c) Developing test plans to establish the objectives, methods, procedures and criteria for the testing;
(d) Designing tests to obtain sufficient data to support quantitative evaluation with an appropriate degree of statistical confidence;
(e) Conducting testing with qualified personnel, trained in the operation of the PPS element being tested and with the related procedures;
(f) Performing the tests with impartial test personnel to ensure data integrity;

(g) Managing the different attributes of test data to understand how to interpret and apply the data;
(h) Developing a data management plan to guide the effective collection, analyses and maintenance of the test data.

9.16. Performance tests should be repeatable and objective: testing by different experts using the same test plan should yield comparable results. The test methodology should be structured to ensure the most efficient and accurate use of individual test results and observations. Established international standards[5] can provide good practices in the use of data sampling and test design.

Performance evaluation methods

9.17. Performance tests used for evaluation include limited scope and full scope response force exercises and force-on-force exercises and are designed to determine whether personnel, procedures and equipment provide the necessary levels of performance. These tests can be designed to test performance of a single PPS component or of a subsystem of the overall PPS. For example, a limited scope test might be an exercise to measure response and assessment times for a particular target, or a test to determine whether a CAS operator can interact with the intrusion detection system to identify the source of an alarm in a storage area within a designated time.

9.18. When practical, multiple performance tests can be conducted for each physical protection element to gather a representative range of test data. For example, three exercises might be performed to determine response times, one for each of the three shifts of responders. Video recordings can be used to record test data.

9.19. Performance testing data might be maintained in a data library that can then be used as a basis to justify assumptions about probabilities of sensing, assessment, delay and response times used in physical protection evaluations. Section 8 provides further information on collecting test data.

Limited scope performance tests

9.20. Limited scope performance tests can be used to test any operation or procedure, verify that a policy is being followed, or verify a required knowledge

[5] For example, those drafted at the International Organization for Standardization's Technical Committee 69 on Applications of Statistical Methods.

or skill. Evaluation techniques such as observations and interviews do not need test plans, but limited scope performance tests should be formally documented and approved in advance. Specific pass/fail test criteria and expected results should be identified to ensure data collection and analysis methods are useful and cost effective for the overall PPS evaluation. Limited scope performance tests can be scheduled or unannounced. During any evaluation process, multiple test techniques should ideally be used to determine whether personnel assigned to PPS activities are performing their assigned functions effectively.

9.21. 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 include the direct observation of a specific activity or process or evaluation of specific actions or responses to an anomalous condition. Limited scope performance tests can provide an indication of a specific protection capability, while multiple tests for a series of actions can provide increased assurance of an overall capability.

9.22. Limited scope performance tests can be focused to evaluate specific PPS measures, plans or procedures or to gather data for training and qualification of operations personnel, security specialists and guards.

Full scope performance tests

9.23. Full scope performance testing includes both full scope response exercises and force-on-force exercises. Both types of exercise are integrated tests designed to evaluate all the measures employed in response to an attack by a specific adversary at a facility. Where a full scope response exercise verifies the response plan, timelines and procedures, the force-on-force exercise allows realistic evaluation and verification of the effectiveness of the PPS. Data can be gathered to validate assumptions, assess the effectiveness of the PPS against defined threats and evaluate the ability to implement protection strategies, assess training and identify areas needing improvement.

9.24. Force-on-force exercises need extensive planning and coordination with all parts of the operating organization, including managers, facility personnel, staff with physical protection responsibilities, emergency responders and off-site responders. Such exercises are also demanding and costly, so careful planning and coordination are needed to obtain the maximum benefit. Simulated weapons can be used to collect data on adversary and response force personnel engagement during the exercise. An overall exercise plan should be used to plan, coordinate and implement a force-on-force exercise and record meaningful data from it.

Many elements might be included, but a force-on-force exercise plan normally includes at least the following:

(a) Clear test objectives;
(b) General and specific attack scenarios;
(c) Specific adversaries and capabilities (from the threat assessment or design basis threat);
(d) Facility (or facilities) involved and exercise boundaries;
(e) Compensatory measures to protect the facility during the test, including a shadow force (additional response force on standby) if required;
(f) Measures to protect the participants during the exercise, including specific actions to be taken by exercise participants if an actual response is initiated during the exercise;
(g) Communication between the exercise participants and shadow forces to ensure no compromise of safety or security during the exercise;
(h) Test methodology;
(i) Schedule.

Scenario development

9.25. Force-on-force exercises and limited scope tests are based on specific attack scenarios. In developing such scenarios, subject matter experts aim to develop a range of scenarios to address the threats defined in the threat assessment or design basis threat. These scenarios can include external adversaries, insider threats or attacks involving collusion between them. Information used to develop scenarios is derived from many sources, including the following:

(a) Characteristics of the nuclear facility;
(b) Characteristics of the specific targets for unauthorized removal and sabotage;
(c) Characteristics and capabilities of the adversaries, as indicated in the threat assessment or design basis threat;
(d) Results of previous analyses, such as a path analysis.

9.26. Some considerations for developing adversary scenarios include:

(a) The capabilities of the adversaries (including the combination of tactics to be used, e.g. force, stealth or deceit);
(b) Different facility operating conditions at the time of the attack (e.g. nuclear material vault open or closed);
(c) The amount of information an adversary might have;
(d) Any actions of an insider in a collusion scenario.

9.27. When a range of scenarios has been developed, a scenario or scenarios should be selected to be tested in a force-on-force exercise or during the PPS evaluation. Considerations for selection include identifying a 'worst case' scenario or bounding scenarios (scenarios that present more difficult tests of the PPS, and thereby can serve as testing less demanding scenarios), selecting a scenario to test a specific feature of the PPS or testing a range of scenarios over time. Whichever scenario is selected needs to be such that the test objectives can be met.

9.28. The choice of scenarios to test will determine the extent to which the results provide useful information with regard to the effectiveness of the PPS. In some cases, a PPS might perform better in attack scenarios that appear before testing to be more challenging, and less well in scenarios that appear to be less challenging. Evaluating a range of scenarios can therefore provide a better indication of the effectiveness of the system. Other methods to conduct scenarios evaluations include tabletop exercises and computer simulations.

10. PHYSICAL PROTECTION SYSTEM ANALYSIS

10.1. This section describes the analysis process and methods used in evaluating the results of performance tests, modelling and simulations to determine the effectiveness of a PPS in meeting established performance requirements based on a threat assessment or design basis threat, including the following:

(a) Path analysis: A method of evaluating potential adversary paths and determining the probability that the response can interrupt the adversary before their goal is accomplished.
(b) Neutralization analysis: A method of determining the probability that the response can stop an adversary before their goal is accomplished or cause an adversary to abandon the attempt.
(c) Insider analysis: A method of determining the effectiveness of the PPS against an act by a person with authorized access at a nuclear facility.
(d) Scenario analysis: A method in which a specific attack plan (scenario) is developed and the PPS is evaluated to determine its effectiveness against it.

10.2. The objective of an analysis of the effectiveness of a PPS is to determine the likelihood that it will protect appropriately against unauthorized removal of nuclear material or sabotage of nuclear material and nuclear facilities. Performance testing is the most important method to acquire information with

regard to the effectiveness of a PPS, and the results of performance testing can be used to support the analysis methods described in this section. For example, performance testing can be used to determine the probability of detection by a perimeter intrusion detection system at a nuclear facility, which can then be used to conduct a path analysis [2]. The path analysis is a comprehensive analysis of all potential paths for an adversary from outside the facility to the target. Other methods, such as results from performance testing can also be used in determining the effectiveness of a PPS against defined threats.

10.3. The functions of detection and delay of the PPS are intended to facilitate a timely response to a nuclear security event. The response function is then intended to interrupt and neutralize or otherwise stop an adversary before their goal is accomplished, or cause the adversary to abandon the attempt. The effectiveness of a PPS can be expressed quantitatively as the probability of system effectiveness (P_E), in the form:

$$P_E = P_I \times P_N \quad (1)$$

where

P_E is the probability that the PPS meets its performance requirements;
P_I is the probability that the response interrupts the adversary, meaning that a sufficient number of appropriately trained and equipped members of the response forces arrive at the appropriate location in time to stop the adversary's progress towards completing unauthorized removal or sabotage;

and P_N is the conditional probability that the PPS (including the response) defeats the adversary, given that an interruption occurs.

10.4. Path analysis aims to evaluate P_I, which depends upon the relationship between detection capabilities, delay times and the time between first sensing of the adversary and a timely response. Neutralization analysis aims to evaluate P_N, which depends on the response force's numbers, weapons, training and equipment compared to those of the adversary. Neutralization analyses need to take account of legal and regulatory requirements as well as the quality of response plans. Path and neutralization analyses are used to determine potential or real weaknesses by considering relevant factors, to assess whether performance requirements for P_I and P_N are met, and to determine whether the PPS as a whole provides sufficient defence in depth and balanced protection.

PATH ANALYSIS

10.5. Path analysis produces estimates of P_I for each credible path an adversary could take to reach the defined target, assessing for each path how likely it is that an adversary will be detected while there is enough time for the response forces to interrupt the adversary before an act of unauthorized removal or sabotage can be completed. This can be used to identify the adversary paths with the lowest P_I, which are the most vulnerable paths and are sometimes called critical paths. The effectiveness of the PPS design in providing interruption is measured as the value of P_I for a most vulnerable path: if P_I is too low for the most vulnerable path then the PPS design is considered inadequate. P_I is determined for a single path using timelines such as those shown in Fig. 42.

10.6. Figure 42 shows the adversary's timeline at the top, indicating the time it takes the adversary to complete all of the tasks on the specified path, along with the PPS sensing opportunities along that timeline that might allow the adversary to be detected. Each PPS sensing opportunity has an associated probability of detection, P_D, which can in principle be estimated based on performance tests. The last sensing opportunity that would provide detection in time to allow timely interruption of the adversary is called the critical detection point. Below the adversary timeline, the figure shows the PPS response times, and the adversary task time remaining on the path after first sensing for each possible sensing

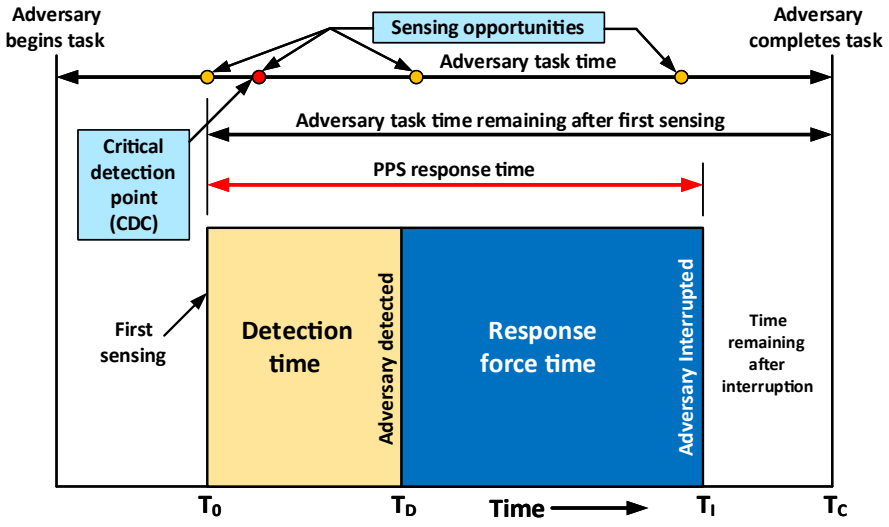


FIG. 42. Comparison of adversary and response timelines.

opportunity. The adversary task time and PPS response time are typically measured or estimated quantitatively based on performance tests.

10.7. A sensing opportunity associated with the path is considered 'timely' if the PPS response time for the response to interrupt an adversary after first sensing is less than the remaining time that the adversary would need to complete the intended act; otherwise, the sensing opportunity is not timely. In Fig. 42, the first two sensing opportunities are timely, and in this case P_I is the probability that the adversary is detected at one or more of those two timely sensing opportunities on the specified path. If there are K timely sensing opportunities, then P_I is calculated as:

$$P_I = 1 - \left\{ \prod_{i=1}^{K} (1 - P_{Di}) \right\} \quad (2)$$

where

P_{Di} is the probability of detection associated with the sensing opportunity;
K is the number of timely sensing opportunities;

and i is a single timely sensing opportunity.

10.8. Path analysis applies this calculation of P_I conceptually to every path to the target. The set of paths to be evaluated is defined in terms of concentric layers of protection around a particular target (see Fig. 43).

10.9. The protected area layer comprises two barriers (Gate, Fence), while the second protection layer has four barriers (Door 1, Door 2, Wall 1, Wall 2). There are therefore eight paths to the target: {Fence, Wall 1}, {Fence, Wall 2},{Fence, Door 1}, {Fence, Door 2}, {Gate, Wall 1}, {Gate, Wall 2},{Gate, Door 1}, {Gate, Door 2}. During path analysis of this hypothetical facility, P_I for each of these eight paths would be calculated and the path with the lowest P_I would be identified as the most vulnerable path. If that P_I value is sufficiently high, then this PPS might be deemed to provide effective interruption capability at this target.

10.10. As well as determining P_I for the most vulnerable path, path analysis can provide insight into whether there is adequate defence in depth, by considering protection measures that would be encountered before or at the critical detection point on each path. For example, the hypothetical facility in Fig. 43 would not have defence in depth if only one layer were timely, for example if the fence and gate on the perimeter boundary provided timely sensing opportunities but the four

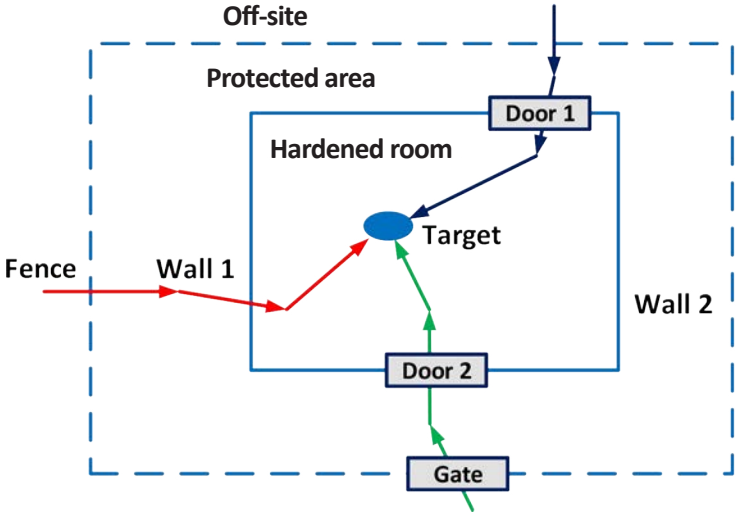


FIG. 43. Three adversary paths indicated on a hypothetical facility with two protection layers.

inner area barriers did not. Alternatively, if the hypothetical facility in Fig. 43 has the critical detection point at the Hardened Room boundary, then defence in depth is provided by the fence and gate at the perimeter boundary allowing for two opportunities for timely detection.

NEUTRALIZATION ANALYSIS

10.11. Neutralization analyses aim to evaluate P_N as a measure of the effectiveness of the response. This probability is determined based on information about the response, the threat, the PPS and the choice of methodology for determining neutralization. P_N is evaluated by considering a set of engagements, in which two opposing forces (response and adversary) use weapons and tactics in an attempt to achieve their respective goals. Many random factors might affect the result of an engagement, and so there are many possible outcomes. The outcome is defined as a 'PPS win' if the adversary force is killed, captured or abandons the attack. The probability of neutralization, P_N, can be defined by:

$$P_N = \frac{\text{Number of wins}}{\text{Number of engagements}} \quad (3)$$

10.12. For this expression to hold, the number of engagements in the denominator should be assumed to be an arbitrarily large number. As the number

of engagements increase, the proportion of wins will tend towards the actual probability of that event. In using Eq. (3), all engagements should be modelled using identical assumptions, such as the same initial conditions, and there should be only two possible outcomes of an engagement, either a win or a loss for the response forces.

10.13. Methods for determining P_N include the following:

(a) Expert judgement;
(b) Mathematical models;
(c) Simulations;
(d) Analysis of results from real events.

10.14. Each method has advantages and disadvantages, in terms of the time cost of performing them and their accuracy. Some methods include consideration of only a few factors, while others take account of many more, but there is no method that can account for all of the factors that affect the outcome of a single engagement. Nevertheless, such methods can provide insight into the strength of a response.

10.15. Simple methods, such as expert judgement, might need only data on the personnel and weapons (numbers and types) on each side, and the times at which they arrive at an engagement. More complex simulations might need a significant amount of data, including the following:

(a) Initial locations of response forces and adversaries;
(b) Response deployment routes and final locations;
(c) Adversary path;
(d) Adversary attack plan;
(e) Terrain;
(f) Building characteristics;
(g) PPS characteristics (e.g. barrier delays).

10.16. When used as part of the design process, neutralization analysis will be based on some combination of expert judgement, mathematical modelling and simulations. The analysis might include consideration of general response planning issues, such as contingency plan options, response forces' numbers and weapons, and training of response forces (taking account of regulatory requirements).

10.17. Neutralization analysis might also include a performance based component that could address in detail the performance of response forces against

adversaries in different scenarios and under different conditions. In this approach, a number of scenarios are created, each defined by information and assumptions about the adversary and target(s) to be attacked. These assumptions include the measures provided by the PPS (including the response), the adversary's capabilities, the adversary's intention and attack plan, including a sequence of postulated adversary actions and one or more adversary paths. The scenarios to be evaluated might be known at the beginning of the neutralization analysis or might be developed as the analysis proceeds.

10.18. Neutralization analysis focuses on response aspects of the PPS and therefore assumptions are typically made about the PPS element or protection layer in the adversary path that first leads to detection of an adversary. This might be chosen because the critical detection point or the first element or layer considered provides a significant probability of detection. Effectiveness exercises, either limited scope or force-on-force exercises, or simulations are then conducted starting from that element or layer.

10.19. Since it is often difficult to conduct a large number of tests, especially force-on-force exercises, methods can be used and documented to estimate P_N from the available sample set. One method of estimating P_N is the expression in Eq. (4), which is a less reliable approximation when the sample size is small. Other methods of determining estimates of probabilities from small sample sizes exist.

$$P_N = \frac{\text{Number of simulation wins by the response}}{\text{Number of simulations performed}} \quad (4)$$

PROBABILITY OF EFFECTIVENESS OF A PHYSICAL PROTECTION SYSTEM

10.20. When determining the probability of the effectiveness of a PPS, one method is to evaluate P_E as the product of P_I and P_N for a given path, determining the location of the critical detection point of the most vulnerable path, and then exercising or modelling scenarios to estimate P_N starting with the adversaries at the critical detection point. A disadvantage of this approach is that the critical detection point is typically at or near the target location, and it is often unrealistic that detection would not occur before this point.

10.21. Another method to evaluate P_E from P_I and P_N is to select a location on an adversary path before, at or after the critical detection point, and then

exercise or simulate scenarios to estimate P_N with the adversaries starting at that location. In this case, P_I is the cumulative probability of detection for all the sensing opportunities on that path up to the selected location. In this approach, the scenario can be analysed using the most probable point of detection. In this case, the calculated value of P_E will not equal the value from the previous method if the chosen element or layer is not the critical detection point, since in such a situation, P_I would not be equal to the cumulative P_D at the chosen element or layer.

INSIDER ANALYSIS

10.22. Guidance on measures against insider threats is provided in Refs [8, 9]. Paragraphs 10.22–10.26 describe a method to analyse a PPS against insider threats acting alone or in collusion with external adversaries. Methods widely used to analyse insider threats include expert reviews, path analyses and tabletop analyses. Insiders are a particular challenge to a PPS because they have detailed information and are capable of using defeat methods not available to external adversaries. Insiders have special:

(a) Access: Authorized access to nuclear facilities, such as access to an inner or limited access area.
(b) Authority: Defined authority to influence or control others. For example, a guard force supervisor might have the authority to direct a guard to disregard a requirement to search a vehicle entering a protected area.
(c) Knowledge: The specific knowledge a person would have based on their function or experience. This might include information on, for example, facility characterization and operations, PPS measures, capabilities and operation, and targets.

10.23. The approach used to analyse insider threats involves developing credible insider scenarios based on identified targets and defined insider groups. Scenarios should take into account the threats defined in the threat assessment or design basis threat and should include descriptions of the specific tasks that an insider would need to carry out. Insider threats might be:

(a) Passive: Willing to provide information to external adversaries, but not participate in an attack.
(b) Active: Willing to act alone, collude with other insider threats or with external adversaries to commit unauthorized removal and sabotage. An active insider threat might or might not be willing to use violence.

10.24. An analysis of passive insider threats includes determining the information that an insider might provide and developing scenarios involving adversaries that have such information. The effectiveness of the PPS is determined by performance testing those scenarios.

10.25. An analysis of the threat from an active insider alone involves using subject matter experts to develop scenarios in which the insider exploits their advantages of having access, authority and knowledge. Scenarios should also be developed involving multiple insiders if required by the threat assessment or design basis threat. Consideration should be given when developing insider scenarios to the possibility of an insider threat exploiting weaknesses in administrative or technical measures for surveillance, containment and control. The effectiveness of the PPS against these threats might be estimated by using experts, insider adversary path analysis (incorporating data from performance tests of access control, containment and surveillance systems) or tabletop exercises.

10.26. Insider collusion with external adversaries can include direct and indirect actions by the insider to support the successful completion of unauthorized removal or sabotage. An analysis of such possibilities involves developing scenarios representing the external adversary and including the use of access, authority and knowledge by a selected insider threat in an active role supporting the attack. These attack scenarios are then evaluated as described previously using performance tests, path analyses and neutralization analyses.

SCENARIO ANALYSIS

10.27. Scenario analysis involves creating a detailed representative set of adversary scenarios, determining what the response would be in each scenario, based on facility security plans, procedures and tactical deployment of response forces; and performing a simulation of the interaction between adversaries and the PPS, as realistically as possible.

10.28. Scenario analysis is a PPS effectiveness evaluation technique that is based on postulating adversary attack scenarios and determining P_E directly without calculating P_I in one analysis and P_N in another. Adversary paths should be selected that take advantage of possible PPS vulnerabilities, as a real adversary might be expected to do. The analysis therefore involves identifying PPS measures that might be susceptible to defeat due to characteristics of their installation or operating procedures. Consideration should be given to possible defeat methods for sensors, barriers and communication systems as well as possible

diversion or elimination of part of the response force. Tools that can be used in a scenario analysis include tabletop exercises, computer combat simulations and force-on-force exercises.

10.29. The results of the scenario analysis can be used to derive a P_N value in Eq. (1) or can be used to directly estimate P_E if detection of the attack is at a location with a reasonably high detection probability.

11. MANAGEMENT SYSTEMS FOR NUCLEAR SECURITY

11.1. The role of management at a nuclear facility is to perform functions such as planning, organizing, staffing, leading and directing work, controlling, monitoring and assessing work and evaluating results. Management systems are methods, processes and tools used by the managers of a nuclear facility to create a framework to carry out work in a safe and secure manner while ensuring that the objectives of the facility operator are achieved within the legal and regulatory framework of the State.

11.2. Since the management systems used in all areas of nuclear facility operations are based on common concepts and principles, integrating them into one comprehensive framework results in increased efficiency and effectiveness and allows the operator:

(a) To establish and apply consistent policies, processes and procedures to meet competent authority and operator requirements;
(b) To improve overall efficiency by eliminating duplication;
(c) To make it easier to continuously improve management systems;
(d) To foster change and to encourage innovation by creating a framework for continuous improvement and performance on the basis of experience from each discipline;
(e) To manage changes effectively, such that security is maintained or improved;
(f) To make decisions that best address the overall needs of the facility in a coherent and disciplined manner;
(g) To bring together expertise from different disciplines, to address conflicting requirements and to identify optimal solutions to address all requirements;

(h) To prevent risk reduction in one discipline, such as safety, from increasing or creating new risks in another discipline, such as physical protection;
(i) To ensure that physical protection does not unduly affect facility operations.

11.3. An integrated management system incorporates the management of all aspects of a nuclear facility into one coherent system, applying the core management principles and processes to each specific discipline (e.g. physical protection, nuclear material accounting and control, safety, operations). Activities that have an effect on operational performance or regulatory compliance should be part of the management system. An integrated management system provides a single framework for the arrangements and processes to address all the objectives of the facility operator, including safety, health, environmental, nuclear security, quality, economic and information management aspects. The coordination of elements such as organizational structure, strategic decision making, resource allocation and the processes of auditing and reviewing performance are parts of an integrated management system. All processes, and the documents that describe these processes, should be integrated into a single framework. Care should be taken to ensure that sensitive information relating to the PPS, as well as any other sensitive information, is appropriately protected and shared only on a need to know basis.

11.4. Operators of nuclear facilities should use an integrated management system for all phases in the lifetime of the facility, and for a new nuclear facility the management system should be integrated with all activities from an early stage [17]. If an integrated management system does not already exist at a nuclear facility, it can be developed by integrating the existing management systems, including quality management, into one system. The guidance in this section assumes that an integrated management system exists at a nuclear facility.

11.5. Duties and responsibilities for physical protection, and for quality assurance of physical protection, should be established within the framework of the management system [2]. Operators should adopt through their management system an integrated and coordinated approach to reviewing all proposed changes to physical protection arrangements before implementation to ensure that they do not result in any unintended effects on safety. Application of an integrated management system to nuclear facilities is addressed further in Refs [25–27]. Reference [2] states that operators should comply with the State's legal and regulatory framework, have primary responsibility for the implementation of a PPS, encourage a strong nuclear security culture and cooperate with other State

entities having physical protection responsibilities, such as off-site response forces. IAEA Nuclear Security Series No. 7, Nuclear Security Culture [28], states:

> "Staff performance is influenced by the quality of management and the provision of expectations, requirements and standards for the conduct of work, training, documented procedures [and] information systems".

APPLICATION OF MANAGEMENT SYSTEMS TO THE PHYSICAL PROTECTION SYSTEM

11.6. An integrated management system is used by facility managers to monitor and control all activities throughout a nuclear facility, including the PPS. For the purposes of this publication, the term 'operation of a PPS' includes all of the activities associated with the PPS, including maintenance and testing. Application of the management system helps to ensure that the PPS continues to meet its original design specifications and is modified as needed to address changes in requirements.

11.7. An integrated management system can be applied to the PPS at a nuclear facility through a series of elements: requirements management; work direction and control; resource management; and assurance activities (see Fig. 44).

11.8. Some functions at a nuclear facility might be performed by other organizations, in which case the facility management system might not address all of the PPS functions. For example, the response for a nuclear facility can be provided by the national police or military organizations, in which case the operator of the facility is responsible for operation of the detection and delay components of the PPS, and might implement the overarching quality assurance processes that are part of the facility management system. The national police or military organizations will use their own quality assurance practices for their own activities. In the absence of an integrated management system at a facility, efforts should be made by the operator to integrate physical protection with other disciplines, such as facility operations, nuclear material accounting and control and safety, especially in relation to common activities, such as quality assurance. The operator should develop strong interactions with all State and operator organizations involved in all phases of the design, development and installation of physical protection measures and operation of the PPS.

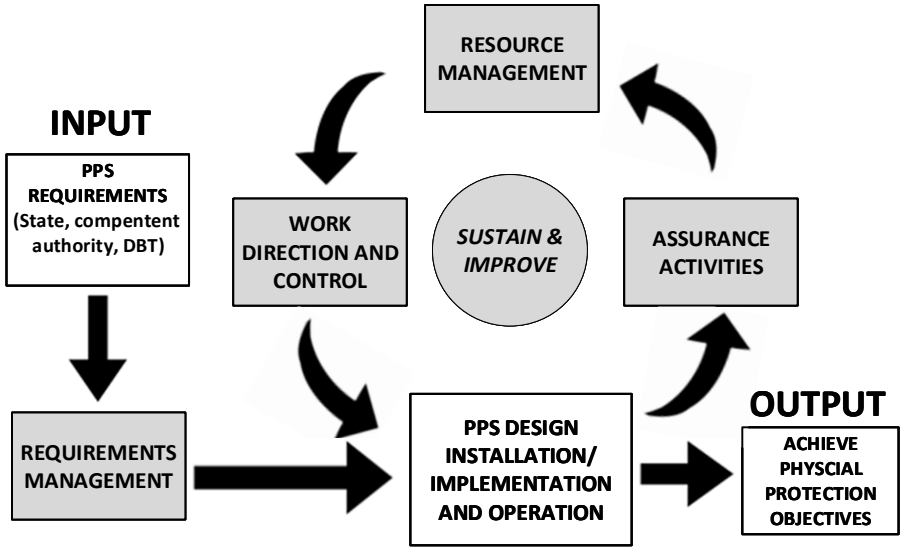


FIG. 44. The management system applied to the physical protection system.

REQUIREMENTS MANAGEMENT

11.9. A PPS should be designed to meet a set of objectives, established by the State and its competent authority. These objectives might be expressed in the form of prescriptive requirements, performance requirements or a combination, which are used in the PPS design to develop specifications. Once the PPS design has been developed, approved and installed, the design specifications form the basis for verification activities to ensure that the PPS continues to meet the requirements for its operation. A range of methods and tools used to manage requirements typically includes four steps:

(1) Assembling stakeholder requirements;
(2) Analysing the requirements;
(3) Verifying the requirements;
(4) Documenting traceability of the requirements.

11.10. These steps can be performed sequentially as the design process proceeds or, in some cases, can be performed in parallel. Industry standards provide more information on how stakeholder requirements can be collected and how a requirements analysis is performed (see Ref. [29]).

Assembling stakeholder requirements

11.11. The first step in the process is to identify applicable requirements of all relevant stakeholders. These might include requirements of the State and the competent authority, and operational or safety requirements. During the design phase, these stakeholder requirements will be used to develop additional derived requirements, which are used to define design specifications.

Analysing the requirements

11.12. When all applicable stakeholder requirements have been assembled, the second step is analysis to ensure that the requirements are clear, to identify any conflicting requirements and to transform the requirements into derived requirements for the PPS and design specifications for operating and maintaining the PPS, using a risk management approach. The applicable stakeholders should be able to understand how the derived requirements reflect their requirements.

11.13. The following examples indicate how derived requirements can be developed (*original emphasis*):

(a) Recommendation (para. 4.39 of Ref. [1]): "*Inner areas* should provide delay against unauthorized access to allow for a timely and appropriate response to an *unauthorized removal*." Additional information would need to be obtained from the relevant stakeholder (e.g. the competent authority) or assumed in order to develop design specifications: for example, the recommendation does not specify the amount of delay for the inner area barrier, the response time for response forces or the adversary capabilities that might be used to defeat the barrier. If the adversary capabilities as defined in the threat assessment or design basis threat allow the use of explosives to defeat a barrier, for example, the barrier would need to be more robust than if the capabilities are assumed to be limited to the use of manual tools. The analysis might therefore result in a derived design criteria that the inner area wall provide a minimum of a 30 minute delay against forced entry.

(b) Recommendation (para. 4.42 of Ref. [1]): "Only authorized persons should have access to the *inner area*." This is a recommendation that the operator develop plans, processes and procedures before the PPS becomes operational and that they define:
    (i) Job positions or personnel categories requiring access to the inner area to perform assigned job functions;
    (ii) How the process to approve access for authorized persons to the inner area is controlled;

(iii) The process to allow an authorized person access to the inner area;
(iv) The security related training required before personnel are granted access.

11.14. The requirements management analysis should identify any potential conflicts between physical protection recommendations and safety requirements. For example, para. 4.40 of Ref. [1] states that the "number of access points to the *inner areas* should be kept to the minimum necessary (ideally only one)." However, there might be a safety requirement that an emergency exit be provided within 25 m of any location within a hazardous area. There might also be operational requirements to have access points at locations in the inner area to streamline movements of nuclear material between other inner areas and reduce processing time. Having only one access point would, in some circumstances, create a conflict with the operational and safety requirements. Such conflicts should be resolved during the analysis step in a manner that balances the competing criteria.

11.15. The requirements analysis process is carried out in parallel with the PPS design process, to ensure that requirements are transformed into formal derived requirements and design specifications for operating and maintaining the PPS.

Verifying the requirements

11.16. During the installation and implementation of physical protection measures, the stakeholder and derived requirements will be used as the basis for verification activities. Verification of the requirements is intended to ensure that the design specifications and all requirements for operating and maintaining the PPS are met (and therefore that the stakeholder requirements will be met).

11.17. Verification might include performance tests, assessments, inspections, audits or other means to provide assurance that the formally documented requirements are met. Verification activities can also be performed at the component, subsystem or PPS level.

Documenting traceability of the requirements

11.18. Requirements management includes documenting how each formal stakeholder requirement can be traced through derived requirements for the PPS to specifications for the design, installation and implementation of physical protection measures and their operation.

11.19. Documenting this traceability provides evidence that the requirement has been met, and also an efficient mechanism to identify those plans, processes, procedures and training that need to be changed if that requirement changes. A common method for simple systems is to create a traceability matrix that lists each requirement and all the associated plans, processes and procedures, and records the measures used to meet that requirement. For more complex systems, traceability matrices become impractical and more formal tools are used.

11.20. For example, there might be a regulatory requirement that personnel receive a certain type of security training every six months to be allowed access to an inner area. This requirement is included in the facility security plan. Use of a traceability matrix for this requirement might be as follows:

(a) A training plan is developed, along with lesson plans, for security staff to provide the training at the specified frequency.
(b) A process is established that requires managers to ensure that training is scheduled for personnel needing access to the inner area, and that they receive the training before being granted access to the area and at the required frequency thereafter, and to record each individual's completion of training and send a copy of the log to designated security staff each time the individual completes the training.
(c) Security staff create and manage a list of personnel with authorized access to the inner area, containing each name, their department, the date(s) on which training was received and the date when refresher training is next required. The list is updated on a monthly basis, at which time security staff identify all the personnel on the list who will require refresher training in the coming month and notify the appropriate departments. Security staff provide to the access control point a list of personnel who have taken the training between monthly updates.
(d) Procedures are developed for the guards working at access control points to the inner area to verify that individuals are on the current list, and that their training is up to date, before granting them access.

11.21. In this example, the single stakeholder requirement is reflected in the security plan, a training plan, training lesson plans, logs and procedures. A traceability matrix would list all of these, so that when a change occurs, such as to the required frequency of the training, all the plans, processes, procedures and records can be updated to reflect the new requirement.

WORK DIRECTION AND CONTROL

11.22. Work direction for the management of the PPS includes determining the functions that need to be performed, establishing security policies, establishing an organizational structure to perform those functions, defining roles, responsibilities and accountabilities, developing strategic and tactical goals, and establishing performance criteria for the PPS.

11.23. Determining the functions that need to be performed to design, install and maintain a PPS involves an understanding of the technical, administrative and support functions to perform the work. Some of the functions might be provided by the facility security personnel, and some might be performed by other departments. For example:

(a) The design phase of a PPS might involve security professionals, a designer, personnel responsible for the infrastructure of the facility, operations personnel, guard and response forces, safety professionals, IT support staff and budget personnel.
(b) Installation of PPS facilities, barriers or other systems involves construction and infrastructure personnel.
(c) Operation of a PPS involves personnel to operate and maintain the PPS measures, supervisory personnel and other security personnel who provide functions such as training, assessment, performance testing, quality assurance, trustworthiness checking, records management, information security, computer security, administration, budgeting, procurement and contract management.

11.24. A policy is needed which states the commitment of the facility's senior management to physical protection. This security policy should ideally be issued directly by the senior management to make its importance clear and to demonstrate their commitment to physical protection. All personnel need to understand that adherence to this policy is expected of everybody at the facility. This policy emphasizes senior management's leadership with regard to physical protection matters in all areas including the PPS.

11.25. Establishing an organizational structure to effectively manage a PPS involves defining the framework within which the physical protection department operates. The most appropriate organizational structure for physical protection at a specific nuclear facility will depend on many factors, including the broader organizational structure, the type of nuclear facility, State laws and requirements, cultural norms and other factors. However, the objective is to develop an

organizational structure that provides for effective management of the work to design, install and operate a PPS. Some common considerations when defining the organizational structure of a physical protection department include the following:

(a) Establishing a clear chain of command, an unbroken line of authority from the physical protection manager to the individual personnel performing functions relating to the PPS.
(b) Identifying appropriate 'spans of control' (the number of subordinates under a manager or supervisor). Depending on the nature of work performed, and the complexity of the work, the span of control can be adjusted so that both the personnel and the work can be effectively managed.
(c) Identifying how decisions are made within the organization, and who within the chain of command is responsible for making them. If decisions are made by a single person at the top of the chain of command, this is referred to as a centralized decision making model. The appropriate level for decision making is determined by factors such as the potential impacts of the decision for other organizations, and the risks and costs associated with each option.
(d) Dividing work activities or tasks between individual jobs (division of labour). Some jobs involved in operation of a PPS need specialized training, such as a locksmith or an armourer, and some need general skills, such as a security planner responsible for developing security plans and procedures relevant to the PPS.
(e) Formalizing job functions within an organizational structure for security. A guiding factor is the degree to which specific job tasks and activities only involve following established processes and procedures and which may demand discretionary action.
(f) Grouping specific jobs together to help to coordinate common activities and tasks. Some security organizations have a technical security group comprising personnel who can perform all of the functions to maintain a PPS, such as engineers, designers, technicians, network specialists, performance testers and labourers. In other cases, a technical security group may have some of the functions but use personnel from other departments, such as network specialists from the IT department, as needed for a specific activity.

11.26. Defining roles and responsibilities of departments and personnel plays a significant role in establishing an effective physical protection management structure. All facility personnel need a clear understanding of their own roles and responsibilities and those of personnel with whom they need to interact in order to achieve the desired results. This includes all managers understanding their delegated responsibility for the physical protection of targets within their areas, including information and computer systems and support tasks such as

staff and training and implementing a trustworthiness policy. Managers also need to be made responsible for ensuring that personnel under their authority understand their responsibility for physical protection, apply physical protection requirements and procedures as a contractual condition, and are appropriately supervised in this respect.

11.27. Establishing performance criteria for the PPS involves development of performance requirements or expectations that should be met by the PPS as a whole, or by individual components. Performance criteria should be specific, measurable, achievable, realistic and time specific (SMART). Performance criteria can be developed to address many factors, including quality, quantity or timeliness, which define how well work is performed, how accurately it is performed or how effective the result is. An example of a quantity performance indicator for a PPS is the ability to process 100 people per hour through an access control point into a nuclear facility. An example of a timeliness performance indicator is that guards respond to any alarm on the perimeter within five minutes.

11.28. It is suggested that managers establish measurable physical protection goals. All managers then actively seek information on physical protection performance within their area of responsibility with appropriate monitoring and, consistent with information security policies, share this information within the organization, thereby demonstrating commitment to continuous improvement. Performance goals and benchmarking should not encourage adverse behaviour and complacency. Any reward system should be structured so that it does not drive undesirable behaviour. For example, if the objective of a facility is to have no security incidents, personnel might be reluctant to report such incidents.

11.29. Work control involves providing oversight and planning by developing a framework for the conduct of work and ensuring that changes in the design or operation of the PPS occur in a deliberate, controlled and integrated manner.

11.30. Managers should ensure that physical protection activities are accomplished appropriately by planning, assigning and overseeing work activities associated with the PPS. Managers can provide leadership by setting a personal example of commitment to consistently giving physical protection related activities appropriate attention and priority. All work needs to be suitably planned in order to ensure that its purpose is achieved and physical protection is not compromised. Planning is needed for both routine work and non-routine activities or abnormal events, such as exercises, maintenance work, equipment modification and replacement, outages, loss of power, failure of physical protection measures, and nuclear security events, in order to ensure that the integrity of the PPS is

maintained at all times. Compensatory measures will need to be planned for some non-routine activities or abnormal events.

11.31. Ensuring that changes in the design or operation of the PPS occur in a deliberate, controlled and integrated manner involves implementing configuration management and change control programmes for management of the PPS. Configuration management should be part of the sustainability programme of the operator, and documents the physical, procedural and training elements of an operating organization's PPS, including relevant computer systems and software. It provides a repository for the design documents, standard operating procedures and governing guidelines for the PPS. It also includes processes for coordinating changes to the facility's systems or operations that might affect the effectiveness of the PPS. Furthermore, Ref. [2] indicates that configuration management might be one of the management controls used to address safety–security interface issues during design, construction and normal operations, as well as during nuclear security events and emergencies, and during decommissioning.

11.32. Configuration management ensures that changes to a PPS are properly developed, assessed, approved, implemented, verified and documented. Having immediate access to this information can help the operator to recover rapidly from hardware or software failures and ensure that equipment is operating as intended when returned to service. In addition, access to accurate records on training, procedures, maintenance and logistics allows the operator to verify that these important aspects of a PPS are being implemented. The operator:

(a) Should ensure that the implications of changes in the PPS subject to configuration management are reviewed before implementation and are documented appropriately;
(b) Should ensure that configuration management information is accurate, available in a timely manner and appropriately protected;
(c) Should apply configuration management to document the physical layout, procedural operation and personnel training records of its PPS.

11.33. IAEA guidance highlights the importance of management programmes for configuration management of the PPS [2]. Other guidance suggests ways to apply configuration management for the aggregation of all relevant security documents (e.g. design documents, standard operating procedures and governing guidelines) and making informed decisions (e.g. for coordinating changes) [26].

11.34. Change management can ensure that any proposed significant change within the nuclear facility — made by any department for any reason, whether

of a structural, procedural or organizational nature, and whether temporary or permanent — is analysed with regard to its implications for physical protection. No reduction in the effectiveness of physical protection is acceptable, even for short periods of time, without appropriate justification and approval. The change management system can also be used to ensure that any proposed significant changes to the PPS do not compromise other systems, such as those for nuclear material accounting and control and safety.

11.35. Preferably, one manager should approve each change and the change should also be endorsed by those individuals whose area of responsibility is affected. This review and approval process should be given particular attention when the change affects the areas of responsibility of different parts of the organization. Evidence that the change satisfies physical protection requirements needs to be provided to the security organization.

11.36. Adequate monitoring needs to be carried out as the change is implemented to provide early warning of any negative effects on PPS effectiveness, so that there is sufficient time to take any necessary remedial action. Examples of planned activities which could have an adverse effect on physical protection include:

(a) Activities that could cause a loss of primary power to physical protection equipment;
(b) Placing of vehicles or heavy equipment or the installation or development of physical protection measures or barriers that could obstruct sensing or assessment capabilities, reduce delay or increase response times;
(c) Construction activities that remove or degrade physical barriers, allowing access controls to be bypassed.

11.37. In the event of the nuclear facility sharing a common boundary with another existing or planned nuclear facility, arrangements should be made, as appropriate, to ensure that its planned activities do not decrease the effectiveness of the security plan or PPS at the adjacent facility.

RESOURCE MANAGEMENT

11.38. Resource management includes topics such as: training and qualification programmes; selection of personnel for the functions to support design, installation and implementation of physical protection measures and operation of the PPS; procurement of goods and services; and establishing a productive work environment.

11.39. Personnel selection is the methodical process used to select personnel to perform job functions relating to the PPS, to identify people who have the knowledge, skills, capabilities and other characteristics to make the most valuable contributions to the organization. Human resource processes at a nuclear facility are part of the integrated management system, and physical protection managers should aim to recruit and retain the best personnel available within the constraints of the system. Personnel selection also includes ensuring that personnel have all the qualifications necessary to perform a job function, and their trustworthiness is checked before being employed in a position for which such a determination is required.

11.40. Effective physical protection depends upon staff having the knowledge and skills to perform their functions to the desired standards. Managers need to ensure that their staff not only receive specific security training appropriate to their responsibilities, but are also generally educated about and aware of the threats and other topics related to a strong nuclear security culture [28].

11.41. Procurement of goods and services is essential to sustain an effective PPS. Considerations of particular importance in this context include procuring PPS equipment from established vendors and ensuring that replacement parts are available for the expected lifetime of the equipment, testing and evaluating new components before procurement to ensure that they can be integrated into and are compatible with existing PPS components, and evaluating potential security risks relating to the supply chain. The operator retains responsibility for physical protection when using contractors or procuring any goods and services. Operators need to retain the competence to specify the scope and quality required of a product or service and subsequently to assess whether they meet the physical protection equipment requirements and specifications. The management system can include arrangements for the following:

(a) Qualification of vendors, contractors and suppliers of goods and services;
(b) Selection of vendors, contractors and suppliers on the basis of the effectiveness of their management systems and their performance;
(c) Verification that vendors, contractors and suppliers understand and comply with physical protection requirements (including those for the security of sensitive information) relating to the goods and services that they provide;
(d) Prior approval by the operator of any subcontracting by the vendor, contractor or supplier;
(e) Specification of contractual requirements, including physical protection requirements;

(f) Provision, where appropriate, of physical protection advice, information and training to vendors, contractors and suppliers and their staff;
(g) Periodic assessment of the management systems, including physical protection arrangements, of vendors, contractors and suppliers and their performance, using a graded approach;
(h) Verification that goods and services supplied meet the facility's physical protection specifications and are authentic.

11.42. The physical and physiological environment work environment has a large impact on how personnel perform their tasks and comply with physical protection requirements. It is important that physical protection procedures are not regarded as an excessive or unnecessary burden. Managers can involve personnel in reviewing physical protection guides and procedures to make sure that they understand the documents and why they are in place, and are able to offer suggestions to make them more effective.

ASSURANCE ACTIVITIES

11.43. Assurance activities include implementation of quality assurance and assurance programmes. A quality assurance programme ensures the PPS performs as designed and meets regulatory and performance requirements. An assurance programme establishes evaluation and test activities with sufficient rigour to ensure that PPS measures are at all times operational, functioning as intended, and interacting in such a way as to detect and respond to any adversary action before the completion of a malicious act.

11.44. Quality assurance is part of quality management (which in turn should be part of the integrated management system) focused on providing confidence that quality requirements will be fulfilled. A quality management system is as a collection of business processes focused on achieving quality policy and quality objectives to meet regulatory requirements.

11.45. The assurance programme addresses the outcome of inspections by the competent authority, and internal self-assessment results in a comprehensive approach to assure sustained effectiveness of the PPS. Assessment activities should be graded and tailored to the assets at the location and the measures that make up the overall PPS at a nuclear facility. Consideration should be given to development of schedules for assurance activities, planning how results of assurance activities are used, and defining what measures, including compensatory measures, should be taken if the assurance activities indicate an unacceptable

degradation of the effectiveness of the PPS. A self-assessment (or internal review) programme should normally include use of a wide range of assessments, root cause analyses, performance indicators, lessons identified and corrective action tracking programmes.

11.46. Assurance activities include regular evaluations to ensure the ability of the operator to sustain the facility's PPS by identifying both strengths and areas for improvement. The rigour of these evaluations should be based on a graded approach, depending on the type of nuclear material or nuclear facility, the nature of the operations and the measures that make up the PPS. Additional information on assurance activities can be found in Section 9.

SUSTAINABILITY AND CONTINUOUS IMPROVEMENT

11.47. Sustainability includes maintaining the performance of people, procedures and equipment. This involves monitoring performance, and providing motivation and leadership to create an organization that is consistently effective and continuously improving. Sustainability includes maintenance and testing programmes to keep PPS systems working as designed, and working to develop a strong nuclear security culture as described in IAEA Nuclear Security Series No. 30-G, Sustaining a Nuclear Security Regime [30].

11.48. Effectively sustaining a PPS involves sustaining not only the technology but also the people using the technology. Managers need to communicate to personnel what is expected of them, what the organizational goals are, what behaviour will be rewarded and what actions will be punished. All employees and decision makers need to communicate throughout the organization what they are expected to achieve and what behaviours are acceptable in doing so. Managers need to provide leadership consistent with the organization's policies, values and strategies.

11.49. Sustainable high performance depends upon the right personnel being in the right positions with the right leadership qualities. It can be achieved through programmes:

(a) To recruit the best qualified personnel available;
(b) To develop staff skills and abilities through training and qualifications programmes;
(c) To recognize and reward good behaviour;

(d) To retrain, transfer or dismiss personnel performing unsatisfactorily;
(e) To provide a safe work environment.

11.50. Continuous improvement is a process of identifying improvements in policy, processes, plans, procedures, equipment or in the management system as a result of issues identified during assessment activities such as inspections, self-assessments or performance tests, feedback from personnel or lessons identified, or from changes in operations, safety or other programmes at the nuclear facility. In practice, at some point, the performance of a PPS approaches a peak, and improvement after that point is marginal, unless a discrete change (e.g. a new technology) provides a significant improvement in efficiency or effectiveness of the PPS. However, the performance of a PPS is always at risk of declining, due to factors such as ageing or obsolescence of equipment, reduced financial support, loss of motivation by personnel and complacency by managers.

Appendix

EXAMPLE NEEDS ASSESSMENT AND REQUIREMENTS ANALYSIS FOR UNMANNED AERIAL SYSTEMS

A.1. This appendix provides a detailed overview of a hypothetical needs assessment and a requirements analysis. In this example, facility managers have identified the need to have better situational awareness and flexible assessment capabilities to cover the limited access area without exposing guard patrols to possible harm from adversaries. If possible, it would be useful to also warn adversaries away, again without exposing guard patrols.

A.2. One way to provide this capability is to use an unmanned aerial system (UAS). Alternatives might be to have cameras within the limited access area, either mounted on guard patrol vehicles or installed throughout the limited access area. Options and information considered with regard to UASs might include:

(a) UASs can be operated in several ways:
    (i) Persistent presence of an untethered UAS over protected areas to continuously (subject to weather conditions) monitor and direct intelligence, surveillance and reconnaissance personnel and equipment (e.g. cameras, sensors) in areas of concern. This operational approach involves either long flight times (endurance) or rapid exchange of equipment in and out of service to allow recharging of batteries or refuelling.
    (ii) Normal operation on a power and communications tether. Such a system could be designed so that it can be tethered in different places at different times. For example, the tether could be attached to a vehicle or boat to enable mobile operations. This operational approach could be performed over a period of time (subject to availability) but would provide more limited options compared to continuous, untethered operations.
    (iii) Deployed periodically (e.g. once per hour) or on demand for assessment or determining intent of an identified adversary.
(b) Very little reliable information, other than the vendor's claims, is available to assess how well these systems actually perform over extended periods of time.
(c) UAS operation is often controlled by State aviation regulations, and therefore legal and policy limitations on operations will need to be addressed.

A.3. As an example, assume that an operator would like to deploy a UAS on demand whenever there are indications that adversaries are within the limited access area. The first step in exploring use of a UAS is to determine stakeholder requirements for this subsystem; that is, the system capabilities and functions that stakeholders need, as well as standards for quality, testing and evaluation, and performance testing. Stakeholder requirements might include the following:

(a) Operational effectiveness requirements: For example, the UAS needs to be able to positively assess and challenge an adversary within 30 s after detection at the boundary of the limited access area. The UAS needs to be available for deployment at least 75% of the time and to cover 70% of those routes that an adversary is most likely to take through the limited access area.
(b) Regulatory requirements: Aviation regulations in the State limit how government entities may deploy a UAS, and specify weight limits and operational limits for the UAS and training requirements for UAS controllers. UAS controllers are also limited to 8 hours or less of flying time within a 24 hour period. The competent authority might have requirements for the operator if they are a member of the response.
(c) Operator requirements:
    (i) Operator safety policies require that any physical protection subsystem operate within the constraints of a safety plan, protecting both facility personnel and the public;
    (ii) Required documentation, including acceptance testing plans, maintenance plans and training plans for UAS controllers and maintenance personnel.
(d) Cost requirements: No cost limitations are specified in advance but initial and operating costs for deploying a UAS need to be estimated so that managers can decide whether to study the use of the UAS in more detail and to begin conceptual design for such a system.
(e) System maturity requirements: A system for using a UAS should have well characterized risks for operation as well as benefits for use.

A.4. The next step is to determine the concept of operations (i.e. the way the system works from the operator's perspective) including the user needs, goals and characteristics of the system. A possible concept of operations for the UAS might involve the following:

(1) Possible adversaries would be observed within the limited access area using thermal imagers or by patrols using binoculars.

(2) Vehicle patrols and boat patrols of the limited access area would be notified that possibly unauthorized vehicles or personnel are present in the limited access area or in waterside areas where public access is prohibited.
(3) The CAS operator would then instruct one or more selected patrol vehicles and boats to launch a UAS. The personnel in the vehicle or boat would determine whether their UAS is operational and is in a location where it could be launched, and whether weather conditions were suitable for launch. If not, the CAS would be informed and other patrols might be asked whether they are in a position to launch a UAS.
(4) The UAS might also be controlled from the CAS to fly close enough to the vehicle or adversary to determine whether they are armed, are driving armoured vehicles or are carrying suspicious items. If so, the CAS would notify guards and response forces by radio about the intrusion.
(5) If no determination could be made, the UAS would be flown close enough to the adversaries to instruct them by loudspeaker to leave the limited access area or restricted access waterside areas.

A.5. Both stakeholder requirements and concept of operations might lead to derived requirements such as the following hypothetical requirements:

(a) Steps 1–4 of the concept of operations presented in para. A.4 need to be performed within 30 s after detection of a potential adversary at the boundary of the limited access area. Speeds and descriptions that might be assumed for adversaries' vehicles or boats will be specified based on the threat assessment or design basis threat. Performance data might need to be collected to create a timeline for the steps in the concept of operations. The timeline can then be used to verify that stakeholder requirements would be met against possible adversaries.
(b) The UAS should be available to be deployed 75% of the time, based on weather conditions and system reliability constraints. Vendor specifications of the UAS weight, size and speed will be considered alongside historical data on weather conditions such as rain, snow, hail, high winds or high gusts to determine what percentage of the time the UAS can actually be launched.
(c) As the UAS needs to be deployable 75% of the time, some capability needs to be available at night to detect and track adversaries. With present technology, this capability is likely to be provided by thermal imaging, radar or light detection and ranging (LIDAR).
(d) No-fly or prohibited zones where the UAS cannot operate will need to be specified for the limited access area and on the waterside. Such zones will help to define where in the facility area flight is allowed and at what altitudes the UAS is allowed to operate.

(e) Policies and procedures will need to be defined to prevent the UAS from being launched or operated within prohibited zones and to safely land the UAS if it is malfunctioning or control is lost.
(f) Relevant personnel will need to be trained to perform all steps of the concept of operations. This includes the CAS operator, patrol vehicle or boat personnel and maintenance personnel.
(g) Cost requirements will be based on the need to have enough UAS devices available to be deployed 75% of the time to cover 70% of those routes that an adversary is most likely to take through the limited access area.
(h) Assumptions will need to be made about how much sound or light needs to be available to warn adversaries away from the boundary of the limited access area, including under different weather conditions.
(i) To meet system maturity requirements, only UAS models that have been operated at a nuclear facility for at least a year will be evaluated for possible use.

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, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).

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

[8] 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).

[9] 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).

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

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020).

[13] 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 (in preparation).

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Systems and Software Engineering: System Life Cycle Processes, ISO/IEC/IEEE 15288:2015, ISO, Geneva (2015).

[15] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING, Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities, 4th edn, Wiley, Hoboken, NJ (2015).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Security during the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (in preparation).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
[22] AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Management of Alarm Systems for the Process Industries, ANSI/ISA-18.2-2016, ISA, Research Triangle, NC (2016).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a Nuclear Security Contingency Plan for Nuclear Facilities, IAEA Nuclear Security Series No. 39-T, IAEA, Vienna (2019).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Safety of X Ray Generators and Other Radiation Sources Used for Inspection Purposes and for Non-medical Human Imaging, IAEA Safety Standards Series No. SSG-55, IAEA, Vienna (2020).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Management for Research Reactors and Related Facilities, IAEA, Vienna (2016).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[29] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Systems and Software Engineering: Life Cycle Processes — Requirements Engineering, ISO/IEC/IEEE 29148:2018, ISO, Geneva (2018).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).

ABBREVIATIONS

CAS	central alarm station
PIN	personal identification number
PPS	physical protection system
UAS	unmanned aerial system

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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

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

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

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

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

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (57 pp.; 2011)
ISBN 978–92–0–111110–4 Price: €28.00

PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (IMPLEMENTATION OF INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 27-G
STI/PUB/1760 (120 pp.; 2018)
ISBN 978–92–0–111516–4 Price: €46.00

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
STI/PUB/1786 (47 pp.; 2019)
ISBN 978–92–0–103017–7 Price: €38.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8-G (Rev. 1)
STI/PUB/1858 (37 pp.; 2020)
ISBN 978–92–0–103419–9 Price: €24.00

This publication aims to provide comprehensive, detailed guidance for States, competent authorities and operators to assist them in implementing IAEA recommendations and guidance for an effective physical protection system for nuclear material in use and storage and nuclear facilities. It provides further technical detail on how to design and evaluate such a system, with respect to the selection and integration of appropriate, effective physical protection measures.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA