IAEA NUCLEAR SECURITY SERIES NO. XX

NST055

DRAFT, August 2017

STEP 8: Submission to MS for comment

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

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 20XX

FOREWORD

[to be added later]

CONTENTS

1. INTRODUCTION

BACKGROUND

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

1.2. The Convention on the Physical Protection of Nuclear Material (CPPNM) [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] was ratified and entered into force on 8 May 2016, inter alia, extends the scope of the CPPNM to cover nuclear facilities and nuclear material in domestic use, storage and transport used for peaceful purposes, as well as sabotage thereof. Ref. [1] provides guidance to States Parties on meeting their obligations under the CPPNM and its Amendment.

1.3. A Handbook on the Physical Protection of Nuclear Material and Facilities[2], containing details for nuclear facility operators on the design, operation and maintenance of physical protection systems was issued in 2002, before the establishment of the IAEA Nuclear Security Series. This Technical Guidance publication updates the contents of that Handbook where they have not been included in other publications in the Nuclear Security Series.

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 [1] and

[1] For clarity of terms, this document uses the term physical protection system (PPS) to refer to the traditional physical protection measures that provide the functions of detection, delay and response. The term nuclear security is used when referring to the overall nuclear security programme elements, which in addition to the PPS include; computer security, nuclear material accountancy and control, information protection, and trustworthiness programs.

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

implementing guidance [2] for an effective physical protection system (PPS) for nuclear facilities and nuclear materials in use and storage. It provides further technical detail on applying the implementing guidance on how to establish, implement, improve and sustain a PPS, with respect to the selection and integration of appropriate, effective physical protection measures (including equipment). This Technical Guidance publication is intended to serve as a main reference, pointing users to other complementary guidance as necessary.

SCOPE

1.5. This Technical Guidance publication applies to physical protection systems for nuclear facilities and nuclear materials in use and storage against:

(a) Unauthorized removal of nuclear material, and

(b) Sabotage of nuclear facilities.

1.6. This Technical Guidance does not address infrastructural aspects of a national nuclear security regime related to physical protection, such as the legislative and regulatory framework or the institutions and organizations within the State responsible for implementing it. It also does not address in detail security measures complementary to the PPS, such as computer security measures (other than those to protect the PPS) or nuclear material accounting and control. Such aspects are addressed in other guidance [5–8] and, for the purposes of this publication, are assumed to be in place.

1.7. This Technical Guidance 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 all of the equipment and functions of a PPS to provide prevention of, detection of and response to nuclear security events. It refers, where necessary, to other relevant guidance. It also provides some general guidance on the evaluation of a PPS, pending development of detailed specific guidance.

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

1.9. This publication does not include detailed guidance on:

(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 nuclear facilities (except to the extent that physical barriers are used to mitigate the consequences of an attack);

(c) Location and recovery of missing nuclear material; or

(d) Physical protection considerations in the siting of nuclear facilities.

1.10. In addition, this publication does not address security of material in transport, which is covered in Ref. [9] for radioactive material and in Ref. [10] for nuclear material

STRUCTURE

1.11. Following this Introduction, Section 2 of this publication provides guidance on key functions and protection elements 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 detection, delay and response. Section 5 addresses the PPS response, while Section 6 addresses implementation of new and emerging technology. Section 7 addresses a PPS network and support systems. Section 8 addresses periodic equipment testing and the different types of testing such as: acceptance, operability, maintenance and calibration tests. Section 9 addresses evaluation of a PPS, Section 10 provides an overview of a PPS analysis and Section 11 provides guidance on management systems for nuclear security. Annex A provides an example of a needs assessment and requirements analysis for a new technology.

2. KEY FUNCTIONS OF A PPS

2.1. This section describes how the different physical protection measures and subsystems (as described in Section 4) fit together to provide a comprehensive. A PPS provides deterrence and a combination of detection; delay and response measures to protect against an adversary's attempt to complete a malicious act. Guidance on key PPS functions is provided in Ref. [2], while additional detailed guidance is provided later in this publication.

2.2. A PPS should integrate the elements of people, procedures and equipment to implement defence in depth, according to a graded approach, to address the range of threats identified in the applicable threat assessment or design basis threat (DBT) and to protect against both sabotage and unauthorized removal [1].

2.3. A PPS includes physical protection devices such as interior and exterior intrusion detection sensors, cameras, barriers, access control devices and response measures. A PPS normally has several automated sub systems designed to pass information and video images to a central alarm station (CAS) that allow operators to respond appropriately to specific information. The PPS should also provide a 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, including information security of the PPS elements and subsystems. One or more of these

subsystems may be integrated together; for example the intrusion detection system may be integrated with the access control system.

DETERRENCE

2.4. Deterrence is achieved when potential adversaries regard a nuclear facility as an unattractive target and decide not to attack it.

2.5. Penalties for unauthorized removal and sabotage should be part of the State's legislative or regulatory system [1] to deter an adversary from malicious acts. However, like other actions to promote deterrence, the value of deterrence is impossible to measure, especially with a determined adversary. Maintaining confidentiality of PPS sensitive information may deter an adversary as they would then lack the essential information necessary to plan a successful malicious act. However, this information may be compromised by an insider, without the knowledge of the authorities and operator. Enforcing the two-person rule for entry into an inner or vital area can be a deterrent, as well as an aid in detection of a malicious act.

2.6. Other examples of measures that may enhance deterrence at a facility include the following:

(a) A well-lit security area with physical protection systems may provide an impression of high security readiness at a facility to act as a deterrent to a potential adversary. A PPS designer may also want to consider the methodology behind 'crime prevention through environmental design' (CPTED).[3]

(b) The strategic use of guards and response forces may also contribute to deterrence. As an example, the nuclear facility may receive information regarding a planned peaceful protest on a certain day. Because potential threats could use peaceful protests to mask planned violent acts, the nuclear facility can use extra guards or response forces, 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 area of a nuclear facility may enhance deterrence. Additionally, the use of hardened guard positions, guard towers and armoured on-site response vehicles may also contribute to deterrence.

2.7. Although measuring deterrence is difficult, thoughtful use of physical protection measures to increase the visibility of guards and response forces and planned randomness of their actions

[3] See the website for the International CPTED Association: http://www.cpted.net/

(including patrols) may provide deterrence to reduce the likelihood of an adversary action. However, the fact that a PPS has not been challenged by an adversary does not necessarily mean that its effectiveness has deterred such challenges.

DETECTION

2.8. Detection is a PPS process that begins with sensing a potentially malicious or unauthorized act and is completed only when the cause of the alarm has been assessed. Detection without timely and accurate assessment is meaningless. If an alarm is assessed as valid, it is essential that a response is initiated.

2.9. Detection is not only the activation of sensors, but includes the detection of unauthorized persons and prohibited items through access control measures, as well as the reporting of suspicious incidents by guards and personnel. Detailed guidance on detection measures including intrusion alarms, assessment technologies, alarms stations, search systems, and access control is provided in Section 4.

DELAY

2.10. Delay is the function of the PPS elements that slow an adversary down towards a target after detection, providing time for an effective response. Delay is normally provided by physical barriers, but can also be provided by guards or response forces. However, all barriers can eventually be defeated. Detailed guidance on physical barriers is provided in Section 4.

RESPONSE

2.11. Response is the PPS function that seeks to interrupt and neutralize an adversary to prevent the completion of a malicious act. Detailed guidance on response is provided in Section 5.

3. DESIGNING PHYSICAL PROTECTION SYSTEMS

3.1. PPS design is best achieved using a systematic approach employing a systems engineering approach. Systems engineering is an approach used to design and build complex systems, and includes processes for defining requirements, designing systems and evaluating designs.

3.2. The systems engineering approach is accomplished by integrated project teams consisting of multidisciplinary groups of people responsible for developing and implementing a design using relevant systems engineering processes.

3.3. These processes are described in some detail in international standards[4]. For a specific PPS there may be a requirement to use one of these international standards for the systems engineering process, standards adopted within the nuclear industry of a State, regulations developed by the competent authority or some variant (i.e.: engineering change control management) adopted by the company constructing or operating the system.

3.4. This section describes a suggested methodology consisting of three high level PPS design phases using a systems engineering framework. The methodology includes:

(a) Identifying the objectives, requirements and specifications for the PPS;

(b) Designing the PPS to meet the objectives, requirements and specifications identified in Phase 1; and

(c) Analysing and evaluating the effectiveness of the PPS designed in Phase 2 to meet the objectives, requirements and specifications identified during Phase 1.

3.5. The sequencing of these three phases and a broad summary of the activities under each phase are illustrated in Fig. 1. While Fig. 1, here, is consistent with the diagram in Fig. 2 of Ref. [2], it has been slightly enhanced to address the important concept of verification of prescriptive requirements.

[4] See ISO 15288: 2015, Systems and Software Engineering – System Life Cycle Processes and INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities, Version 4.0 2015.

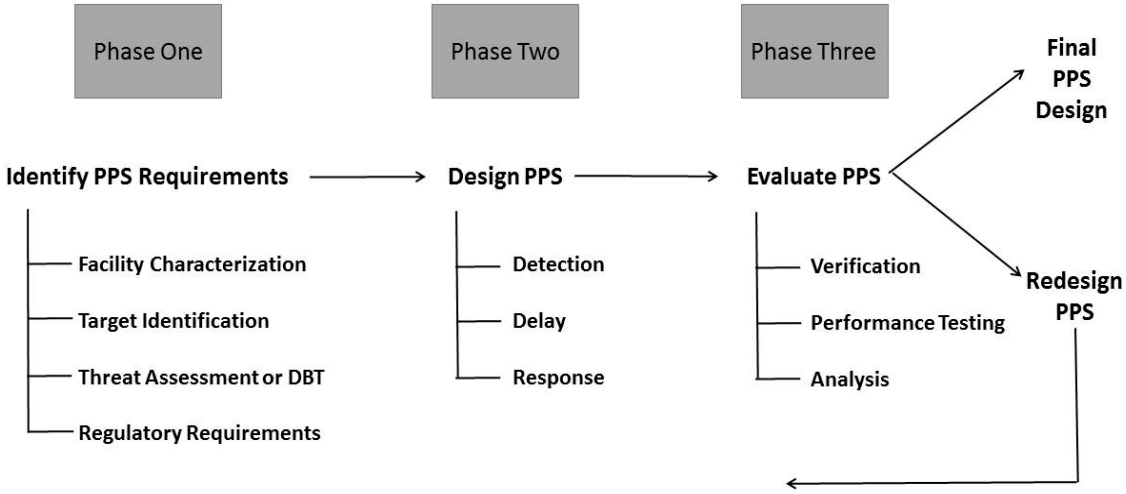

FIG. 1: Process for the PPS design.

3.6. Fig. 1 is an example of a systems engineering process that has been adapted to apply to the design of a PPS. The entire process in Fig. 1 applies either to either the case of a new system design, or to the case of an upgrade to an existing system. The three PPS design phases should normally be repeated, as necessary, in order to arrive at an effective PPS design.

IDENTIFYING REQUIREMENTS FOR A PPS (PHASE 1)

3.7. In order to begin Phase 1 of the design process for a PPS, the designer should first determine the State legal and regulatory requirements for physical protection. Determining how these requirements are applied at a facility or to nuclear material includes target identification, use of the threat assessment or DBT and characterization of the facility.

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

3.9. Other physical protection objectives, beyond the scope related to prevention of unauthorized removal and sabotage, as defined in Ref. 3, may also be identified by individual States (e.g. requirements for safety, economic importance, and potential consequences of loss of power generation or reputational damage).

Target identification

3.10. The target identification process is used determine which material and/or equipment within the facility needs protection and the level of protection required [2].

3.11. Individual State requirements for threshold levels of unacceptable radiological consequences (URC) and high radiological consequences (HRC) should be used to determine the physical protection requirements for nuclear facilities with identified targets [1]. The guidance in Ref. [11] may be used to determine vital areas within a nuclear facility.

3.12. Using a graded approach, each target will require 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 with the more stringent requirements for physical protection, either those against unauthorized removal or those against sabotage [1]. This may have the benefit of no substantial detection or delay measures to be employed for less attractive targets collocated within that area or building. However, the protection of each target still needs to be considered individually, especially from an insider threat perspective. Access to nuclear and other radioactive material, certain safety systems, sensitive information and/or certain computer systems located within an area should be controlled to the minimum number of authorized personnel necessary.

Use of threat information

3.13. A threat assessment or DBT as appropriate should be provided to the designer as a basis for designing and evaluating the PPS [1, 2, 12].

Characterization of the facility

3.14. The PPS should be designed to accommodate the types of processes and operations that will be performed, or are planned to occur, at the facility and to take into account all the different conditions at the facility affecting the PPS (e.g. environmental conditions or operational conditions).

3.15. One or more operational processes are normally performed at a nuclear facility and these processes may consist of one or more activities. Nuclear power plants have different operations and processes than those at nuclear fuel cycle facilities, and therefore the operational activities are different. The following paragraphs describe types of information that should be collected about these activities and processes [2].

3.16. It is necessary to understand the operating conditions expected to exist at the facility (e.g. normal operations, maintenance, shut-down and emergency conditions). Operational schedules define the activities to be performed at different times during the day and on different days. Information about the activities for moving nuclear material is also needed, including shipping and receiving processes for on-site and off-site movements or transfers. Additionally, safety and nuclear material accounting and control (NMAC) each have their own processes and activities that need to be

understood. The interfaces between these functions, for example between safety and physical protection, should be well characterized.

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

3.18. Facility characterization involves developing a thorough description of the facility and includes the location of the facility boundary, the exact location of buildings at the facility, building floor plans, structure elevations and normal and emergency access points. In addition, in the case of an existing facility or design, interconnectivity between buildings, above or below ground should be identified. Construction details about walls, ceilings, floors, doors, and windows of nuclear facility boundaries and target locations should be well characterized. Similar information concerning infrastructure including heating, ventilation, and air conditioning systems; power distribution systems; and locations of non-radioactive hazardous material (e.g., chemical inventories) that may be used as part of an adversary attack should be documented. Information including schematics of systems, such as redundant and dependant safety systems in a nuclear reactor should also be collected.

3.19. Information about the facility can be drawn from many relevant sources, including existing documentation, such as facility drawings and process descriptions, safety analysis reports, security and safety plans, construction diagrams, facility reviews, observations and interviews. When installing PPS into existing facilities, information should also include record drawings[5] that may be derived and validated through facility walk-downs. This information is important to PPS designers in understanding what needs to be protected and what facility-specific constraints (such as safety requirements) must be considered during the design.

[5] Revised set of drawing submitted by a contractor upon completion of a project or a particular job. They reflect 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 under the contract.

DESIGN A PPS (PHASE 2)

3.20. The design must ensure that security and safety requirements are met. During Phase 2, the designer determines how best to combine physical protection measures such as physical barriers, sensors, procedures, video surveillance, communication devices and response forces 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 NMAC, 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 fulfil its mission. The nuclear facility security plan should reflect the final design of the PPS [2].

General design considerations

3.21. Whenever safety, operations, and security requirements are in conflict, an appropriate balanced risk management approach should be achieved. The PPS design should provide adequate protection while not wasting valuable resources on unnecessary protection measures.

3.22. Principles in the design of physical protection systems include providing:

(a) Defence in depth, which is the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised [1]. It increases the adversary's uncertainty, may necessitate the adversary using additional tools and conducting more extensive preparations; and creates additional steps where the adversary may fail or decide to abandon the attack.

(b) A graded approach, which is the application of physical protection measures proportional to the potential consequences of a malicious act [1].

(c) Balanced protection, which is a method to use comparably effective physical protection measures whenever, wherever or however the range of threats defined in the threat assessment or DBT may attempt a malicious act.

(d) Robustness, which incorporates redundancy and diversity in the PPS design so that there is a high probability of effective protection against the range of threats defined in the threat assessment or DBT at all times and under all operational conditions..

3.23. In addition to meeting the principles listed above, a good practice for the PPS designer is to consider implementing designs that may be easily adapted to new and emerging threats, changes in the facility or targets, or changes in requirements. During the design, consideration may also be given to the ability of the PPS to account for the need to temporarily protect a target not normally used or stored in a location, so that it is protected at the appropriate level; e.g., emergencies, system failures,

or other conditions that require the use of alternative or compensatory measures to effectively protect the target. This may include consideration of procurement and use of rapidly deployable systems described in Section 4.

3.24. In order to mitigate the insider threat against unauthorized removal of nuclear material and sabotage, a comprehensive approach should include both preventive and protective measures including those provided by NMAC [8]. These include both administrative measures (procedures, instructions, administrative sanctions, access control rules and confidentiality rules) and technical measures (multiple protection layers providing detection and delay functions) that an insider would need to overcome or circumvent in order to achieve their objective. More detailed guidance on protecting against insider threats is provided in Ref. [13].

Intrinsic security

3.25. Integrating the principles defined above as early as possible in the facility lifetime is central to 'intrinsic security' [14]. If implemented properly, intrinsic security allows early consideration of the concept of adaptability (which might be achieved by buying more land than currently needed to allow for more demanding stand-off protection requirements in the future) and allows for 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 implemented during modifications at an existing facility for the remainder of its lifetime, although the options may be limited. Applying security requirements early in partial redesigns and modifications can result in security that is more cost efficient and effective against the defined threats.

3.26. Nuclear facility designers and operators have an incentive to maximize operational performance of a nuclear facility. Although very important, if this were the only consideration it could lead to negative impacts on nuclear safety and nuclear security. Historically, nuclear facilities have been designed without thought to security until late in the design phase or after facility or operational specifications had already been decided. Security organizations were then expected to simply add on security measures and features after the fact, which often resulted in application of costly physical protection measures that were not integrated with operational, safety, and other requirements. Adding security after-the-fact usually results in long-term reliance on less cost efficient protection measures to achieve compliance with security requirements or to reduce risk to an acceptable level, and may have had potentially avoidable, unintended impacts in these other areas.

EVALUATE THE PPS 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; the first activity is verifying the PPS meets prescriptive requirements. This is accomplished by conducting tests and assessments, as necessary. The second activity involves the conduct of performance tests to determine whether the PPS meets performance requirements. The final activity involves analysing data derived from the assessments, tests, and performance tests to determine the effectiveness of the PPS in protecting the facility against unauthorized removal of nuclear material or sabotage.

3.28. Evaluations of a PPS based on performance testing are recommended [1, 2]. In this Technical Guidance, 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 is in compliance with established performance requirements.

3.29. Periodic equipment testing includes acceptance and sustainability testing. Acceptance testing involves testing of equipment/systems which are newly installed, modified, or recently repaired prior to being brought into service. Acceptance tests determine whether the equipment/systems have been installed and are operating correctly prior to 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 DBT. Performance testing is addressed in Section 9.

3.31. The PPS evaluation programme should be appropriate for the particular phase it will be applied to during the lifetime of the nuclear facility. The operator could consider using independent experts to review its PPS before requesting approval for operation by the competent authority. When using independent experts, the sensitive information they hold or handle, must be protected in compliance with relevant national laws and requirements.

3.32. When physical protection systems are evaluated in conjunction with other systems such as safety engineering, it is advisable that an integrated team be formed that includes representatives from physical protection, response, operations, safety, NMAC, and other disciplines, as necessary, and staffed by personnel whose trustworthiness has been verified.

OTHER DESIGN CONSIDERATIONS

PPS integration

3.33. A PPS is an integrated system of detection, delay, and response measures. The PPS should be integrated and effective against both unauthorized removal and sabotage [1, 2]. Single PPS subsystems may be integrated and linked with each other, as described in Section 7.

3.34. An ideal PPS design process integrates safety, operations, physical protection, NMAC, 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 meet all requirements in the most effective and cost efficient manner. However, each of the four disciplines has different goals:

(a) Operations: the activities and systems required at the nuclear facility to achieve the facility mission (products or output). The goal is to achieve the facility mission most efficiently.

(b) Safety: the activities and systems that protect facility personnel, the public or the environment from harm caused by accident, equipment failure, and natural hazards. The goal is to make operations as safe as possible.

(c) NMAC: the activities and systems to maintain accurate information on nuclear material present at the facility. The goal is to maintain knowledge of the nuclear material amount and location, and to detect any unauthorized handling or movement [8].

(d) Physical protection: the activities and systems that protect nuclear material and nuclear facilities against unauthorized removal and against sabotage. The overall objective is to protect persons, property, society, and the environment from malicious acts involving nuclear material and other radioactive material [1].

Operations

3.35. Operational requirements are aligned with the nuclear facility mission. Some of these requirements include work hours, number of people requiring access to certain locations of the facility, throughput of security area access control points, number and type of entrances into a secure area such as a vital area. These requirements will affect the PPS, and should be considered in the PPS design phase.

Safety

3.36. Effectively managing the interface between safety and security is an important element of both programmes, to ensure appropriate physical protection of nuclear material and nuclear facilities

and health and safety of workers and the public [2]. It is important to ensure that physical protection does not compromise safety (and vice versa). This topic is further addressed under Work Direction and Control in Section 11.

3.37. One area where there is a need for close interaction between physical protection and safety specialists within a nuclear facility is sabotage target identification and subsequent protection of these targets. This should be accomplished using a graded approach, in a manner which does not compromise safety requirements and arrangements, but allows for effective protection of the targets. Each nuclear facility should perform analyses to:

(a) Determine whether the radioactive inventory at each location within the facility has the potential to result in URC, as determined by the State, using a graded approach;

(b) Identify equipment, systems or devices, the sabotage of which could directly or indirectly lead to URC; and

(c) Identify computer-based instrument and control systems important to safety and security.

3.38. Following such target identification, there is a need to design or re-design the PPS to be effective against credible sabotage scenarios derived from the applicable threat assessment or the DBT. This process needs to be carried out every time there is a change in the threat assessment or DBT, a change in the State determination of URC or a substantive change in the inventory of the nuclear facility. The process includes identification of vital areas (which contain radioactive material, equipment, systems and devices, the sabotage of which could lead to high radiological consequences), while taking into account engineered safety systems which already exist [11].

3.39. At the design stage of a facility, the integration of safety and security requirements at the same time may allow a benefit from synergies. For example, for nuclear safety and security reasons, redundancy and segregation of redundant equipment or systems may provide benefits for safety and for safety. On the contrary, providing for redundancy only for safety reasons without providing for segregation may be beneficial for safety but not for security. The segregation of redundant equipment can also provide security protection against sabotage by requiring more preparation, more equipment and more time for an adversary to complete a malicious act. Consequently, they could be very effective to deter, prevent or delay acts of sabotage or to mitigate or minimize the radiological consequences [13, 15].

3.40. Other examples of safety systems that may be the used to assist security are continuous air monitors or glove box negative pressure alarms that provide protection for operator personnel, which may be used to provide alarms for potential sabotage or unauthorized removal. These systems could be integrated for safety and security protection by establishing procedural or automated alarm communications between safety and security disciplines for certain operational or event conditions.

3.41. Radiation protection measures such as thick concrete walls or shielding barriers provide safety measures for personnel and may increase adversary delay time to target locations.

3.42. Nuclear power plants are specifically designed to handle extreme external and internal loads such as vibration, heat, overpressure and impact in the interest of safety. IAEA guidance 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 [15]. 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

3.43. At the nuclear facility level, a robust NMAC programme helps to deter and detect unauthorized removal of nuclear material by maintaining an inventory of all nuclear material and implementing control measures to maintain continuity of knowledge of the nuclear material and its location [8]. It should have the capability to register an alarm and to initiate a response if the system indicates that nuclear material may have been removed without authorization, or is being used in an unauthorized manner. An effective NMAC system can detect malicious insider activity involving nuclear material or NMAC records, and support the correct assessment of an irregularity involving nuclear material [8]. It is therefore important that the PPS and NMAC system function in a coordinated and complementary manner in order to defeat a wide range of threats.

3.44. IAEA guidance regarding establishing an NMAC system for nuclear security at a nuclear facility [2, 8, 16]. Application of this guidance can be used to help ensure an effective interface between the facility PPS and the NMAC system.

Protection of sensitive information

3.45. Adversaries wishing to carry out any malicious acts against a nuclear facility may benefit from access to sensitive information. Sensitive information may exist in many forms, including software where the unauthorized disclosure, modification, alteration, destruction or denial of use could compromise physical protection. Prior to beginning the three phases of designing 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. There is IAEA guidance on the security of sensitive information related to physical protection [1, 2]. Further guidance exists on information security, including an example classification guide to assist in identifying sensitive information [17].

3.46. Computer security is an important element of PPS design and should be considered in all stages of the PPS design [7, 18]. Further information on computer security for physical protection is given in Section 7.

4. PHYSICAL PROTECTION EQUIPMENT MEASURES

4.1. Physical protection measures include people, procedures, and equipment. These measures are implemented and sustained using management systems, as described in Section 11.

4.2. The objective of a PPS is to protect against unauthorized removal of nuclear material and sabotage of nuclear facilities [1, 2]. A PPS accomplishes these objectives using the functions of detection and assessment, delay, and response. These three main functions and their interaction are discussed in greater detail in this section.

4.3. A PPS is designed to meet the fundamental principle of defence in depth by the creation of layered security or concentric security areas [1, 2]. For the purposes of this publication, the term 'security areas' is used to generically to refer to limited access areas, protected areas, inner or vital areas and the concept of a strong room within an inner area. Fig. 2 is a conceptual example of these security areas.

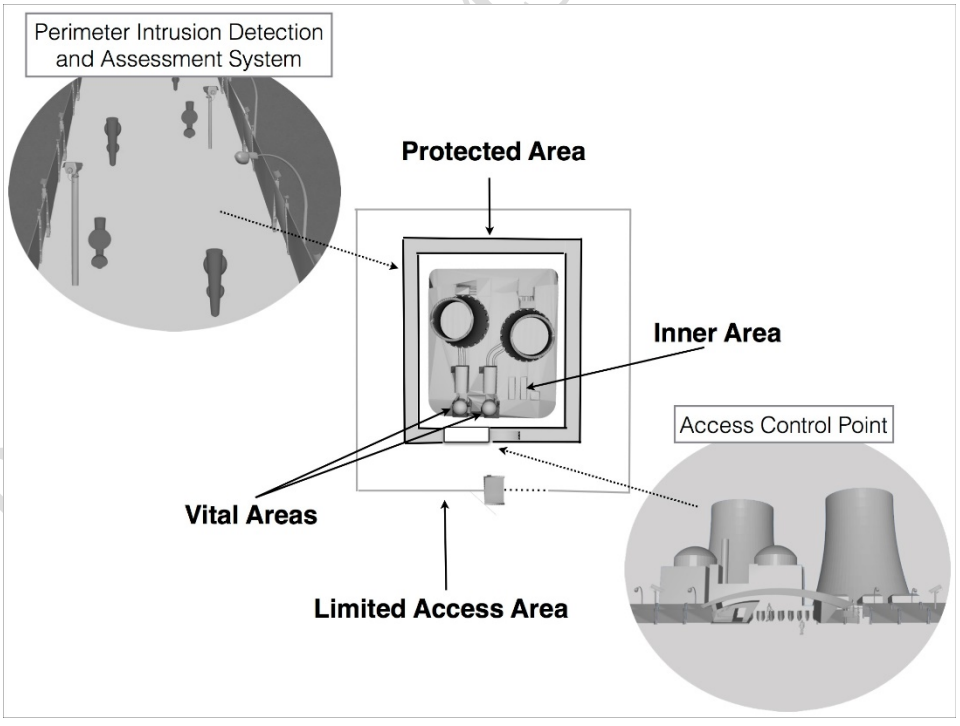

FIG. 2. Illustration of types of security areas.

4.4. PPS design is often a difficult and complex process. It is advisable that designers coordinate PPS design and equipment selection with national experts. Further assistance or advice, if needed, may be obtained through bilateral cooperation with other States, or from the IAEA.

DETECTION

4.5. The intrusion detection system is used to generate alarms that must be assessed to determine if they are caused by unauthorized acts or unauthorized presence. Intrusion detection systems normally consist of exterior and interior intrusion sensors, video alarms, access control, and alarm communication systems all working together to indicate a change in the local environment of a sensor. The intrusion detection system should detect threats and their associated capabilities as defined in the applicable threat assessment or DBT. 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 detection technologies available, how they work and their shortcomings.

4.6. Fig. 3 illustrates typical components of a perimeter intrusion detection system.

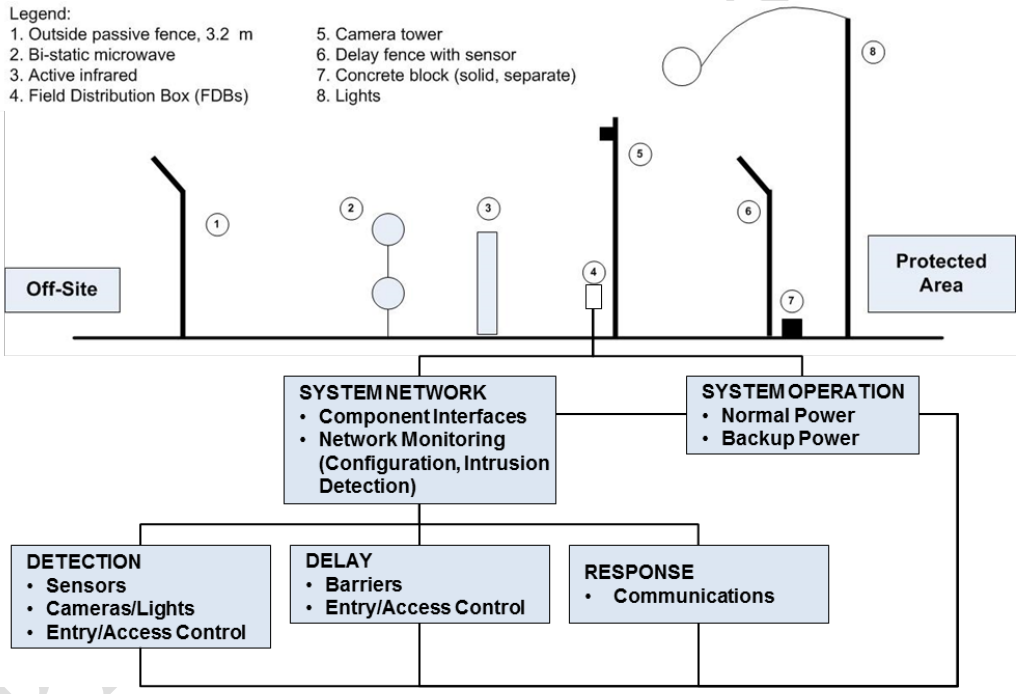

FIG. 3. Perimeter intrusion detection system components.

Performance characteristics

4.7. Intrusion sensor performance is described by fundamental characteristics, including probability of sensing, nuisance alarm rate and vulnerability to defeat.

4.8. Probability of sensing depends upon the area and target to be detected, the sensor design, installation conditions, sensitivity adjustments, weather and other environmental conditions and

condition of the equipment. An ideal sensor detects 100% of attempted intrusions; however, no sensor is ideal, but the probability of sensing should be as high as possible. The probability of sensing may significantly depend upon the capability of the adversary in the applicable threat assessment or DBT.

4.9. Conditions will vary for different installations and despite the claims of some sensor manufacturers, a specific probability of detection cannot be assigned to a sensor or set of sensor hardware. In addition, over time the probability of sensing will vary as equipment ages and conditions change. Therefore, the probability of sensing should be checked by periodic performance tests (see Section 8).

4.10. Nuisance alarm rate is the rate of alarms over a period of time generated by events not associated with an intrusion or with planned events, such as sensor testing. These events may include environmental factors, such as wind, rain, wildlife or authorized personnel inadvertently causing alarms, or poor system installation or design. Nuisance alarm rates are generally expressed as an average of the alarms over a period, for example, one alarm per minute, one alarm per hour or one alarm per day. Nuisance alarms generated by the equipment itself are termed false alarms (e.g., caused by poor design or component failure), and are not discussed further in this section. Controlling and maintaining the sensor environment to minimize nuisance alarms will contribute to the overall effectiveness of the PPS. In an ideal situation, the nuisance alarm rate would be zero. However, all sensors interact with their environment and the sensor cannot discriminate perfectly between intrusions and other events, such as blowing debris in the detection zone. Because many nuisance alarms are caused by uncontrollable factors, such as weather and animals, this number can be highly variable. Since not all alarms are caused by an intrusion, some means of assessment is needed.

4.11. Usually nuisance alarms are further classified by source. Common sources of nuisance alarms for exterior sensors are vegetation (trees and weeds), wildlife (animals and birds), and weather conditions (wind, rain, snow, fog, lightning). Other sources of nuisance alarms include ground vibration, electromagnetic interference, nuclear radiation, acoustic, thermal, and optical effects and chemical exposure.

4.12. Evaluating nuisance alarms to determine their cause is important to understand and reduce them. Nuisance alarms can be reduced by focusing on the cause of the alarm, reducing the sensitivity of the alarm, or the use of technologies that help filter nuisance alarms. Examples of reducing the sources of an alarm include addressing water runoff through a sensor bed during rainstorms, installing fencing to reduce vegetation blowing through the area during high winds, or by implementing sound alarm management processes. An example of changing alarm management processes is implementing procedures to mask alarms in an area occupied by authorized personnel rather than leaving the alarms active, which results in many nuisance alarms. Another way to reduce nuisance alarms is to reduce the

sensitivity of individual sensors. This should be done carefully to ensure the reduced sensitivity does not reduce the probability of sensing a real threat to an unacceptable level.

4.13. A third method to reduce nuisance alarm rates is to select technologies that are designed to filter out some nuisance alarms. An example is the use of dual technology sensors, which is the use of two different sensor technologies that are typically setup as an AND gate logic configuration. The AND gate logic requires both sensors to activate to produce a valid alarm. An example of dual technology would be to place both a passive infrared (IR) and a monostatic microwave in the same housing. The device would not give an alarm until both sensors alarmed, thus avoiding common nuisance alarms from each of the technologies and increasing the probability of sensing an actual alarm. In this mode, the sensitivity of each sensor could be set very high without the associated nuisance alarms of a single sensor type.

4.14. However, when two sensors are combined with AND logic, the probability of sensing for the combined detectors will be less than the probability of sensing of the individual detectors. In the example in the previous paragraph, microwave detectors have the highest probability of detecting motion directly toward or away from the sensor, but IR sensors have the highest probability of sensing someone moving across the field of view. Therefore, the probability of sensing for the combined sensors in a single unit will be less than if the individual detectors are mounted perpendicular to each other with overlapping energy patterns and field of view. If a higher probability of sensing is needed for the application, separately mounted logically combined sensors should normally be used.

4.15. Different types of sensors have different vulnerabilities or defeat methods. Thus, a design objective for the PPS is to have a comprehensive design using different (complementary), overlapping sensors for a particular layer of detection, so that it is difficult for an adversary to simultaneously defeat multiple sensors based on different technologies using the same defeat method. Complementary sensors enhance the overall system performance, expressed in terms of the three fundamental sensor characteristics: 1) probability of sensing, 2) nuisance alarm rate, and 3) vulnerability to defeat. This design philosophy results in detection of a wider spectrum of targets, allows operation of at least one sensor line during any conceivable environmental disturbance, and increases the difficulty of defeating the system.

4.16. Another important aspect for consideration is availability of the intrusion detection system. Availability is the ability of a system to perform its required functions over the life of the system. Availability can be addressed through the use of redundant components, components with longer lifetimes, and through well-designed sustainability programmes, including preventive maintenance, which is discussed in Section 11.

4.17. Exterior sensor technology often requires an unobstructed area around the sensor to allow the technology to detect and provide for clear visual assessment of the causes of sensor alarms. A design

goal for an exterior detection system is to have uniform detection around the entire length of the perimeter. At the perimeter, this area is typically a clear zone usually parallel to the fences. The clear zone is meant to keep people, animals, and vehicles out of the detection zone and is usually cleared of all above ground structures, including overhead utility lines. Vegetation in this area is also eliminated with only the detection and assessment equipment in the zone. In areas where the primary sensor cannot be deployed properly, such as a gate, an alternate sensor is used to cover that gap.

Environmental conditions

4.18. A large number of environmental conditions can produce noise in the same energy spectra that the intrusion sensors are designed to detect. These outside noise sources can degrade sensor performance and may cause the sensor to generate an alarm even when an intruder is not present. The following paragraphs discuss several design considerations and factors which can degrade a sensor's performance.

4.19. General environmental factors that can degrade sensor performance are: electromagnetic energy, nuclear radiation, chemical exposure, as well as acoustic, thermal, optical, seismic and meteorological conditions. These factors influence the selection of appropriate sensor technology and may require specific mitigation measures.

4.20. Sources of electromagnetic energy that could affect the performance of a particular type of interior detection system include lightning, power lines and power distribution equipment, transmission of radio frequency (including linked remote control), telephone lines and equipment, lighting, computer and data processing equipment, electric powered vehicles such as forklifts and elevators, television equipment, automotive ignition, electrical machinery or equipment, intercom and paging equipment, and aircraft. The construction of the building or room to be monitored by an interior 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 sources outside the building or room is possible. The best way to minimize the effects of stray electromagnetic energy is to provide electromagnetic shielding to all system components (including all data transmission links) and to ensure that all the components have a common, adequate electrical ground.

4.21. Radiation can damage some of the components within a sensor. The components in a typical sensor most susceptible to the effects of radiation are semiconductors. Research has shown that current technologies cannot be made totally invulnerable to the effects caused by some radiation environments. System vulnerability can, however, be reduced by the appropriate design and choice of components. Generally speaking, neutrons will degrade the performance of semiconductor devices and integrated circuits, with the degradation primarily depending on the total dose.

4.22. Chemical processing environments associated with the nuclear industry can negatively affect sensors and security electronic components. Exposure of electronic processing boards installed in areas of corrosive substances in conjunction with associated levels of high humidity can deposit chemical residues on circuitry resulting in significant corrosion to the components. This exposure can reduce the performance and reliability of the sensor components. Although in principle, sensor electronics should normally be protected to reduce this adverse effect, new material combinations are emerging and due to the demand for miniaturization the impact of corrosion on these materials is ever changing. To address this issue, environment appropriate sensor maintenance and testing should be conducted to ensure sensor effectiveness.

4.23. Acoustic energy is generated by many sources and energy generated by outside sources can be transmitted into an area to be protected. Some of the forms of acoustic energy that can affect the performance of interior sensors are noise from meteorological phenomena; ventilation, air-conditioning and heat equipment; television equipment; telephone electronic equipment; and exterior sources such as aircraft, vehicles, and trains.

4.24. Changes in the thermal environment can result in stimuli that affect the performance of interior intrusion sensors. These stimuli include uneven temperature distribution that causes air movement within the area and expansion and contraction of buildings. 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.

4.25. The sources of optical phenomena that affect interior intrusion sensors include light energy from sunlight, interior lighting, highly reflective surfaces, and IR and ultraviolet energy from other equipment.

4.26. Sources of seismic interference that can cause nuisance alarms include both natural and man-made sources. The primary natural source of seismic interference is wind energy that is transmitted into the ground by fences, poles, and trees. Examples of man-made sources of seismic interference include vehicular traffic (cars, trucks, trains) and heavy industrial machinery.

Sensor classification

4.27. Sensors are either passive or active, and can be installed in a covert or overt manner. Sensor types may be volumetric, point or line detection. These classifications are listed in the table below. Sensor applications include buried line, fence associated, free standing, terrain following, boundary penetration interior motion, and object.

Passive or active sensors

4.28. Passive sensors detect some type of energy emitted by the target of interest or detect the change of some natural field of energy caused by the target. Examples of the former are mechanical energy from a human walking on the soil or climbing on a fence. An example of the latter is a change in the local magnetic field caused by the presence of a metal.

4.29. Active sensors transmit some type of energy and detect a change in the received energy created by the presence or motion of the target.

4.30. The presence or location of a passive sensor is more difficult to determine than that of an active sensor. Active sensors may be less affected by environmental conditions than passive sensors because they are transmitting signals selected to be compatible with those conditions. Because of this an active sensor typically may have fewer nuisance alarms than a passive sensor in the same environment.

Covert or overt

4.31. Most sensors are originally designed with certain features to be either covert or overt but they can be modified in their installation to provide deterrence or mask the technology.

4.32. Covert sensors are hidden from view, such as sensors buried in the ground or contained in walls. Covert sensors are more difficult for an intruder to detect and locate (than visible sensors), and thus can be more effective. However, active covert sensors can be detected using electronic equipment.

4.33. Visible (overt) sensors are in plain view of an intruder, such as sensors that are attached to a fence or mounted on another support structure. Visible sensors may deter an intruder. Visible sensors are typically simpler to install and easier to maintain than covert sensors.

Detection type

4.34. Volumetric sensors detect intrusion in a volume of space. An alarm is generated when an intruder enters the detection volume. The detection volume is generally not visible and is difficult for the intruder to precisely identify. The detection volume characteristics are based upon a number of factors including frequency, antenna properties (cable spacing, mounting height, sensitivity, alignment).

4.35. Line sensors detect along a line. Detection occurs only if the intruder is disturbing the detection line. The detection zone of a line detection sensor is usually easy to identify.

4.36. Point sensors detect at a specific object. The point sensor detects when someone attempts to touch or move an object.

Sensor applications

4.37. Sensors can be used in an external environment or in an interior application. For an external use the environmental conditions need to be considered. Interior applications of sensors are less effected by environmental conditions and may include boundary penetration, interior motion, and detection of proximity to an object. In addition to typical sensor applications, there are early warning systems that detect beyond the facility boundary. When selecting a sensor for a certain application it is important to consider whether the sensor needs to be line-of-sight or terrain-following.

4.38. Early warning systems may provide a facility with other applications, such as looking for intruders outside controlled facility boundaries. In principle, early detection of the adversary provides the protective force more time to position them or to engage the potential threat prior to reaching the area of interest. These technologies include long and short range ground surveillance radar, scanning thermal imaging, and laser radar. The effective range of these systems varies from hundreds of meters to tens of kilometres, potentially providing seconds or even minutes of early detection. Such systems depend on a line-of-sight between the sensors and the intruder. Sensors may also be installed in areas outside the facility security boundaries not within line-of-site of other sensors and assessment systems. In such applications, the sensors are designed to be covert and totally self-contained.

4.39. Offsetting such benefits, such systems pose significant design and operational challenges which might prevent their effective use. Some of these challenges are described below.

4.40. Early warning systems do not typically have similar performance measures as those required for traditional exterior sensors, if they are used beyond the facility boundary. Objectively determining these performance measures is a challenge given the nature of these systems and the large areas they can potentially cover. Performance can be expected to vary depending on nuclear facility specific factors such as environment and topography.

4.41. Line-of-sight systems should be designed to provide a direct view from the transmitter to the target or from the transmitter to the target back to the receiver, and therefore operate most effectively in open areas. The systems will detect wildlife and wind-induced movement of vegetation within its field of view. In areas where wildlife activity is high and/or vegetation is abundant, the nuisance alarm rate can be high. To be most effective, the system itself should normally have detection range-limiting settings and functions, or masking capabilities, in order to ignore alarms from movement in populated areas outside the desired detection area.

4.42. Terrain-following sensors as illustrated in Figure 4 are used to detect uneven areas where the topography of the perimeter has shapes that are difficult to detect. This type of sensor may or may not be fence associated, and installed to detect areas that are difficult to provide detection using other methods.

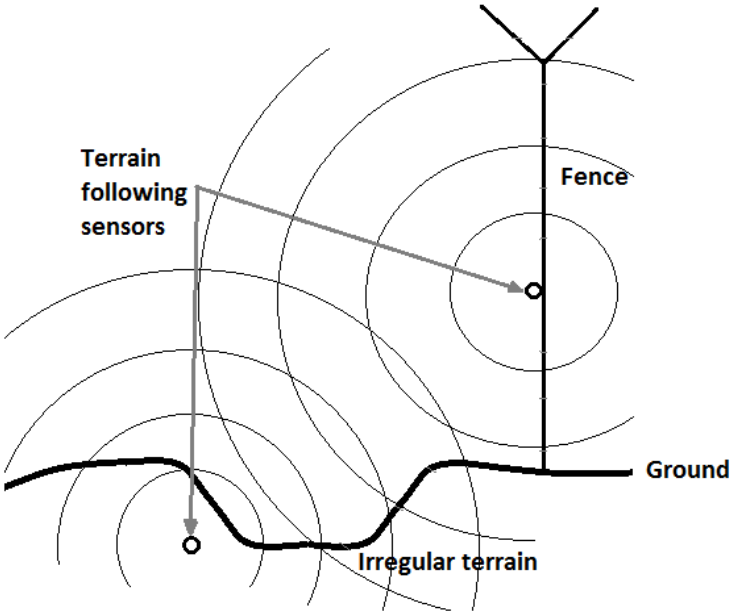

FIG. 4. Example of terrain following sensor coverage.

4.43. Sensors can be used in a range of applications. These applications are briefly discussed in this section. Possible uses of technologies in different applications are summarized in Fig. 4.

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

4.45. Fence associated sensors can either be mounted on a fence or form the structure of the fence. Examples of sensors mounted on fences include fibre optic cables, capacitance sensors and vibration sensors. Sensor fences also include strain sensitive sensors. This list is not exhaustive; indeed many different sensor technologies exist and are in use.

4.46. Freestanding sensors are used for perimeter detection and as area detection (possibly) within the facility. Technologies include: active and passive IR laser, bi-static and monostatic microwave and video motion detection sensors.

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

4.48. Interior motion sensors are used to detect movement within an interior space. Technologies include: IR or microwave sensors.

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

Exterior sensors

4.50. Each nuclear facility requiring physical protection has a unique combination of configuration and physical environmental conditions that can affect the selection of exterior sensors. These conditions include: the physical environment, which will influence the selection of types of sensors for perimeter sensor systems, the natural and industrial environments that provide the nuisance alarm sources for the specific site, and the topography of the perimeter that determines the shapes and sizes of the space available for detection, specifically the clear zone width and the existence of flat or irregular terrain. Thus, a PPS designed for one nuclear facility may not be transferred to another.

4.51. Although the understanding of the interaction between intrusion sensors and the environment has increased significantly in recent years, it is a good practice to set up a demonstration sector (testing area) on site using the possible sensors before making a commitment to a complete system. This demonstration sector located on site is intended to confirm sensor selection and to help refine the final system design. It is advisable that test beds be in place during all seasons to assess the capabilities of the sensors in the actual environments the facility will experience.

Fence mounted sensors

4.52. All fence-associated sensors respond to mechanical disturbances of the fence. Thus, they are intended to detect primarily an intruder who climbs on or cuts through the fence fabric. Several kinds of transducers are used to detect the movement or vibration of the fence. Since fence-associated sensors respond to all mechanical disturbances of the fence, nuisance alarms need to be considered. Disturbances may include strong winds, debris blown by wind, rain driven by wind, hail, and seismic activity from nearby traffic and machinery. Good fence construction, specifically rigid fence posts and tight fence fabric, is important to minimize nuisance alarms

Seismic

4.53. Seismic sensors are passive, covert, line, terrain-following sensors that are buried in the ground. They respond to disturbances of the soil caused by an intruder walking, running, jumping, or crawling on the ground.

4.54. A typical seismic sensor consists of a string of geophones. A geophone consists of 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 both cases an electrical current is generated in

the coil. Far-field effects in seismic sensors can be somewhat reduced by alternating the polarity of the coils in the geophone string.

4.55. The sensitivity of this type of sensor is very dependent on the type of soil in which it is buried. The best burial depth is also dependent on the soil. The trade-off is high probability of sensing with narrow detection width at a shallow depth versus lower probability of sensing with wider detection width at a greater depth. A test conducted on site with short test sections of the sensor buried at different depths is suggested to determine the optimum depth. A typical detection width for walking intruders is in the range of 1–2 m.

4.56. Seismic sensors tend to lose sensitivity in frozen soil. Thus, at sites where the soil freezes in winter, either reduced winter sensitivity may be accepted, or a seasonal adjustment to pressure and seismic sensors may be made to obtain equivalent sensitivity throughout the year.

4.57. Many sources of seismic noise may affect these sensors and cause nuisance alarms. The primary natural source of nuisance alarms is wind energy that is transmitted into the ground by fences, poles, and trees. Seismic sources made by man include vehicular traffic (cars, trucks, trains) and heavy industrial machinery. Because it is difficult to distinguish between footsteps close to the sensor and vehicle traffic much farther away with these types of sensors, they are seldom used in perimeter applications and are more frequently used in border applications.

Magnetic field

4.58. Magnetic field sensors are passive, covert or overt, volumetric, fence-associated and terrain-following. They respond to a change in the local magnetic field caused by the movement of nearby metallic material.

4.59. This type of sensor consists of 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 a current. Magnetic field sensors can be susceptible to local electromagnetic disturbances such as lightning. It is difficult to tell whether the alarm was caused by an intruder with a small weapon close to the sensor or a large vehicle passing outside of the perimeter. This technology is not designed to detect non-metallic threats.

4.60. These sensors can be designed to be used underwater or on surface areas at boundaries for early detection of the intrusion to the protected area. They provide detection of the intruders and their direction of movement if they are carrying metallic objects (i.e.: weapons).

Ported coax

4.61. Ported coaxial cable sensors are active, overt or covert, volumetric, fence associated, terrain-following sensors that are buried in the ground. They are also known as leaky coax or radiating cable

sensors. This type of sensor responds to motion of a material with a high dielectric constant or high conductivity near the cables. These materials include both the human body and metal.

4.62. The name of this sensor is derived from the construction of the transducer cable. The outer conductor of this coaxial cable does not provide complete shielding for the centre conductor, and thus some of the radiated signal leaks through the ports of the outer conductor. The detection volume of ported coax sensors extends significantly above the ground: about 0.5 to 1.0 m above the surface and about 1 to 2 m wider than the cable separation. The sensitivity of this sensor depends on the conductive soil.

4.63. Some ported coaxial cables use a foil shield with a slot instead of actual ports. A semi-conductive inner jacket allows the combination of the two cables into a single outer jacket. This allows the sensor to be installed more easily using a single trench and cable spacing is no longer an issue. The disadvantage is that the detection volume is slightly smaller than for a dual cable system with wider cable spacing.

4.64. Older versions of this technology provided a single alarm indication for a single zone, typically 100 metres, and also allowed only a single alarm threshold for each zone. Newer versions can provide the location of where the alarm occurred along the cables within a few meters of resolution. In addition, the alarm thresholds may also be varied along the length of the cables, allowing more even sensitivity settings as the sensor cables pass through different burial mediums.

4.65. Metal or water in the ported coax detection zone can cause two types of sensor problems. Moving metal objects and moving water are large targets for ported coax sensors and thus are a major potential source of nuisance alarms. Both flowing water and standing water contribute to this problem. The second problem is that fixed metal objects and standing water distort the radiated field, possibly to the extent of creating insensitive areas with no detection. Nearby metal objects, utility lines, fences and poles, underground water lines, and electrical cables should be excluded from the detection volume.

Fibre optic

4.66. Fibre optics sensors can be passive or active, covert or visible, line, buried line or fence associated and is terrain following. Fibre optics uses transparent fibres to guide light from one end to the other. A fibre optic cable consists of an inner core of pure material and a cladding material. Because the cladding is designed to have a different refraction of light, the light ray is bent back towards the centre of the core. Fibre optic cable does not need to be straight because of the characteristics of the fibre, the light tries to remain in the core of the fibre. The light diffraction (speckle) pattern and the light intensity at the end of the fibre optic cable is a function of the shape of

the fibre over its entire length. Even the slightest change in the shape of the fibre can be sensed using sophisticated sensors and computer signal processing at the far end (100 meters or more).

4.67. Fibre optic continuity sensors may be used for the detection of structural boundary penetration such as breaking through walls or ceilings. Fibre optic micro-bend sensors can be applied as vibration or pressure sensors.

4.68. A single mode fibre can also be used as a sensor by splitting the light source and sending it both directions around a loop. If the fibre is disturbed, the two light sources come back in a different phase. The change in phasing relates to the amount of disturbance. Thus a single strand of fibre optic cable, buried in the ground at the depth of a few centimetres, can very effectively give an alarm when an intruder steps on the ground above the fibre. To ensure that an intruder steps above the fibre, it is usually woven into a grid and buried just beneath the surface.

4.69. For fence mounted applications fibre optics can be either mounted on the fence or woven into a mesh that can be installed on a fence to create a sensor fence. These mesh fences usually use some type of continuity detection to determine when an intruder has cut through the fence. The upper portion of the fence is usually configured mechanically in such a manner that the fibre is crimped when an intruder attempts to climb over the fence. The crimp of the fibre reduces the amount of light passed through the fibre causing an alarm.

4.70. Nuisance alarm sources for micro-bend fibre optic sensors are similar to sources for vibration sensors. Vibrations caused by external sources such as rotating machinery, low flying aircraft, nearby trains, or large vehicles can cause nuisance alarms. Some nuisance alarm sources can be filtered out by adjusting the sensitivity, frequency filtering, event counting, and event timing. It is advisable that caution be exercised against decreasing sensitivity to intrusion detection system when adjusting to reduce nuisance alarms.

Strain sensitive

4.71. Strain sensitive sensors are passive, visible and line or fence associated. These sensora can make up the fabric or be attached to the fences and are designed primarily to detect climbing or cutting on the fence.

4.72. Taut wire type fencing is a form of strain sensitive sensors consisting of many parallel, horizontal wires with high tensile strength that are connected under tension to transducers near the midpoint of the wire span. These transducers detect deflection of the wires caused by an intruder cutting the wires, climbing on the wires to get over the fence, or separating the wires to climb through the fence. The wire is typically barbed wire, and the transducers are mechanical switches, strain gages, or piezoelectric elements. Taut wire sensor fences can either be mounted on an existing set of

fence posts or installed on an independent row of posts. Other configurations of fence vibration sensors use strain sensitive cables for detection.

Sonar

4.73. Sonar acoustic sensors are active, covert, volumetric and free standing. A sonar sensor system typically uses acoustic sensors and can be designed for protection of water areas adjoining the protected facilities and provides detection and tracking of persons or objects penetrating into the controlled or protected area. Sonar provides reliable detection of underwater objects under unfavourable marine conditions. Operation of several systems can be used as overlapping detection zones as part of the overall PPS.

4.74. Sonar works on the principle of pulsed sounding hydro-acoustic signals formation and emission and the subsequent reception of the detected echo signals, reflected from the moving underwater threats. Antenna module signals are transmitted through the main cable to the hydro-acoustic service device. Sonar can be installed both at the bottom of water area, and on hydraulic engineering constructions-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 depends on the underwater terrain and operational conditions.

Radar

4.75. Radar sensors are active, visible, volumetric, line-of-sight, and free standing. Radio detection devices are designed to emit a radio signal to detect anomalies in the area being protected. It is used for monitoring a controlled area and provides detection and tracking of persons and objects, such as a small watercraft and an above-surface swimmer. It can determine the exact location, speed and route of the threat's movement. This technology works on the principle of short radio signals emission and timing between radio signals reflected from the potential threat.

Laser radar

4.76. Laser radar sensors are active, visible, volumetric, line-of-sight, and free standing. Radio detection devices are designed to emit a laser beam to detect objects in the path of the laser. It measures the time it takes for the light to return to the transmitter in order to detect objects. This technology works on the principle of reflection of the laser beam.

Interior sensors

4.77. Interior sensor selection consists of identification of the equipment and installation methods that best meet the intrusion detection system objectives for a given facility. A consideration of the interaction among equipment, environment, and potential intruders is integral to the selection of the

proper technological type of equipment necessary to ensure the desired intrusion detection system functions. Two important physical conditions that affect sensor performance are the building or room construction and the equipment or objects that occupy the same area or room to be monitored.

4.78. It is usually easier to identify appropriate interior sensors since building environments are usually predictable, measureable, and controllable. However, correct sensor choice requires that the particular susceptible nuisance alarm stimuli be known, as well as whether these stimuli are contained in the environment in question. This is particularly true of the motion detectors (microwave and IR), all of which can be installed to provide acceptable detection coverage and which typically have nuisance alarms from different stimuli.

4.79. Optimum performance of an interior intrusion detection system can be achieved by an appropriate combination of sensors and sensor technologies. Fig. 5 shows an example arrangement of interior sensors layout.

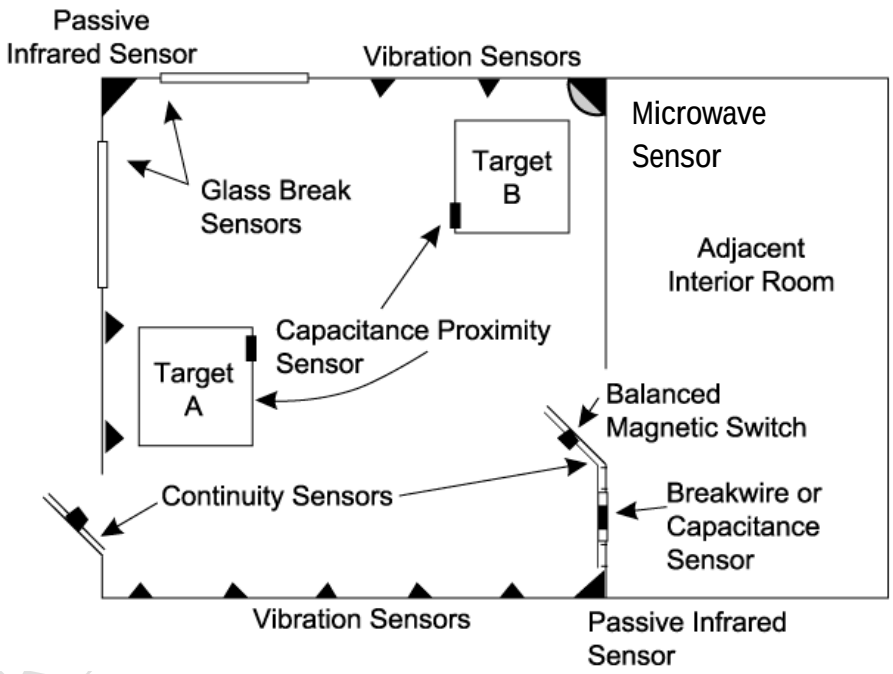

FIG. 5. Example layout on interior sensors.

Pressure

4.80. Pressure sensors are passive, covert, point, object and boundary penetration. They are often in the form of mats, can be placed around or underneath an object. Pressure mats consist of 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. They are constructed so that when an adequate amount of pressure, 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 carpets or even under tile or linoleum floor coverings.

Break-wire

4.81. The break-wire (continuity) sensors are passive, covert, line, and boundary penetration. They are usually attached to, or enclosed in, walls, ceilings, floors or windows to detect penetration through many types of construction materials. The sensor consists of small electrically conductive wires and electronics to report an alarm when the conductor is broken. The wires can be formed in any pattern to protect areas of unusual shape. Printed circuit technology can be used to fabricate continuity sensors if desired. Break-wire grids and screens can be used to detect forcible penetrations through vent openings, floors, walls, ceilings, locked storage cabinets, vaults, and skylights. Nuisance alarm rates for this class of sensor are very low since the wire is broken to initiate an alarm. When an alarm occurs, the sensor should be repaired or replaced. A similar capability can be achieved using continuity fibre optic sensors. An alarm is caused when the fibre optic cable is broken.

Glass break

4.82. Glass break sensors are passive, visible, line and boundary penetration. They employ either vibration or acoustic technology. Parameters for an effective use of these sensors include glass thickness, type, and maximum mounting distance from protected windows and possible window coverings (curtains, blinds, laminates, and other large objects that may deaden the sound of the glass). Vibrations in glass due to machinery or objects striking glass with sources that generate the higher frequencies of breaking glass can cause nuisance alarms as well as dropping keys or glass items. Vibration glass break sensors that are mounted directly on the glass are likely to provide better performance because the direct contact with the glass provides better glass break detection. Windows with vibration glass break sensors may have additional magnetic contacts to detect the removal of the glass from the frame.

4.83. Acoustic sensors are typically mounted on a ceiling or wall within a specified distance from the window(s) being protected. In order to generate an alarm, most of these sensors need to sense the initial low frequency impact followed immediately by the higher glass breaking frequencies.

4.84. Vibration sensors are mounted directly on glass and are designed to generate an alarm when the frequencies associated with breaking glass are present within the glass or when an initial impact on the glass is extremely hard. These frequencies are normally above 20 kHz. The vibration type can employ piezoelectric sensor or jiggle switch technology.

Interior and exterior sensors

4.85. Some sensors can be used for both interior and exterior applications. With certain adjustments in installation, sensors can be used in different environments. Considerations for installation of sensors should normally include:

(a) Location (near target vs at the boundary);

(b) Mounting;

(c) Resistance to tampering;

(d) Weather proofing (e.g. against water, extreme temperature, dust);

(e) Varying light levels;

(f) Ease of access for maintenance; and

(g) Manufacturer's specifications.

Active infrared

4.86. Active IR sensors consist of active, visible, line or volumetric, line-of-sight, 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 applications for filling gaps, such as for gates, doors, and portals. They may also be used in applications with long ranges up to about 100 m.

4.87. Active IR sensors work by transmitting a beam from an IR light-emitting diode through a collimating lens. This beam is received by a collecting lens that focuses the energy onto a photodiode. The IR sensor detects the change of the received IR energy when an opaque object blocks the beam or changes the reflection characteristics. These sensors operate at a wavelength which is not visible to the human eye.

4.88. Although single-beam IR sensors are available for point to point systems, multiple-beam sensors are normally used for high-level security applications because a single IR beam is too easy to defeat or bypass. Fig. 6 shows a point to point system with multiple-beam IR sensor system that typically consists of two vertical arrays of IR transmitter and receiver modules. The specific number and configuration of modules depends on the manufacturer. Thus the IR sensor creates an IR fence of multiple beams but detects a single beam break. Multiple beam sensors usually incorporate some type of logic that will alarm if an intruder attempts to capture a receiver with an IR source.

FIG. 6. Active point to point infrared system using multiple beams.

4.89. Conditions that reduce atmospheric visibility have the potential to block the IR beams and cause nuisance alarms. If the visibility between the two arrays is reduced, the system may produce nuisance alarms. This could be caused by fog, snow, smoke and dust. Falling objects, small animals, or anything that could interrupt the IR beam long enough can cause an alarm.

4.90. Active IR sensors require a flat ground surface because the IR beam travels in a straight line. A convex ground surface will block the beam, and a concave surface will permit passing under the beam without detection.

Passive infrared

4.91. Passive infrared (PIR) sensors consist of passive, visible, volumetric, line-of-sight, and can be free standing or used for interior motion detection. PIR detectors sense the change of thermal energy caused for example by a human entering the detection area. Special lenses focus the IR energy onto the detector of the sensor and create a specific detection field of view. The field of view can be changed from covering a wide angle to narrow long distance view by changing lenses. The wide angle lenses provide volumetric detection, such as within a room, while the long narrow lenses can be used to protect a corridor. The lenses also segment the field of view into sensitive and non-sensitive areas.

4.92. It is advisable for passive infrared sensors to be mounted such that the motion of the intruder will most likely be across the line of sight, since that is the most sensitive direction. Nuisance alarms could be caused by atmospheric conditions, blowing debris and animals. The passive infrared detector is most sensitive when the background is at a significant different temperature than an intruder. Detection ranges can exceed 100 m. Because these are optical devices, the only way to limit the maximum range is to aim the detector at a solid object, such as the ground, at the end of the desired detection zone as shown in Fig. 7. Detection may also be reduced during periods of heavy rain.

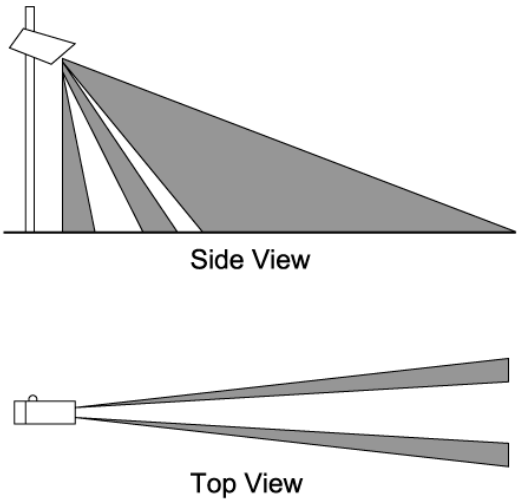

FIG. 7. Passive infrared sensor coverage.

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

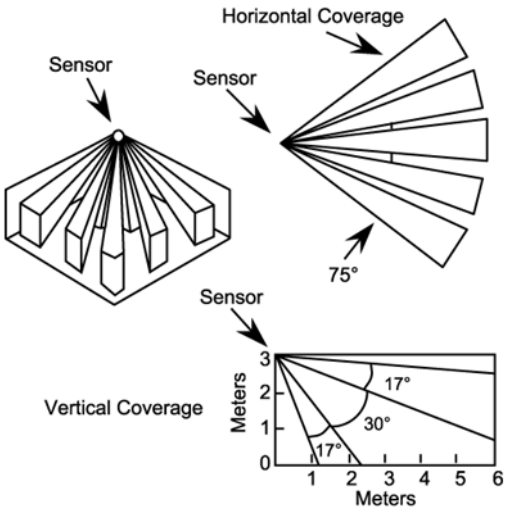

FIG. 8. Passive infrared sensor pattern.

4.94. PIR sensors are most sensitive with motion across the field of view, and least sensitive directly toward or away from the sensor. (This is the opposite of microwave sensors). Motion through the field of view will result with more segments being entered in a shorter distance. This characteristic plays an important role in determining where to mount the sensor.

4.95. To reduce nuisance alarms in exterior applications 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 imbalance. Weather changes

should affect both areas equally and would not cause an alarm. Indoor application may only use a single sensor.

4.96. Sources of nuisance alarms may include: insects crawling on the lens, other sources of infrared energy. Sunlight passing through windows can produce locally heated surfaces that can radiate energy in the relevant wave length including heat sources (e.g. radiators, heaters, hot pipes).

Electric field or capacitance

4.97. Electric field sensors are active, visible, volumetric, line or point, and can be fence associated, free standing and boundary penetration and are terrain following. Capacitance sensors are active, visible, line or point and can be fence associated, free standing and boundary penetration. They establish 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 may have a fixed frequency of oscillation or the oscillator frequency may vary.

4.98. For perimeter applications the sensitivity of some electric field sensors can be adjusted to extend up to 1 m beyond the wire or plane of wires. A high sensitivity typically has a trade-off of more nuisance alarms. Electric field and capacitance sensors may be susceptible to lightning, rain, fence motion, and small animals. Ice storms may cause substantial breakage and damage to the wires and the standoff insulators. Good electrical grounding of electric field sensors is important to reduce nuisance alarms. Other metal objects (such as the chain-link fence) in the sensor field should also be well grounded; poor or intermittent grounds will cause nuisance alarms. Because the detection volume 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.

4.99. Electric field or capacitance sensors can be mounted on their own set of posts resulting in improved performance due to a wider detection volume for the sensitive electric field sensor and a lower nuisance alarm rate by eliminating extraneous motion from the chain-link fence. For the freestanding version of electric field sensors, some electronic signal processing techniques employ additional wires in the horizontal plane to reduce the effects of distant lightning and alarms due to small animals.

4.100. This type of sensor may also be used to detect boundary penetration through existing building openings such as grills, ventilation ducts, or metal window frames and doors.

4.101. For interior applications capacitance 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 should be grounded, the object can be considered the ground plane. This requires the fabrication of a capacitance blanket for draping over the protected

object. If the blanket is made large enough to cover the object entirely, any access attempts will cause blanket movement, capacitance change, and alarm. Capacitance proximity sensors detect capacitance changes of a few Pico farads

4.102. The sensitivity of capacitance sensors can be affected by changes in relative humidity and the relocation of other metal objects closer to or away from the protected item. Changes in the relative humidity vary the dielectric characteristics which can either increase or decrease the air conductivity. If the sensor's sensitivity is adjusted to detect an intruder several metres from the object, this change in conductivity could be enough to initiate a nuisance alarm. Capacitance sensors using a self-balancing circuit adjust automatically to the change in relative humidity and relocation of metal objects close to the protected object. It is advisable that care be taken if the object is in an area of high pedestrian traffic to avoid nuisance alarms.

4.103. Sometimes objects requiring protection are located in areas with poor grounding conditions. In such places, a reference or ground plane can be established by installing a metal sheet or screen under the object to be protected. Avoid using wooden blocks to isolate the protected metal object from the ground plane. Wooden blocks might absorb enough moisture over a period of time to change the dielectric enough that the protective object is no longer isolated from ground, resulting in nuisance alarms.

Microwave

4.104. Microwave sensors are active, visible, volumetric, line-of-sight, and freestanding or interior motion. Normally, bi-static microwave sensors have two identical microwave antennas are installed at opposite ends of the detection zone. One antenna is connected to a microwave transmitter and the other is connected to a microwave receiver that detects the received microwave energy. The receiver detects a change in the received energy of the direct beam between the antennas and the microwave signals reflected from the ground surface and other objects in the transmitted beam. Microwave sensors respond to changes in the vector sum caused by objects moving in that portion of the transmitted beam that is within the viewing field of the receiver.

4.105. Some considerations when specifying microwave detection criteria include the following:

(a) The ground surface should be flat so that the object is not shadowed from the microwave beam, precluding detection.

(b) A zone of reduced detection capability exists in the first few meters in front of the antennas. Because of this, antennas should overlap, rather than being adjacent.

(c) The detection volume for bi-static microwave sensors is large compared to most other intrusion sensors. The detection cross section may reach 4 m wide and 3 m high.

4.106. Microwave sensors tolerate a relatively wide range of environmental conditions without producing nuisance alarms. However the detection zone should be kept clear from snow and vegetation. To minimize nuisance alarms from reflecting surface water (from rain or melting snow) the flat plane in detection zone should have a cross slope for water drainage.

4.107. For monostatic microwave detectors, the transmitter and receiver are in the same unit. Radio frequency energy is pulsed from the transmitter and the receiver looks for a change in the reflected energy. Motion by an intruder causes the reflected energy to change and thus causes an alarm. These sensors are 'range-gated' meaning that the nuclear facility can set the range beyond which motion can occur without an alarm. The monostatic installations are typically used in a fixed volume (e.g. hallway).

4.108. Detection is based on the microwave frequency shift between the transmitted and received signal caused by a moving object within the energy field. Microwave sensors are most sensitive with motion directly towards or away from the sensor. This is because the largest amount of microwave frequency shift is created with motion towards or away from the sensor. This needs to be kept in mind when determining a location for the sensor. It is advisable that the sensor be located so that an intruder's movement in the direction of protected items from likely points of entry will have a considerable vector of movement towards the sensor. The shape of the detection zone is governed by the design of the antenna as shown in Fig. 9.

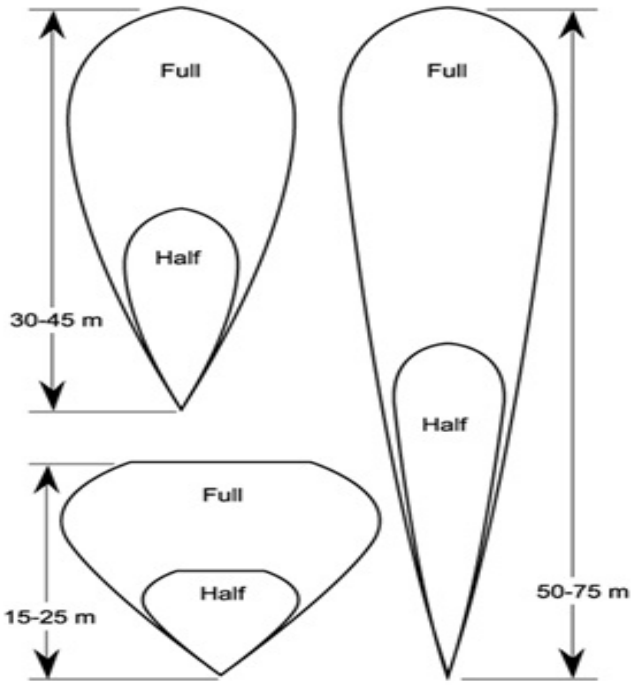

FIG. 9. Typical microwave detection patterns.

4.109. Range gating is used to limit the distance of effective detection and is desirable 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. Microwave energy will readily penetrate most glass, as well as plaster, gypsum, plywood, and many other materials used in normal wall construction. Such penetration can cause unwanted interference with effective sensor operation. Metal objects, such as large bookcases or desks and screens or fencing within the protected area, will cause shadow zones and incomplete coverage.

4.110. For interior applications, it is advisable that microwave detectors be mounted high, near the ceiling of the area being protected and aimed in the direction of desired coverage, yet pointed away from metal objects that might reflect microwave energy and cause nuisance alarms.

Video motion

4.111. Video motion detectors are passive, covert, volumetric, line, point, line-of-sight, and free standing or interior volumetric. These sensors process the video signal from closed-circuit television (CCTV) cameras. These cameras are used in both interior and exterior location. They are generally installed on towers, ceilings or walls to view the scene of interest and may be jointly used for detection, surveillance, and alarm assessment. Lighting may be required for continuous 24-hour operation.

4.112. Video motion detectors with video analytics capability can be added to either analogue or digital camera systems and can be effective using daylight cameras, near-infrared cameras, thermal imagers and 360 degree-view cameras. It requires the addition of hardware modules and/or video alarm processing hardware and software. The technology is modular so that it can be implemented at either the camera or at the CAS.

4.113. Video motion detectors 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. The probability of sensing may be reduced during conditions of reduced visibility, such as fog, snow, and heavy rain.

4.114. Video motion detector systems have a higher probability of sensing for motion across the field of view rather than towards/away from the camera. It is advisable that the scene background be a neutral colour rather than a very light or very dark colour. A scene with a very light or very dark background colour makes it easier for an intruder to blend in with the background.

4.115. Potential sources of nuisance alarms for video motion detectors used outdoors include: apparent scene motion due to unstable camera mounts, changes in scene illumination caused by such things as cloud shadows, shiny reflectors, and vehicle headlights, and moving objects in the scene

such as birds and other wildlife, blowing debris, and precipitation on or near the camera. Preventive maintenance is essential especially in terms of clear optics to reduce nuisance alarms.

Vibration

4.116. Vibration sensors are passive, visible, line that can be buried line, fence associated and boundary penetration. This type of sensor includes glass break. They detect the movement of the surface to which they are fastened. An impact on a surface will cause that surface to vibrate at a specific frequency determined by its construction. The vibration frequencies are determined to a lesser extent by the impacting tool. 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 air-conditioning or heating equipment noise.

4.117. When applying vibration sensors, the designer should be aware that the detector might generate nuisance alarms if mounted on the walls or structures that are exposed to external vibrations. If the structures are subject to severe vibrations caused by external sources such as rotating machinery, the use of vibration sensors not advisable. However, if the structures are subject to occasional impacts, vibration sensors with a pulse accumulator or count circuit might be effective.

Electromechanical

4.118. Electromechanical sensors are active or passive, visible, line or point, and boundary penetration and object. The most common type is a relatively simple switch generally used to detect the opening of doors and windows. These sensors are only adequate if the intruder opens the door or window for entry. Most of these switches are the magnetic switches, which consist of two units: a switch unit and a magnetic unit. Fig. 10 shows the magnetic reed switch and its components in the closed and open positions.

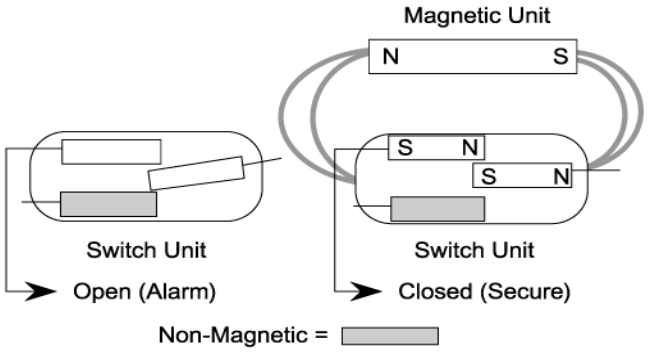

FIG. 10. Magnetic reed switch principle.

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. With the door or window closed, the spacing between the switch unit and 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 of the door or window (removal of the magnet) results in the decrease of the magnet 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. Those with bias magnets are generally referred to as balanced magnetic switches. Other variations include multiple reed switches and multiple magnets; fusing and voltage breakdown sensing devices; and shielded case construction. Some units incorporate internal electro-magnets, which have very complex interactions with the movable magnets, increasing the complexity of the unit and decreasing its vulnerability to defeat. Features are available on some models to make them self-testing.

4.121. A Hall effect switch is electronic without mechanical-type reed switches. It contains active electronics and requires power. It is intended to provide a higher level of security than the balanced magnetic switches. Similar to other magnetic switches, it consists of a switch unit and a magnetic unit. Operation of the switch is based on Hall effect devices in the switch unit measuring and monitoring the magnetic field strength of the magnetic unit. If significant enough magnetic field changes occur, an alarm condition is generated. Both the balanced magnetic switches and Hall effect sensors provide better protection against insider tampering and defeat than does the simple magnetic switch.

Thermal imaging

4.122. Thermal imaging sensors are passive, covert, volumetric, line-of-sight, and free standing or interior motion. Thermal imaging cameras allow detection, recognition and identification of different types of threat under unfavourable meteorological conditions and/or lack of light at different distances.

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

TABLE 1. SENSOR TYPES AND TYPICAL APPLICATIONS

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

[a] P (passive) and/or A (active).

[b] V (volume), L (line) and/or P (point).

[c] BL (buried line), FA (fence associated), F (freestanding), BP (boundary penetration), IM (interior motion) and/or O (object).

Alarm Assessment

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

(a) Determining the cause of each sensor alarm;

(b) Deciding if the alarm is caused by a threat or is a nuisance alarm (e.g. due to environmental events or false alarms); and

(c) Providing information about the threat such as who, what, where, when and how many (if the alarm is confirmed as a threat).

4.125. Alarms may be assessed by using video technologies or response personnel. Both assessment methods require adequate lighting and appropriate lines of sight. Use of video assessment can minimize the assessment time and improve overall response time.

4.126. The use of video assessment typically includes technology that allows prerecording, instant replay, stop action, and ergonomic human-machine-interface enabled real-time assessment.

4.127. Assessment by personnel can be accomplished by using guards, response forces, or other personnel depending on the facility security concept. Assessment by personnel may be needed if the video alarm assessment system is not operable (maintenance, weather); the video alarm assessment is not adequate for a particular situation, or in the absence of such a system. However, the assessment by a person will rely on deploying that person to the right location. The probability of a correct assessment by personnel decreases as the time to arrive at the assessment location increases.

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

4.129. Alarm assessment is dependent upon properly trained personnel; people assisted by adequate video, lighting and communications capabilities.

Video technology

4.130. Video technology applications include alarm assessment, intrusion detection, access control, detection of prohibited items, situational awareness, and post event video. Examples of video applications include:

(a) Alarm assessment to provide guards and responders with the ability to timely and accurately determine the threat to the facility. This enables the initiation of an appropriate response.

(b) Intrusion detection to provide both video motion detection and surveillance capability.

(c) Access control of personnel or vehicle identification. Special face recognition software could be used to support the identification process. Video technologies could also support remote operation of security equipment (gates or vehicle stopping equipment)

(d) Detection of prohibited items. Examples include: under vehicle surveillance equipment and endoscope inspection cameras.

(e) Situational awareness to provide information to the response forces regarding adversary actions and locations during an attack.

(f) Post-event video used after the event to support investigations and criminal prosecution.

4.131. To support these applications, the selection of the correct degree of video resolution should be determined. Resolution is the degree to which one can see the fine detail in a viewed image and is dependent on the correct selection of all video system components (lens, camera, transition system, recording equipment and monitor) to determine the level of resolution of a system. The amount of

resolution required is determined by the level of assessment needed at a particular camera location. Three levels of resolution to consider are detection, classification and identification.

4.132. Commercially available security video systems may offer resolutions (image point/meter) as low as 10 pixel/m, but this normally not sufficient for physical protection purposes. To detect the presence of an object in an area of interest, a resolution of 25 pixel/m is necessary. An increased resolution of about 125 pixel/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 require an improved resolution of about 250 pixel/m to be sufficient to uniquely identify an object on the basis of details of appearance. This resolution equals 40 Pixel/16cm, which is close to the size of a human face.

Cameras

4.133. 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 a remote display area. Most cameras are solid-state and have a variety of features to optimize the image produced by the camera. The camera format and the resolution are specifications provided by the manufacturer.

4.134. Cameras should normally be mounted using 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; a camera used for surveillance may be mounted at a considerable elevation to allow an extended view. Camera installation considerations include the field of view, accessibility for maintenance (collapsible tower), and protection from both insider and external threats. One example for the protection of cameras from both insider and external threats is to place them between in the inner and outer perimeter fences to restrict access to authorized maintenance personnel entering the detection zone.

4.135. Using the lens iris control, exposure time, and electronic signal amplification, most cameras average the total scene brightness detected by the imager. As a result, there is a limit to the amount and intensity of bright areas and dark areas in the camera's field of view for which the camera can compensate. This is known as the camera's dynamic range. Bright spots in the camera's field of view raise the average imager illumination level, causing the camera electronics to compensate by lowering the average video signal output. This tends to cause the darker portions of the image to become too dark and will negatively impact an operator's ability to assess the scene.

4.136. Under low-light conditions, most cameras automatically compensate for the lack of illumination by increasing some combination of both the exposure time (shutter control) and amplifier gain depending on the overall brightness level desired by the user. Cameras with auto-iris lenses compensate for changing scene light levels by opening or closing the lens iris. The mechanics of

illumination level compensation for some digital cameras can be programmed. The sequence of iris control, shutter control, and amplifier gain can be prioritized as to the order in which they are used to control imager illumination.

4.137. Using shutter control for low-light compensation causes the shutter to be open for longer exposure times. Long exposure times will blur moving objects while higher amplifier gain on very low-light signals will produce grainier images. Both of these outcomes are undesirable for purposes of alarm video assessment. Camera manufacturers often state camera sensitivity using different test conditions and camera parameter settings. Often, camera sensitivity is stated in terms of minimum illumination level at the camera's imager to provide a usable picture. These camera specifications do not account for the illumination level degradation caused by the camera lens. While the amount of light needed at the camera's imager to produce a usable picture is specified, the amount of light that needs to enter the lens to achieve that light level at the imager may be significantly higher. Also, illumination and scene conditions during which the camera's sensitivity is determined may not necessarily be documented in the camera's specifications. Along with minimum light level, it is important to have the following information:

(a) Condition of output video, i.e., camera output and/or gain and exposure time;

(b) Lens transmittance – the percentage of incident light appearing at the front of the lens that passes through on to the imager;

(c) Lens f-stop – the level of light reduction to the imager determined by the lens iris (or aperture) opening; and

(d) Test scene reflectance – the percentage of incident light on a scene that is reflected back to its source.

4.138. In some cases, the parameters used to claim sensitivity may be unrealistically assumed to indicate a better performance than will be experienced in actual installations. For example, three of the favoured parameters for specification enhancement are higher scene reflectance than normally encountered, unacceptably long exposure times, and a large lens aperture (low f-stop). These parameters are usually determined with the camera viewing a static scene. If the need to effectively observe motion is factored into the specification process, the actual camera sensitivity experienced would most likely be less than (i.e., not as good as) that stated on manufacturer's data sheets.

4.139. Camera imagers are sensitive to a portion of the electromagnetic spectrum. If the output spectrum (colour) of the illumination source and the camera imager spectral response are not compatible, either more light will be required to provide adequate illumination or a different light source will be needed. The physical differences between the imagers will impact the low-light performance (sensitivity) of the camera as a whole, typically by a factor of two.

4.140. It is very important that the camera imager is sensitive to the colour of light produced by the lighting source. Less illumination is required for a black and white camera compared with a colour camera to produce the same level of video output. If a near-infrared energy source is used, a black-and-white camera provides a visible video image even if the near-infrared light was not visible to the human eye.

4.141. When using video systems for alarm assessment it is advisable to consider the use of more than one camera to assess a single alarm. For example if one perimeter sensor covers a long distance, the automatic display of multiple cameras may prove to be beneficial. In addition, factors affecting the operability of the camera should be considered and addressed. As an example, in severe cold climates, a mechanism to heat the camera housing to maintain minimum temperatures may be required. Another example is using methods to address snow and ice build-up that may affect camera performance.

4.142. Some video alarm assessment system designs seek to reduce the number of cameras used by employing pan tilt mounts and zoom lenses (the combination of these mounts and lenses are often referred as pan–tilt–zoom cameras). These cameras can be redirected to view the area where an alarm occurred often within a second or less. Older systems had to be manually controlled while newer pan–tilt–zoom systems can be programmed with pre-sets that cause the camera to automatically slew to the alarm scene as soon as the alarm is received. With this approach, as many as four or five alarm zones can be covered by one camera.

4.143. However there are some significant disadvantages associated with the use of this approach. One of the main disadvantages of the use of pan–tilt–zoom cameras is in the case of multiple simultaneous alarms within the zones covered by the single camera. The system will not allow recording of all of these scenes and, without prioritization, there will be some question as to which alarm the camera will rotate to view. The use of pan–tilt–zoom cameras precludes the use of pre-alarm recording, since the camera will unlikely be aimed at the source of an alarm prior to the alarm occurring. Also, the mechanical pan-tilt mount may require more frequent repairs.

4.144. Compared to a fixed camera, it may not be advisable to use pan–tilt–zoom cameras for immediate detection assessment but they could be useful for post alarm monitoring for surveillance of an event or area. They are also useful when tracking an adversary beyond the alarm location.

4.145. Thermal imaging cameras may also be used as part of a CCTV. These cameras allow detection, recognition and identification of different types of threat under unfavourable meteorological conditions and/or lack of light at different distances.

Lenses

4.146. Lens selection parameters (format, focal length, field of view and f-number) are interdependent variables and vary with the designer's objectives, including the manner in which the video system will interface with other security systems.

4.147. Lenses may have other features that can enhance the performance of the lens. Some lenses have automatic iris aperture controls that work with the camera circuitry to allow for automatic adjustment of the light levels, including neutral density filters in the centre of the lens. This allows for a greater magnitude reduction of bright light when the iris aperture is smaller than the neutral density spot. Some lenses have special coatings to enhance or filter certain wavelengths of light energy to optimize the lens performance. For example some lenses have broader bandwidth transmissions to enhance the transmission of near IR (from 800nm to 1100nm), which is usable to solid state cameras not equipped with IR cut filters.

4.148. Lens selection depends on the required resolution and field of view required. 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 may be assessed with a particular camera and lens combination. Fig. 11 shows a typical perimeter configuration. Note that the lower field of view (bottom of scene on TV monitor) is not normally the zone width. Likewise, the upper field of view is not normally the resolution-limited field of view width. Also note that between the camera location and lower field of view, there is a blind area that cannot be seen by the camera.

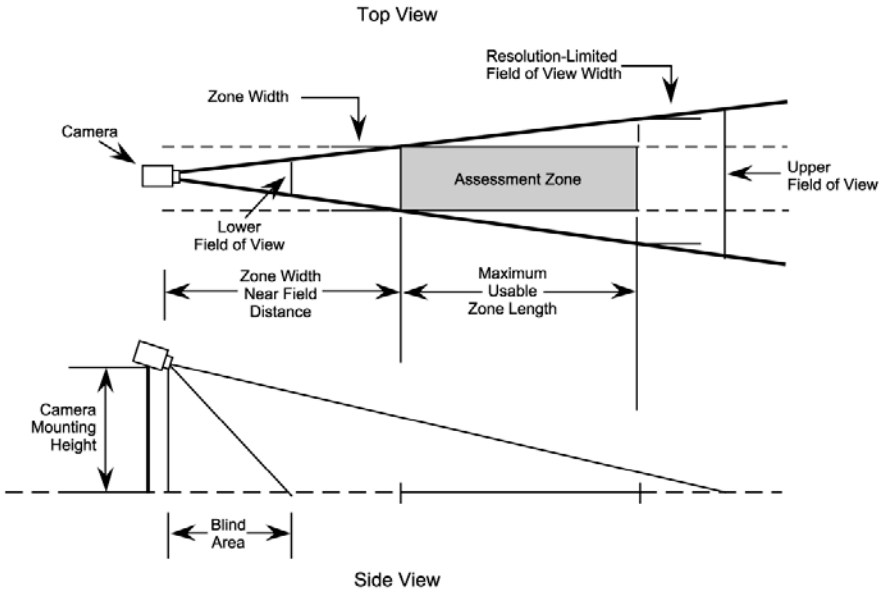

FIG. 11. Perimeter assessment zone geometry.

Video transmission system

4.149. The function of a video transmission system is to connect cameras to the CAS video displays with no undesirable effects introduced to the video signal. A typical system comprises cameras, transmission systems, processing equipment and storage and display components. For the majority of applications a lighting system will be required. Video systems consist of analogue, digital systems or a combination of the two systems.

4.150. Video transmission using multiple cameras may be accomplished in several ways, for example:

(a) Coaxial cable transmission (analogue).

(b) Fibre optics (digital and analogue).

(c) Microwave links, optical (infrared), or other wireless systems (digital or analogue).

(d) Network connection (digital).

4.151. Fig. 12 shows an analogue system, where the display should have a bandwidth of at least that of the cameras being used in the assessment system. For digital systems, the display should be capable of displaying the required resolution.

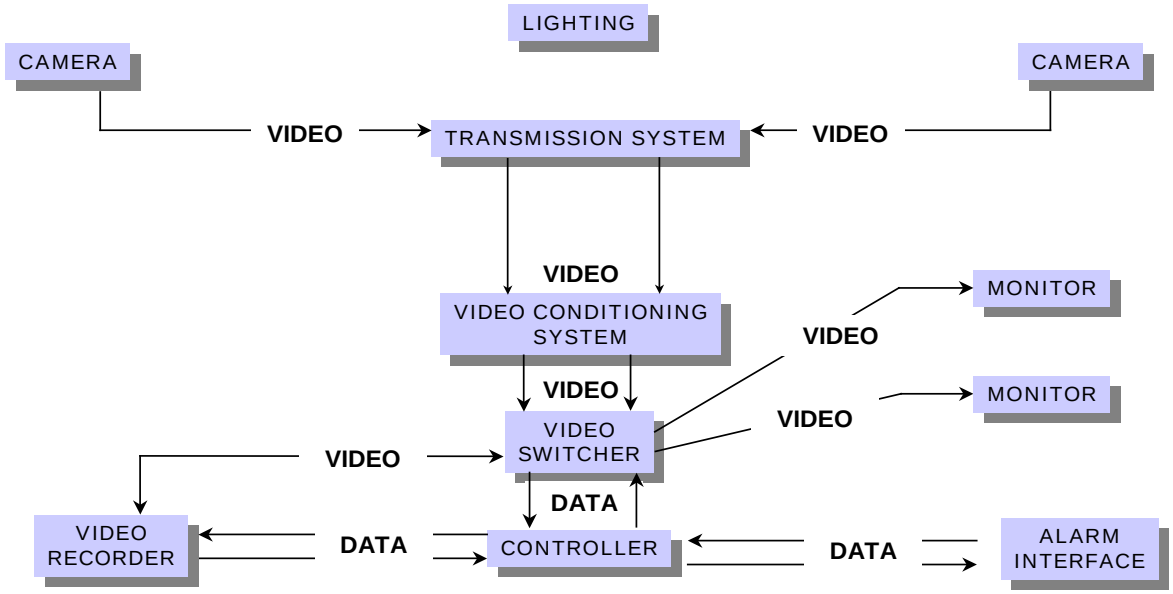

FIG. 12 Analogue components of a video system.

4.152. A digital system is typically set up using IP addressable components (cameras, storage devices and displays) on a network. System designers need to ensure adequate picture quality, availability and reliability of the system before deciding on a digital or analogue system. Security considerations for video transmission networks are addressed in Section 7.

4.153. Digital transmission can occur at a range of transmission rates at full resolution but at slower frame rates. Digital compression of images allows for reduction of the bandwidth required to transmit the image, but the many different compression techniques can also involve reduction of image resolution or quality.

4.154. Hardwire transmission uses either copper or fibre optic cables. Fibre optics uses an optical path rather than an electrical path for transmission. The use of copper cables (e.g. coaxial) may lead to some degradation of the signal therefore conditioning of the signal maybe required. In comparison, fibre optic cables have less signal loss but may require additional analogue/digital conversion.

4.155. Ground loops, induced noise, and surges from lightning that can damage equipment do not occur with fibre optics. Fibre optic transmission does not require signal conditioning with equalizers, isolation transformers, or clampers, but may need repeaters to provide enough signal strength on very long cable distances.

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

4.157. Types of switching system include:

(a) Manual switching performed by push-button contacts and the video signal is routed through the switcher with no electronic conditioning or timing.

(b) Sequential switching where all camera outputs are sequentially scanned, usually with an adjustable the scan rate or amount of time each image is displayed.

(c) Alarm-activated switching where the alarm sector camera information is automatically presented to the output regardless of the selected input before alarm activation.

(d) Remote switching involves multiple switching with some of the switching executed remotely and done prior to entering the signals into the central alarm station.

4.158. 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 into a single line.

Video recording

4.159. Video management systems provide historical (audit trail) information for subsequent study and instant replay/stop action to aid a real-time assessment. Video recording systems consist of either analogue (videotape) or digital video recorders.

4.160. An advantage of digital recordings is that it may be used for real time assessment purposes. The number of cameras, the number of frames of video that is recorded per second (typically ranging from 2 to 30 frames per second) for each individual camera and the resolution of those images as well as the required storage time determine the necessary storage space. The amount of data that is recorded is a balance between the requirements of the video system and the existing storage limitation (e.g. a high overall video quality supports live playback for real time assessment, a high resolution in the stored data may help to determine the identity of an intruder, a high frame rate may help assess the action of an insider). Video management systems compress video data for storage and allow for an automatic adjustment of the quality for stored video data during alarm situations (high frame rates and resolution) and video data during normal situations (low frame rates and resolution).

4.161. Digital video recorders can be controlled by an alarm control and display computer to be interactive with the sensor alarm monitoring portion of a security system. Upon sensor alarm notification, the digital video recorder can be directed to playback pre- and post-alarm video from the camera assessing the area covered by the alarming sensor.

4.162. The size of the video files stored on the hard drives can be reduced by increasing the degree to which each captured image is compressed. A good camera may provide a high resolution image but the captured image may be compressed to save storage space. To view a recorded, compressed image, the image is decompressed, but when viewing the decompressed image, fine detail in image detail can suffer. Overall image quality is a function of camera resolution, captured image resolution and the amount of compression applied to the original digital image.

4.163. Video displays should be installed to allow effective, rapid assessment without interference from other system controls and outputs, using human factors engineering considerations of function and frequency of use.

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

Lighting technology

4.165. Adequate security lighting is required for areas or structures that form the perimeter of nuclear facility where intrusion detection systems are used and assessment is required. Lighting may also be used to support assessment of alarms in areas such as vital areas, nuclear material storage areas, inner areas, and other important areas, such as where utilities or critical infrastructure for physical protection are located.

4.166. Security lighting provides illumination for:

(a) CCTV (including video motion sensors) for detection, assessment, and surveillance of intruders;

(b) Deterrence of a potential adversary action;

(c) Areas of concealment (e.g. unnecessary dark patches);

(d) Access control points (e.g. personnel and vehicle identification, detection of prohibited items); and

(e) Support of guard and response force activities.

4.167. Security lighting also enhances personal protection of guards and response force personnel by reducing the possibilities of concealment by an intruder. When security lighting is poor, additional security posts, patrols, night vision devices, or other provisions may be necessary.

4.168. Contrast between an intruder and the background is also an important consideration when planning a security lighting system. For example using light colours on the lower parts of buildings and structures or light colour surface on the ground may expose an intruder wearing dark clothing.

4.169. It is essential that any proposed lighting solution is planned in conjunction with other security systems including CCTV and intrusion detection systems. The use of security lighting can also impact operational or conventional health and safety requirements. These interactions will need to be understood as different priorities may be an issue. Provisions should be made to ensure lighting failures are reported and corrected in a timely manner.

4.170. In some instances, if a facility is using thermal imaging cameras as the means for providing alarm assessment at night, illumination may not be required if only used to support camera assessment.

4.171. If local laws require that a facility reduce power consumption or use lower light levels for environmental reasons, the use of low-light cameras or covert infrared illuminators or motion activated lighting systems are other options to consider. Light emitting diodes systems are another option that can be used to reduce power consumption.

Types of lighting system

4.172. The type of lighting system implemented depends on the installation's overall security requirements. Four types of lighting approaches can be used for security lighting: continuous, standby, movable (portable), and emergency.

4.173. Continuous lighting is the most common type of security lighting used. It consists of a series of fixed lights arranged to continuously illuminate a given area during low light conditions with

overlapping cones of light. Standby lighting has a layout similar to continuous lighting. However, the luminaries are not continuously energized during night-time hours but are either automatically or manually turned on when suspicious activity is detected or suspected by the intrusion sensor system or guards. The use of standby lighting needs to be carefully managed and can have unforeseen consequences (e.g. warning the adversary that he has been detected). Movable lighting consists of manually operated, movable integrated groups of light fixtures and generator assemblies that may be operated during hours of darkness or as needed. This type of system is normally used to supplement continuous or standby lighting or as a compensatory measure. Emergency lighting is a system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source such as installed or portable generators and its battery powered uninterruptable power supply.

Illumination

4.174. Illumination (lux units) is either natural or artificial. The human eye, when adjusted to low light levels and with good contrast between the subject and the background, can detect an intruder at a light level of approximately 1 lux. Considerably more illumination is needed to recognize the individual. Adjusting the human eye to low light levels can take between about 5 and 20 minutes depending on a person's age. For this reason the time taken to adjust to working in a low light environment needs to be understood when planning a guard patrol strategy.

4.175. To ensure that a sufficient amount of natural illumination during low light conditions is reflected back to the camera and that sufficient scene contrast exists for intruder detection. It is advisable that the ground surface of the assessment area has adequate reflection.

4.176. Assessment zone illumination and reflection are typically measured using a light meter at a specified distance. Normally, measurements are made at a 15 or 30 cm distance above the ground. An area's average illumination is determined by taking several measurements at equally spaced locations in an illuminated zone. Several measurements can be taken within a zone covered by a number of lamps and then averaged together. These are measurements of 'horizontal scene illumination' or simply scene illumination.

4.177. Average scene illumination is the average amount of light illuminating an area. The average scene illumination should be high enough to achieve adequate video assessment as well as visual assessment by guards and response. For example, an average scene illumination of 10 lux onto a ground cover surface with 25-35% reflectivity may provide sufficient light for assessment purposes in clear environments.

4.178. The light-to-dark ratio within an area influences the ability to assess the scene. Fig. 13 has a light-to-dark ratio of approximately 20:1 showing significant blind spots. These are greatly reduced in

Fig. 14 which has a light-to-dark ratio of approximately 4:1. Tests have shown that lighting designs with at least a 6:1 light-to-dark ratio provide sufficient illumination contrast for assessment purposes. Is it advisable that at least 75% of the camera's field of view have even illumination that meets the minimum average illumination and light-to-dark ratio requirements.

FIG. 13. Scene with a high light to dark ratio of approximately 20:1.

FIG. 14. Scene with a low light to dark ratio of approximately 4:1.

4.179. Since most lighting applications are associated with bulbs that produce visible light, errors can be made in estimating the light required if the camera imager spectrum is not considered.

Lighting layout

4.180. To prevent cameras from looking directly into a light source, all light fixtures need to be located above the camera and out of the camera's field of view. See Fig. 15. It is advisable that the light source not be mounted directly above the camera to mitigate the potential effects of dust and fog induced backscatter. However, the use of a sunshield that extends beyond the front cover glass of a camera enclosure like the brim of a hat can also minimize those effects. The location of perimeter light poles should be on the inside of the perimeter so they cannot be used by an adversary as a means to bridge over the perimeter.

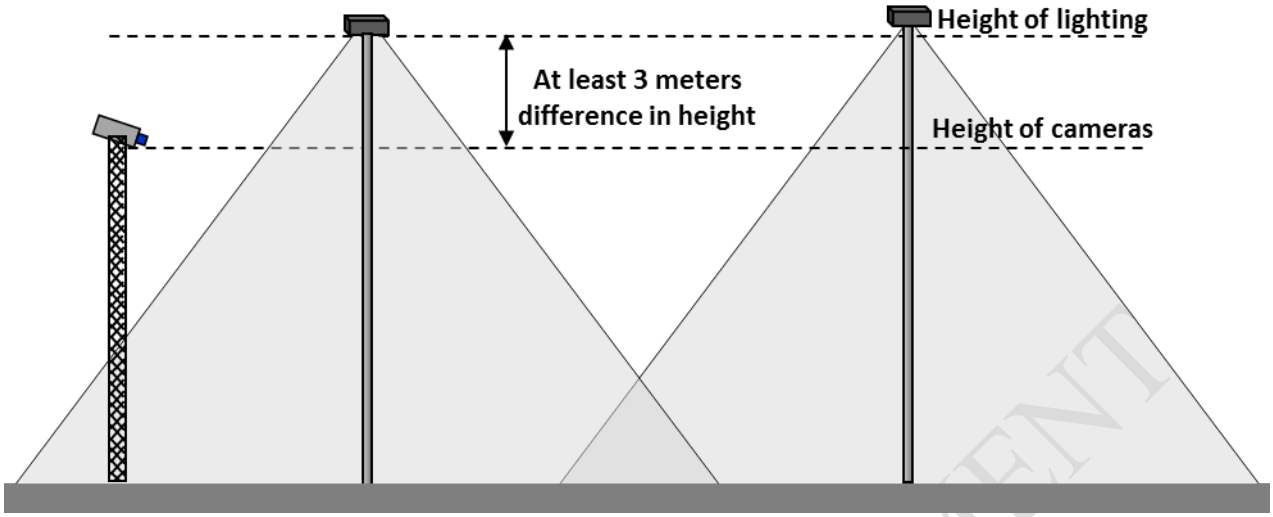

FIG. 15. Suggested height difference between exteriors lighting and cameras.

4.181. Modelling of a proposed lighting system can be used to estimate scene illumination levels and light-to-dark ratio. It is advisable to physically test the lighting design prior to installation in the final perimeter lighting configuration. This is accomplished by installing a minimum of five fixtures (for single row installations) and actually measuring the illumination based on the suggested criteria discussed above.

4.182. Adjustment and modification of the total lighting system after installation should be anticipated. It is not uncommon to discover during camera testing that there are unidentified reflections or bright spots that should be corrected.

4.183. Similar lighting layout should be considered for interior applications. Normal interior lighting levels allow the use of a video camera with less sensitivity than is required for exterior video assessment applications. The internal use of near-infrared illumination sources may provide a measure of covertness for the video assessment.

Lighting requirements

4.184. Perimeter lighting involves specific requirements based on whether the perimeter is isolated, semi-isolated, or non-isolated. Lighting could be controlled to keep guard patrol routes in relative darkness while illuminating the clear zone or area under surveillance. The State or operator's safety requirements should be considered when guard patrols are conducted in areas with low light levels.

4.185. Access control points have different lighting requirements. Pedestrian access control points need to have sufficient lighting to enable recognition and examination of credentials. The requirements may differ for access points using automated access control systems. Vehicle entrances may need additional lighting to facilitate searching the vehicles and identifying the occupants. Semi-active and inactive entrances may have the same lighting levels as the surrounding perimeter with the

option of increasing the light levels as required. Guard posts at access control points will need to control the interior illumination levels to enable the occupants to see approaching vehicles and pedestrians whilst minimizing the ability to see into the building.

4.186. Other areas and structures within the nuclear facility perimeter may consist of areas requiring lighting, such as yards; storage spaces; large, open working areas; piers; docks; and other sensitive areas and structures and have their own lighting requirements. Open yards (unoccupied land only) and outdoor storage spaces (such as material storage areas, railroad sidings and parking areas) should normally be illuminated to provide guards on patrol adequate lighting to assess the area. It is advisable for an open yard adjacent to a perimeter be illuminated according to the perimeter's illumination requirements. Lighting should normally be used in outdoor storage spaces to provide an adequate distribution of light in aisles, passageways, and recesses to eliminate shadowed areas where persons may hide.

4.187. Illumination is needed for water approaches, piers and docks of a facility. Search lights may be used to illuminate an area of interest or for specific reasons as needed. The lighting should not in any way violate marine rules and regulations (e.g.: it should not be glaring to pilots).

Lamp types and characteristics

4.188. The characteristics of the assessment system and other security lighting will impact the choice of lamp types (e.g. if infrared based assessment equipment is specified, appropriate lighting is needed). More common lamp types used for security purposes include:

(a) Incandescent: Light is emitted from a heated filament inside an evacuated globe.

(b) Fluorescent lamp: Light is generated by an electric arc in a tube filled with mercury vapour. The low-pressure vapour emits ultraviolet radiation that is converted to visible light by fluorescent powders on the inner surface of the tube.

(c) High intensity discharge lamp: The light energy is generated by direct interaction of an arc with the gas to produce visible light. High intensity discharge lamps include mercury vapour lamps, metal halide lamps, and high- and low-pressure sodium vapour lamps. Argon is normally added to aid starting and powders or vapours may be added to improve colour rendition.

(d) Light emitting diode (LED): The light energy is generated based on the LED, solid-state technology. Lamps are usually constructed in cluster LEDs within a suitable housing.

(e) Near-infrared: The light energy is generated from either light emitting diode arrays or incandescent bulbs with external filters to remove the visible light.

Alarm stations

4.189. The function of a CAS (or an alarm monitoring station when a CAS is not required) is to provide continuous monitoring of alarms, assessment of alarms when CCTV is used for assessment, use of CCTV for surveillance purposes, and to communicate with guards, facility operations personnel, and response forces. For purposes of this document, the term CAS is used throughout, though it is not recommended for all nuclear facilities in Ref. [1] (i.e., Category III or nuclear facilities below the potential for high radiological consequences). In some cases, CAS personnel operate remote access control equipment. In addition, and important function of a CAS is to maintain records used for a number of purposes, including investigation of incidents. A CAS should be located in the protected area, permanently staffed and its access should be controlled. Guidance on the role of the CAS is given in [2].

4.190. A CAS should be designed and operated in a manner similar to a nuclear reactor control room. Although less technical in nature, the same principles apply. A range of publications and national standards exist which provide guidance on designing an alarm monitoring stations. Though developed for alarm management systems used in the process industry, guidance documents such as ANSI/ISA-18.2 [23] contain useful principles that may be considered when designing a CAS for a nuclear facility.

4.191. The CAS should have 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. In order for the CAS to perform its role effectively:

(a) All sensors installed in the facility should transmit their signal directly to the CAS

(b) All CCTV assessment and surveillance systems should be integrated into the CAS and appropriate managed.

(c) Where alarms are not monitored by CAS operators, 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 staff.

(d) Facility personnel should have the ability to provide the CAS information about incidents including unauthorized access, introduction of prohibited items, the activation of safety alarms, such as radiation detection alarms or any other suspicious incident or activity.

Monitoring of alarms

4.192. The primary tasks of personnel in a CAS include monitoring alarms from sensors, assessing as appropriate, and initiating an appropriate response. All CAS operator duties should be performed in compliance with approved procedures. Fig. 16 shows an example of a CAS layout.

FIG. 16. Example of a layout of a central alarm station workstation.

Assessment and surveillance

4.193. Alarm assessment should be performed directly by CCTV and/or indirectly by deployment of guards or response forces to assess the cause of the alarm and report to the CAS. The CAS should utilize CCTV and subsequent alarms to track (provide surveillance) the cause of the alarm. The intruder(s) path and detailed descriptions of their movement, appearances, 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. The use of video technology that includes instant replay/stop action, prerecording and an ergonomic human-machine-interface enables real-time assessment.

Communication

4.194. Communication systems between the CAS, guards, response forces, and facility management should be dedicated, redundant, secure, diverse, immediate, and reliable. CAS personnel should also effectively communicate and provide situational awareness with other organizations such as emergency responders, staff, and PPS maintenance personnel. CAS communication initiates a response and provides information to personnel assigned command and control functions during a response to malicious acts.

Access control

4.195. An access control system monitors and controls the movement of people around a facility and can complement other systems. For example occupancy accountability systems, emergency evacuation, radiation protection programmes and vehicle identification.

4.196. Access control is a system that may be integrated into the CAS as either part of a security network or a used as an independent, standalone system. In either case, the protection of any networked system should be considered.

4.197. Access control systems collect and store data regarding authorized access through an access control point and unsuccessful access attempts. It can also be configured to displayed access requests or provide automated control functions. The intrusion detection system should be integrated with the access control system so authorized access does not generate nuisance alarms. As an example, a door with an access control system and an alarm should be configured so the alarm is not displayed when the access control system provides authorized access through the door.

4.198. Some access control systems are configured to allow a person to remotely verify whether a person is allowed access into an area and grant access. In these systems, when an operator is required to confirm the identity of a person before access is allowed, the access control system may display a stored copy of the individuals photograph as well as CCTV images of the relevant area. The operator can then make a determination to allow or deny entry, for instance by remotely releasing the final lock on the door.

Record keeping

4.199. All access control activities, alarms and video assessment events should be recorded and archived for future review. Interconnected security systems (alarms, camera and recording systems) need to have a time stamp feature so that all elements of the system use the same time reference.

4.200. 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 security purposes, but also to safety management. Access control records may be used to check that all individuals who were in a building are safe following an emergency evacuation.

4.201. 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. Alarm and video assessment logs/records are also useful for investigations following nuclear security and emergency events. Additionally, written and automated operator records and logs can be examined to verify that alarm tests are performed at the required frequency and that compensatory measures were initiated as required. Information acquired at the CAS should be stored in a secure manner.

Human interface

4.202. The CAS should be permanently staffed by personnel whose trustworthiness has been verified and who are authorized, appropriate skilled and knowledgeable to undertake the assigned tasks. The work as CAS operator demands certain personal attributes and therefor a proper selection of staff is

important. A two-person rule may be implemented in the CAS to reduce the insider threat. For certain CAS functions, such as putting a sensor into access mode (non-secure) or remotely opening a high security door, the two-person rule can be required.

4.203. An effective CAS should be staffed with the adequately number of operators to monitor and assess alarms, initiate a response, and to receive and assess information coming in from other sources. During a security incident, CAS operators should have the capability of communicating details of the incident to the facility management and advising on any response required by facility personnel.

4.204. Candidates for operator positions should be well-versed in security technologies and go through extensive training and be tested prior to being assigned as a CAS operator. Typically, the CAS operators are guards and/or response force members, as they have sound knowledge and understanding of the site, security operations, procedures and contingency plans. The functions of the CAS and its operators should be regularly exercised.

Human factors

4.205. When designing the systems within the CAS, it is essential to identify the required operator functions and the interface required to support these functions. Information to be displayed may include system status, nuclear facility layout, alarm status and video display and access control information. It is advisable to consider when to display information to the operator (always, upon alarm, upon request, or not to display such as when an alarm is associated with a door operated by an authorized person). This may alter according to the time of day.

4.206. The human decision remains the most important factor in the alarm assessment process. A large nuclear facility may have several hundred cameras and alarms to monitor. The ability for the operator to quickly and accurately initiate appropriate action depends on the ability to interpret the data provided to the operator's decision making capability. Care should be taken during the design of the CAS console to prevent overloading a CAS operator. For larger systems, multiple operator stations may be necessary to effectively monitor and maintain control of the security system. When using multiple operators, the interrelationships among the operators and equipment need careful consideration. If a single operator is assigned to the CAS, the system may be designed to monitor the state of health of the person (e.g., alert appropriate personnel if the operator is incapacitated).

4.207. The layout of hardware and software systems should be considered when establishing a CAS. The system should be designed to make the work area comfortable and easy to use for multiple operators. The operator should be able to see people, equipment, and displays; hear other operators, communications and alarm warning indicators; and manipulate computer controls and communication equipment.

Layout and design

4.208. The operator work space consists of zones of varying accessibility and visibility. All displays and controls should be given adequate space for their intended function. Primary displays should be clearly visible from the operator's normal working position requiring very little eye or head movement. The operator should be able to easily control all required functions rapidly and adequately. Consider the use of techniques such as variable letter sizes, shaded backgrounds (contrast) and colour to improve the visual presentation of information.

4.209. It is advisable for the designer to choose input devices (e.g. mouse, keyboard, push button) that work best for the intended function. Communication equipment, such as microphones and telephones, should also be within easy reach. The location of any support equipment should be related to its importance and frequency of use.

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

(a) Use of auditory alarms to alert the operator that an alarm has occurred. Different sounds can be used to separate classes (priority) of alarms.

(b) Using colour coding (or a flashing symbol) on the screen to emphasis and categorize information, See Fig. 17.

(c) Using separate computer monitors for graphic and text displays for different types of data

(d) Using multi-layer graphics with links between layers. For example, a map of a floor plan may indicate there is an alarm in a particular room. See Fig. 18. Selecting the link to that room would bring up a display of the room and the specific sensor in alarm. See Fig. 19.

FIG. 17. Illustration of a colour console alarm text screen.

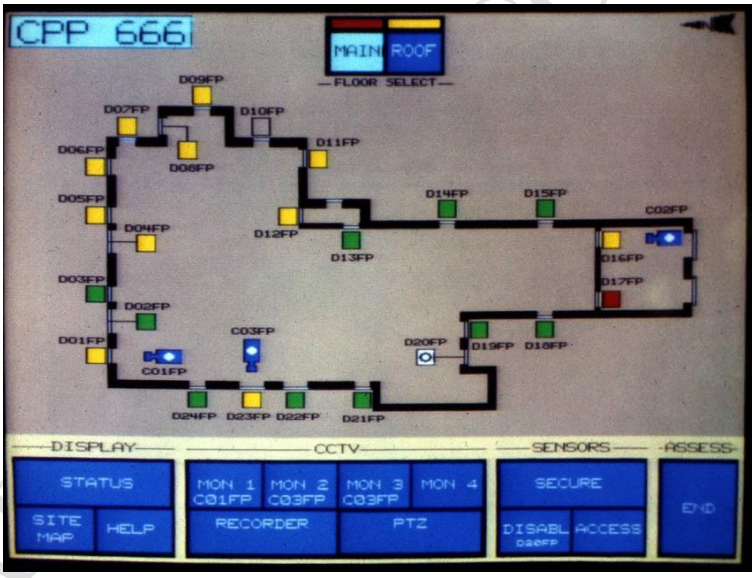

FIG. 18. Illustration of a facility floorplan map screen.

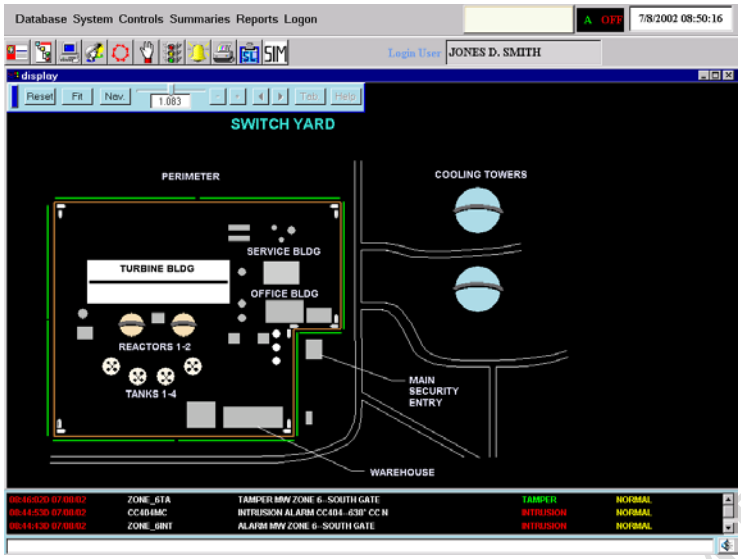

FIG. 19. Floor plan with alarm sensor detail display.

4.211. The alarm management system should be configured to prioritize, display on the visible screen, and distinguish between the location of alarm (alarm in sensitive areas prior to perimeter alarms) and the alarm purpose (intrusion, system failure, loss of line/power, unauthorized activity or tampering). This system establishes the time order of assessment for multiple simultaneous alarms and sets a priority for each alarm based on the importance of the asset being protected and the probability that an alarm event corresponds to a real intrusion. The alarms are displayed to the operator in order of decreasing priority; all alarms are eventually assessed. As an example, in a perimeter intrusion detection system, the alarm priority is established typically by taking into account the following: the number of sensors in alarm in a given sector, the time between alarms in the sector, the order in which the alarms occur in relation to the physical configuration of the sensors, and alarms in the two adjacent sectors.

4.212. The CAS should normally be located away from the perimeter boundary inside a hardened structure (e.g. bunker), away from its exterior walls to increase its protection against direct assault or stand-off attack. For category I and II and high consequence radiological facilities, the CAS should normally be located within a protected area. Access to a CAS needs to be strictly controlled. Methods of access control can include either manually controls where an operator releases the entry door upon video verification or through automated systems. To prevent unauthorized entry by following an authorized individual in to the CAS, use of two interlocking doors covered by a CCTV, with enhanced access control, may be used.

4.213. Computer security measures should apply to the CAS systems, such as controlling access to the equipment and controlling and detecting access to the information during nuclear security incidents. See also Section 7 regarding computer security.

4.214. The CAS should provide continuity of service during scheduled and unscheduled outages. Systems associated with the CAS should be redundant, diverse, and tamper-protected, if practical. If one system fails another should be designed to meet the same objective. The power supply to the CAS should be provided by two independent sources, equipped with uninterruptible power supply and when necessary a backup generator. Voice communication should also be dedicated, redundant and secure. The CAS should able to continue to function during nuclear emergencies and security incidents.

4.215. As a CAS is a potential single point of failure for a PPS, a good practice is to establish a backup station that can take over CAS functions in the event it is unable to perform its functions. This could be caused by hardware or personnel failure, an attack on the primary station, or the need to evacuate the CAS for emergency reasons (e.g., radiological release, fire, earthquake, or flood). The back-up functions should include the monitoring and control of alarms, CCTV and communications. The backup station should be geographically separated from the CAS in a location that ensures continuation of this function. The backup station should be tested regularly.

Voice communications systems

4.216. Reliable voice communication plays a key role in an effective PPS. The ability to communicate during a security incident is important. Adequate communication allows the CAS, emergency personnel, facility operations, guards and on/off response forces to communicate with each other. Some effectiveness measures for guard and response force communication are:

(a) The ability to communicate at all times, under different conditions,

(b) The ability to switch to a secure communication method when needed,

(c) The time required to communicate to authorities and/or an off-site response force, and

(d) Whether a secondary or alternate method of communication is available.

4.217. Resilient communications systems should be designed to resist compromise. A robust communications system includes multiple modes of communications such as two-way radios, mobile phones, intercoms, and land-line telephones. Many voice communication systems operate over a computer network that may use wireless technology to transmit the signals. Concerns regarding the protection of networks are discussed under PPS Network and Support Systems and Equipment Testing in Section 7.

Radio systems

4.218. One of the most common systems used for guards and response forces is a system of hand-held radios. Hand-held radios are battery-operated and operate on low power. They are easy to use,

and require minimal infrastructure other than electricity to charge the batteries periodically. A typical radio operates on any one of several frequencies or channels. A maximum range for reliable communication between two radios is 2 to 5 km depending on terrain, facility layout, and condition of the radio's battery and antenna. More powerful transmitters and better receivers, commonly called base stations, can be used at alarm stations and fixed posts. Mobile vehicle mounted systems are also used. These units can allow reliable communication to ranges in excess of 20 km. In most cases, the radio systems used throughout the world for response force communications are on a dedicated frequency using dedicated channels, narrow-band frequency modulation (FM), clear-voice radio systems. Clear voice means that no attempt has been made to encode or scramble voice transmissions.

4.219. Clear-voice radio systems also suffer from some disadvantages such as interception, deception, and the possibility of jamming. Encrypted voice radios make the system more secure and resistant to interception and to the transmission of deceptive messages. Deception is when an adversary monitors radio traffic for some period, learns some communication protocols, and attempts to send messages to confuse or divert part or all of the response force. Jamming refers to the placing of unwanted signals into the frequency channel of a communications system, thereby masking desired communications. Radio frequency systems are most vulnerable to jamming because the potential attacker can jam the channel from a remote location. Developing a communications network highly resistant to jamming can be accomplished by using higher power radios, which require higher powered jammers to block transmissions, using more sophisticated radio technologies, or use multiple communications systems. Encrypted radios by themselves do not prevent jamming. As a radio system becomes more secure and resistant to jamming, it will also become more complex, expensive, have reduced battery life, and have more noise in the communication channel, reducing its effective range.

4.220. Depending on the nuclear facility configuration, its area, and on-site building construction, radio systems can suffer from a loss of signal (signal fading), a deficiency common to radio frequency communication systems. Higher output power from hand-held units via radio frequency repeaters can minimize this deficiency. A radio frequency repeater receives voice transmissions from the hand-held units and transmits them again on a separate frequency to all other units within the system. By placing the repeater at an elevated location, the range of the radios can be increased.

4.221. The best option to ensure the ability of guards and response forces to communicate during a security incident is to use a variety of communication methods. Many of these systems may already be used for other purposes such as (land line) telephones and intercoms. Using these means of communication during security incidents creates a communication system that is robust, reliable, more secure, and increasingly resistant to eavesdropping and deception, as well as jamming. Radios may also be equipped with duress alarm features that transmit an alarm at the base station to alert the operator of a security incident involving the person operating the device.

Search systems

4.222. Upon entry into or exit from security areas, personnel and material may be subject to search using search systems, dogs, or personnel. Search system technologies include metal, radiation, X-ray and explosive detection to search personnel, packages and vehicles. Upon entry, searches are conducted to detect the introduction of prohibited articles. When exiting, vehicles, personnel, and materials are subject to search to detect unauthorized removal of nuclear material. Upon receipt of an alarm from an automated search system or a dog, guards may be required to perform a manual search to determine whether the alarm is a nuisance alarm or a valid alarm, and, if necessary, initiate a pre-planned response.

Manual searches

4.223. A manual search is a common secondary screening technique, used to search personnel, packages, and vehicles, and to resolve alarms from the technologies described above. Hand searches of people are often referred to as pat-down searches. The effectiveness of manual searches by guards relies on the adequate training and procedures. An important consideration is educating the guards on what the items being sought might look like: for example, their size, mass and shape. In principle, all items can be searched by hand, from small packages, to people, to vehicles, to large shipping containers.

Vehicle searches

4.224. Because vehicles are generally difficult to search, a facility may require vehicles to remain outside a nuclear facility. If they are allowed into a nuclear facility, the use of a vehicle lock (controlled area) to isolate a vehicle until it is searched is a good practice, see Fig. 20.

FIG. 20. Example of a vehicle access control portal.

Metal detection

4.225. Metal detectors are typically used to search personnel at entry and exit locations. The detection of metal can be divided into two broad categories:

(a) Active metal detectors transmit electromagnetic energy and detect metal by sensing the response of the transmitted field to the presence of the metal object.

(b) Magnetometers that rely on the Earth's surrounding magnetic field to detect ferromagnetic materials, which distort the local field.

4.226. While portal and hand-held metal detectors will detect metallic forms of nuclear materials and metallic shielding, some forms of nuclear materials and shielding materials cannot be detected by metal detectors. Two commonly used metal detection technologies are pulsed field and continuous wave.

Metal portal detector

4.227. In a pulsed field metal detector, low inductance transmitter coils are used to produce bursts or pulses of magnetic energy typically short in duration (as short as 50 microseconds), 200 to 400 times per second. During the time that the transmitted field is present, the received signal is ignored. Following the end of the transmitted pulse, the received signal is analysed for a short time (typically a few tens of milliseconds). When there is no metal present in the arch, the output of the receiver is only the background electromagnetic noise (which hopefully is very low). When there is a metallic object present in the arch, the collapse of the magnetic pulse induces an eddy current in the metal. This eddy current decreases rapidly (as a function of resistivity of the metal) but persists long enough to be present when the received signal is analysed. The signal is then further amplified and phase

detected. If the signal exceeds a selected threshold, an alarm is generated. Detectors based on this technique represent the large majority of portal metal detectors in use today.

4.228. For screening individuals passing through search checkpoints, several walk-through personnel portals have been developed for screening high throughput areas for metal detection on both entry and exit. On entry the primary purpose of searches are the detection of weapons and other prohibited items. On exit the purpose of searches are for the detection of radiation shielding materials that may conceal the removal of nuclear material.

4.229. Metal detector alarms should also detect power line failure, equipment failure or equipment tampering. The environment surrounding a metal portal detector can affect its performance, including:

(a) Moving metallic objects such as doors, even when more than a meter away.

(b) Static metal objects distorting the magnetic field and creating areas of high or low sensitivity.

(c) Electrical devices operated in the vicinity of a metal detector that can have adverse effects. Radios, X-ray imaging devices and computers can cause false alarms.

(d) Metal reinforcing rods in the floor.

(e) The floor that supports the metal detector, which needs to be strong enough to minimize bouncing when people walk through the area. Motion induced into the metal detector arch from floor movement may cause unwanted alarms.

(f) Pipes carrying water close to the metal detector. Most likely, the water causes the metal pipes to move within the walls or floor rather than the detector responding to the moving water.

Hand held metal detectors

4.230. The majority of hand-held metal detectors are typically based on continuous wave technology. These detectors generate a steady-state magnetic field within the frequency band of 100 Hz to 25 kHz. While early portal metal detectors were based on this technique they have been largely replaced by pulse portal metal detectors described above.

4.231. In a continuous wave metal detector, a steady-state sinusoidal signal is applied to the transmitter coil located at one side of the detector arch. This coil produces a magnetic field of low strength (typically 1/2 Gauss or less). The receiver coils are mounted on the opposite side of the arch such 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. When there is no metal present within the arch, there is no change in the signal over time.

4.232. Hand-held metal detectors need to be operated very close to the person being scanned, see Fig. 21. At the normal operational distance from the body they are highly sensitive and can be used to find much smaller objects than those that can be found by a portal detector. They may be better suited to the task of screening for metal materials that may be used to shield nuclear material during exit. The effectiveness of a hand-held metal detector is highly dependent on the technique used by the person doing the screening. A dedicated individual following a well-designed procedure can be very effective but the process will take a considerable amount of time. Because of the time it takes to use a hand-held detector properly and the short time it takes for a person to pass through a portal, hand-held detectors are mostly used to resolve portal metal detector alarms. With this important secondary role, every screening point with a portal metal detector should also be equipped with a hand-held detector. Hand-held metal detectors can also detect very small quantities of metals and may be better suited to the task of screening for nuclear materials.

FIG. 21. Hand held metal detector search.

Detection of explosives

4.233. X-ray absorption or neutron activation/absorption methods are commonly used for inspecting cargo and luggage for explosives. These methods are unacceptable for screening personnel because the ionizing radiation is harmful to humans.

4.234. Several approaches have been developed for the trace vapour detection of explosives. These passive methods of detection are trace detection (typically ion mobility spectrometry systems) and trained dogs. Smaller packages are inspected for explosives using these devices by detecting the trace amounts of vapour that are emitted from surfaces contaminated by persons who have handled explosives or where explosives have made contact. These methods are typically more appropriate for personnel search.

4.235. X-ray imaging methods use X-rays to search personnel, using low energy millimetre wave technology, or conventional X-ray technology to search packages.

X-ray absorption

4.236. Bulk explosives detection devices measure some bulk characteristics of materials to detect the presence of explosives. Some of the bulk characteristics that may be measured are the X-ray absorption coefficient, the X-ray backscatter coefficient, the dielectric constant, gamma or neutron interaction and, microwave or infrared emissions. Further analysis of these parameters can result in calculated mass, density, nitrogen content and, effective atomic number. While none of these characteristics are unique to explosives, they are sufficiently unique to indicate a high probability of the presence of explosives. The false alarm rate for bulk detection devices can be low enough to allow for automatic detection of materials that may be explosives. After the system generates an alarm, the human operator by secondary screening can investigate and determine whether or not explosives are present.

4.237. In most cases, X-ray technology bulk detectors are modified package search X-ray scanners. These devices usually serve a dual purpose. The package being searched for weapons or other prohibited items are analysed simultaneously. Simple single-energy-transmission X-ray scanners do not provide enough information to make automated explosives searches, depending on the operator's interpretation of the image; a method to extract more information is needed. Dual energy technologies allow the determination of a material's approximate mass absorption coefficient. Dual energy devices (typically around 80 and 130 keV) measure the ratio of transmitted energy at the two energies, and by comparison with known elemental attenuation coefficients, can measure an effective atomic number for the region scanned. Typically, false colours are added to the images to indicate areas of low atomic number and high atomic number materials. The coloured regions may aid personnel in interpreting the images. Computed tomography scanners can extract enough information to calculate the material's mass, density, and mass absorption coefficient. Backscatter technology can determine a material's effective atomic number by examining the amount of X-ray energy scattered back in the direction of the source (a process mainly due to Compton backscatter, most effective for hydrogen-rich materials like explosives, plastics, and food). X-ray systems to screen vehicles are available.

Neutron activation/absorption

4.238. The thermal neutron activation (TNA) detector and the pulsed fast neutron absorption (PFNA) can also be used to detect explosives. Thermal neutron devices can determine the nitrogen content of a material. Nuclear absorption of a thermal neutron generates N-15 in an excited state from N-14. The excited state is not stable and emits a gamma ray of characteristic frequency. Detection of

this gamma ray is then a measure of nitrogen content. Since most explosives are nitrogen rich, these devices can automatically detect their presence. PFNA devices can roughly measure the hydrogen, carbon, oxygen composition of the material. When combined with thermal neutron measurement of nitrogen content, a more specific identification of the material is possible. Drawbacks of PFNA systems are a high cost, its size, and the throughput. Some package search systems are based on TNA and some systems for searching vehicles and large shipping containers are based on PFNA.

Trace vapour detection

4.239. The challenge involved in detecting explosive vapours is evident when one considers the low vapour-phase concentrations of several common high explosives, see Table 2. Concentrations in the parts-per-billion or parts-per-trillion range are typical, with further reductions in vapour pressures encountered when the explosive constituent is packaged in an oil-based gel or solvent (e.g., RDX in C-4 plastic explosives).

TABLE 2. VAPOUR PRESSURE OF EXPLOSIVES MOLECULES AT ROOM TEMPERATURE AND ATMOSPHERIC PRESSURE

Explosive	Constituent of	Vapour Pressure (parts per billion)
ethylene glycol dinitrate (EGDN)	Dynamite	92 000
nitroglycerin (NG)	Dynamite	340
dinitrotoluene (DNT)	Military TNT	300
trinitrotoluene (TNT)	Military TNT	8
cyclonite (RDX)	C-4, Semtex	0.006
pentaerithrytol tetranitrate (PETN)	Detasheet, Semtex	0.002

4.240. In an Ion Mobility Spectrometry system, the molecules in the air sample are ionized. The ions then pass into a drift region through a shutter that opens periodically over millisecond intervals. Within the drift region, the molecules separate by weight, with the lightest molecules progressing more quickly than the larger molecules. At the end of the drift region, the ions strike a Faraday plate, which records the output current as a function of molecule drift time.

4.241. Ion mobility spectrometry based detectors provide high sensitivity to dynamite, military-grade TNT, and plastic explosives compounds. Due to the sensitivity and relative ease of operation and maintenance, the ion mobility spectrometry technology for explosive detection is widely used. Because ion mobility spectrometry instruments can detect very small masses (nanograms) of some explosives, it can be challenging to clear explosives residues out of the instrument after a large detection.

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

4.243. For screening individuals passing through sensitive high traffic checkpoints, such as airport boarding areas, several walk-through personnel portals have been developed for screening high throughput areas for explosives.

4.244. Trained dogs are also used widely throughout the world to search for explosives. However, dogs require constant retraining to continue to identify synthetic compounds such as explosives. 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 on 6-10 odours and are effective in identifying compounds for a limited period each day. For these reasons, commercial explosive detectors are gaining greater acceptance as the preferred method for screening personnel for explosives.

X-ray imaging

4.245. Devices are commercially available that use low energy backscatter X-rays to image materials on the bodies of persons being screened. The device can provide an image of prohibited items, including explosives hidden under the clothing of persons being scanned. This backscatter device subjects the person to approximately 0.025 micro Sieverts (μSv) per scan. While the energy level is very low and considered safe, many people find any exposure to X-rays objectionable. Invasion of privacy is another issue because the screened person's body is imaged through the clothes. This may be solved by an automated analysis of the produced image that highlights the need for additional search of the individual.

4.246. Millimetre wave imaging is also a commercially available technology for imaging people. The active electromagnetic radiation is approximately 100 GHz in frequency. Most clothing is transparent at this frequency and the skin reflects brightly. Metals strongly absorb this frequency and therefore images produced can reveal hidden items like guns, knives and explosives. Software exists to change the images to address privacy issues.

4.247. In both instances above, secondary screening, typically pat-down searches, is required to resolve detected anomalies.

4.248. Packages may be searched for prohibited items manually or by active interrogation. Active interrogation methods used to detect objects considered to be prohibited items include single energy transmission X-ray, multiple energy transmission X-ray, computed tomography scan and backscatter X-ray. Some X-ray transmission methods are not safe for use on personnel because of the amount of

ionizing radiation. In general, single energy transmission X-ray imagers are used to find metallic items (such as weapons), while dual energy and backscatter X-ray techniques are designed to image materials with low atomic numbers. Examples of prohibited articles made from low atomic number materials are explosives, drugs, and food.

4.249. A conventional single energy transmission X-ray package search system will not penetrate heavy materials sometimes used for shipping containers. High-energy X-rays or multiple energy X-rays (320-keV and 630-keV) are sometimes used to assess the contents of the package being examined. Single energy systems cannot determine the effective atomic number of the material being screened. Most of the development of screening devices for low atomic number materials is directed toward the detection of explosives.

4.250. Screening vehicles, cargo trucks, and large cargo containers requires higher energy interrogating radiation than is common for small package search systems. X-ray systems with energies of 320 and 630 keV are used for vehicle searches. Gamma radiation is used for interrogation in some vehicle screening systems, using nuclides like Cs-137 (661 keV) and Co-60 (1173 and 1333 keV), to provide the radiation which is even more penetrating than the X-ray systems. These high-energy systems, X-ray or gamma ray, require occupants to be out of the vehicle during screening.

Nuclear material detection

4.251. The purpose of nuclear material detectors is to detect the unauthorized removal of nuclear materials on persons, in packages, or in vehicles leaving a security area. There are two commonly used methods to detect nuclear materials, which are applied either in portal or in handheld configurations:

(a) Passive methods use gamma ray and neutron detection technologies to detect the natural radiation and emissions from nuclear materials.

(b) Active methods use neutron activation for detection of shielded nuclear materials.

Gamma ray detectors

4.252. Detection of radiation emitted from nuclear materials is accomplished by using one of several detection materials. Scintillators may be crystalline or organic (within a plastic matrix), semiconductor (solid state) detectors conduct electrically when exposed to radiation, and proportional detectors contain gas that can detect neutrons.

4.253. Some nuclear materials detectors contain scintillators that detect gamma rays from the radioactive decay of nuclear materials. Scintillation is the process by which photons are produced as a result of the absorption of ionizing radiation in scintillator material. Typically, the detectors are crystalline (sodium iodide) or plastic, the latter being used extensively in pedestrian portals.

4.254. Thallium-activated sodium-iodide (NaI(Tl)) coupled to a photomultiplier tube is commonly used to detect gamma rays. Pure sodium-iodide crystals scintillate efficiently when cooled to around 77 K but lose most of that efficiency when near room temperature. The addition of thallium not only increases the efficiency at room temperature, but also causes a shift in the wavelength of the scintillation light such that NaI(Tl) is transparent to its own scintillations. One drawback is that exposure to small amounts of moisture causes the NaI(Tl) to discolour, thus lowering its transparency to the scintillation light and making it useless for radiation detection. NaI(Tl) detectors have some energy resolution and are somewhat useful for distinguishing between radioisotopes have no sensitivity to neutrons. Lanthanum bromide ($LaBr_3$) has slightly better resolution than NaI(T1).

4.255. Plastic scintillators emit photons when high energy rays (X-ray, gamma, neutrons) are incident on the plastic. They cannot discriminate the energy of the radiation that produces the scintillation, thus they cannot identify the isotope detected. The plastic material is more economical per unit area than the crystalline scintillators described above. The plastic material also has lower efficiency than the crystalline materials per unit area. When the cost and efficiency are combined, plastic scintillators provide more sensitivity at a lower cost, but with the loss of any energy resolution. Providing some neutron detection in addition to gamma detection, they are commonly used for radiation screening of personnel.

4.256. Solid state detectors like high purity germanium and cadmium zinc telluride can measure the energy of the gamma ray incident on the crystal. This allows the specific identification of the isotope, because the energy of the gamma emitted is characteristic of the isotopic decay. Such specificity is particularly useful in distinguishing the source of nuisance alarms. For example, a person that has recently had a medical procedure using a radioisotope (like technetium-99m) will present enough gammas to be detected. Solid state detectors can have enough resolution to distinguish the technetium gamma energy spectrum from that of a real hazard like U-235. While these semiconductor crystals have excellent efficiency (sensitivity per unit area) and good energy resolution, they are more expensive per unit area than plastic scintillators. Often, germanium-based detectors require expensive cooling with liquid nitrogen while cadmium zinc telluride detectors achieve reasonably good energy resolution at room temperatures. Solid state detectors also have some neutron sensitivity.

Neutron detection

4.257. Neutron detection is attractive because some nuclear material (especially plutonium) emits neutrons that are difficult to shield, and because the neutron background is generally very low. Thus, neutron detectors can be very sensitive and the detection of neutrons is a good indicator of the presence of nuclear material.

4.258. Alarms are generated when a statistically significant increase over the normal background reading has occurred. Selection of an alarm threshold should be close to the normal background level

but not so close as to cause a large number of nuisance alarms. The signal count is compared to an alarm level derived from an average background count. The background level is established by making counts over a number of counting time intervals. This reference background count is continuously being accumulated, updated, and averaged. Typically, in commercial walk-through models, the signal count is accumulated only during occupancy. Each time the signal count is updated, it is compared to the alarm level, and an alarm occurs if the signal count exceeds the alarm level.

4.259. Nuclear material detector alarms should also detect power line failure, equipment failure, excessively high or low background, or equipment tampering.

Neutron activation detection

4.260. As compared to neutron detection discussed above, neutron activation detection is the process of using a neutron source such as Californium-252 to bombard difficult to search containers (i.e. cargo trucks and railcars) in order to detect the presence of uranium. The radioactive source is used to interrogate the package with neutrons for a few seconds and the source is quickly removed to a shielded location followed by the measurement (counting) of delayed neutrons being emitted by uranium fission fragments. Once neutrons are produced, they are difficult to shield, and because the neutron background is generally very low, detection of delayed neutrons is a good indication of nuclear material. Due to the use of a highly radioactive source in this process, this search method restricts the presence of humans from the container being searched.

Nuclear material portal detectors

4.261. Radiation detection equipment can be installed in portal configurations to search vehicles and railcars to provide detection, see Figures 22 and 23. These nuclear material portal detectors can be incorporated into vehicle or railcar search locations. Detectors can be mounted on a concrete foundation or walls and can be single high or stacked to increase the height of the detection zone. Portals can also be equipped with video monitoring to record the vehicle or railcar detection event. The nuclear material can be detected in either stationary or moving vehicles. Dues to the height of vehicles and railcars, stacking nuclear material portal units may be required to ensure detection coverage.

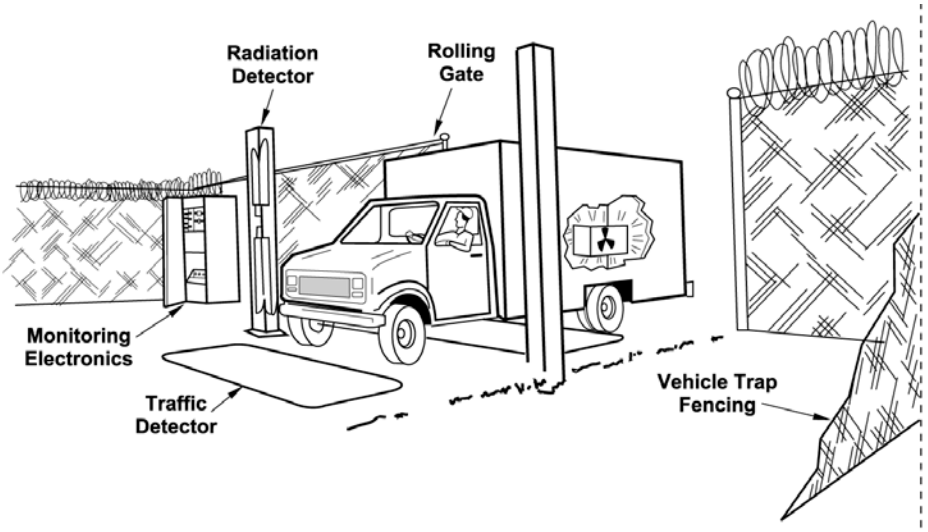

FIG. 22. Vehicle nuclear material portal configuration.

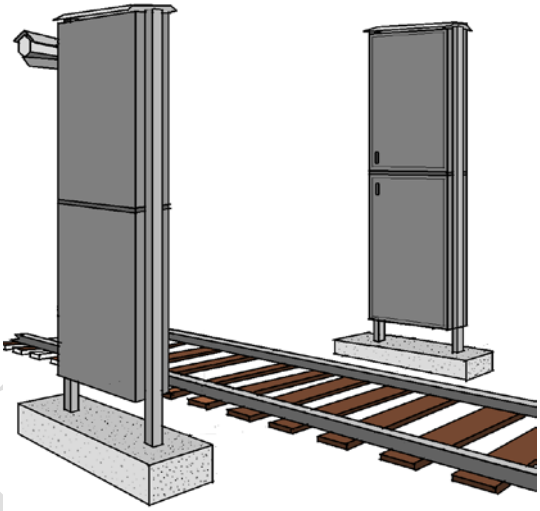

FIG. 23. Railroad nuclear material monitor with CCTV.

Hand held nuclear material detection

4.262. Hand-held nuclear material detectors are available for searching people, packages, and vehicles. Hand-held nuclear material detectors can be used to detect a wide range of nuclear materials or they can be adjusted to search 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 nuclear material portal is not effective. Hand-held nuclear material detectors should be operated very close to the person or location being scanned. At the normal operational distance from the body or object being scanned they are highly sensitive and can be used to detect much smaller quantities of nuclear material than those that can be found by a portal detector. The effectiveness of a

hand-held nuclear material detector is dependent on the technique used by the person doing the screening. A dedicated individual following a well-designed procedure can be very effective but the process will take a considerable amount of time. Because of the time it takes to use a hand-held nuclear material detector properly and the short time it takes for a person to pass through a nuclear material portal, hand-held detectors are mostly used to as a secondary search method for determining the exact location of nuclear material on the person being searched. With this important secondary role, every screening point with a nuclear material portal detector should also be equipped with a hand-held detector, see Fig. 24.

FIG. 24. Examples of hand-held nuclear material detectors.

Shielded nuclear material

4.263. The use of metal detectors, in combination with nuclear material detectors, is considered essential to detect shielded nuclear material. When used in combination to detect nuclear materials and the materials used to shield them, the metal detector should be able to detect relatively small quantities of high atomic number 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, very high sensitivity operation will be required. Because high sensitivity operation will sharply increase the nuisance alarm rate, an area for personnel to change out of steel-toed shoes and to remove other metallic items from their clothes may be required.

Summary of search technologies

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

1 TABLE 3. SEARCH SYSTEM CLASSIFICATION AND TYPICAL APPLICATIONS

Search Type	Typical Items Inspected	Portability	Principle of Operation	Interaction	Alarm Type
Metal Detection					
- Portal	Personnel	Stationary or Built-in.	Electromagnetic	Active and Passive	Alarm
- Hand Held	Personnel	Mobile	Electromagnetic	Active	Alarm
Explosive Detection					
X-ray Absorption	Vehicles, Cargo Containers, Hand carried items	Stationary	Display Monitor, X-ray	Active	Interpreted
Neutron Activation/ Absorption	Vehicles, Cargo Containers, Hand carried items	Stationary	Display Monitor, Radiation	Active	Interpreted
Trace/Vapour	Personnel, Hand carried items	Stationary, Mobile	Gas-Analysis	Active	Both
Trained Dogs	Personnel, Vehicles, Cargo Containers, Hand carried items	Mobile	Explosive Odours	NA	Interpreted
Nuclear Material Detection					
Portal					
- Gamma Ray - Neutron	Personnel, Vehicles, Cargo Containers, Hand carried items	Stationary Built-in.	Radiation	Passive	Alarm
- Neutron Activation	Vehicles, Cargo Containers	Stationary, Stand alone	Radiation	Active	Both
Hand-held					
- Gamma Ray - Neutron	Personnel, Vehicles, Cargo Containers, Hand carried items	Mobile	Radiation	Passive	Both
Combined Metal and Explosive Detection Portals					
X-ray Imaging - low energy backscatter	Personnel	Stationary	Display monitor, X-ray	Active	Interpreted
Electromagnetic radiation - 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

Items inspected – what type of object is typically inspected
Portability – If the system is stationary system, built-in (combined with other applications), or is mobile (can be moved from location to location)
Principle of operation – Type of technology used
Interaction – Active or passive interaction with item being searched
Alarm Type: Audible/Visual Alarm or Interpreted by the Operator.

ACCESS CONTROL SYSTEMS

4.265. Access control systems are used to prevent or to detect unauthorized entry into security areas. Access control systems should allow only authorized persons and vehicles to enter and exit and therefore supports the detection and prevention 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 [2]. Keys, locks, combinations, passwords and related devices used to control access to security areas (limited access areas, protected areas, inner areas, and vital areas) and physical protection equipment should be protected accordingly.

4.266. An access control system may be:

(a) Stand-alone – such as a lock on a door;

(b) Interconnected – a group of access control devices controlled locally; or

(c) Integrated – an access control system with the capability to be integrated with an intrusion detection system.

4.267. The number of personnel authorized to enter each layer of security is typically decreases due to policies to minimize authorized person to a minimum into higher security areas. This allows the access control system to provide detection measures of increasing rigor for each subsequent layer. The throughput requirements at each access point should be weighed against the equipment and screening processes that are put in place. Access controls may include the use of something a person possesses, such as personnel credentials, the use of something a person knows, such as a personal identification numbers (PINs), and a unique feature of a person such as a fingerprint used by biometric devices. The access control system need to be supervised by guards in order that any attempts to circumvent the system is detected and a response is initiated.

4.268. When an access control system is integrated with an intrusion detection system, the requirements for necessary communication paths between servers and access control devices are addressed in Section 7. This type of access control system needs to communicate with the subsystem that detects the state (opened or closed) of access points (such as turnstiles) to be able to accurately record that the individual went through and that the access point is in proper state again after entering. The access control system needs to communicate at some level with the alarm reporting and assessment system. The two systems can be integrated so long as the system manages alarm and access control messages with proper prioritization. If the two systems are not integrated, there should

be at least some level of interaction between the two systems where the systems need to discern between authorized door openings and unauthorized opening of a door, which should initiate an alarm.

4.269. Fig. 25 illustrates an example configuration of the components in an access control portal.

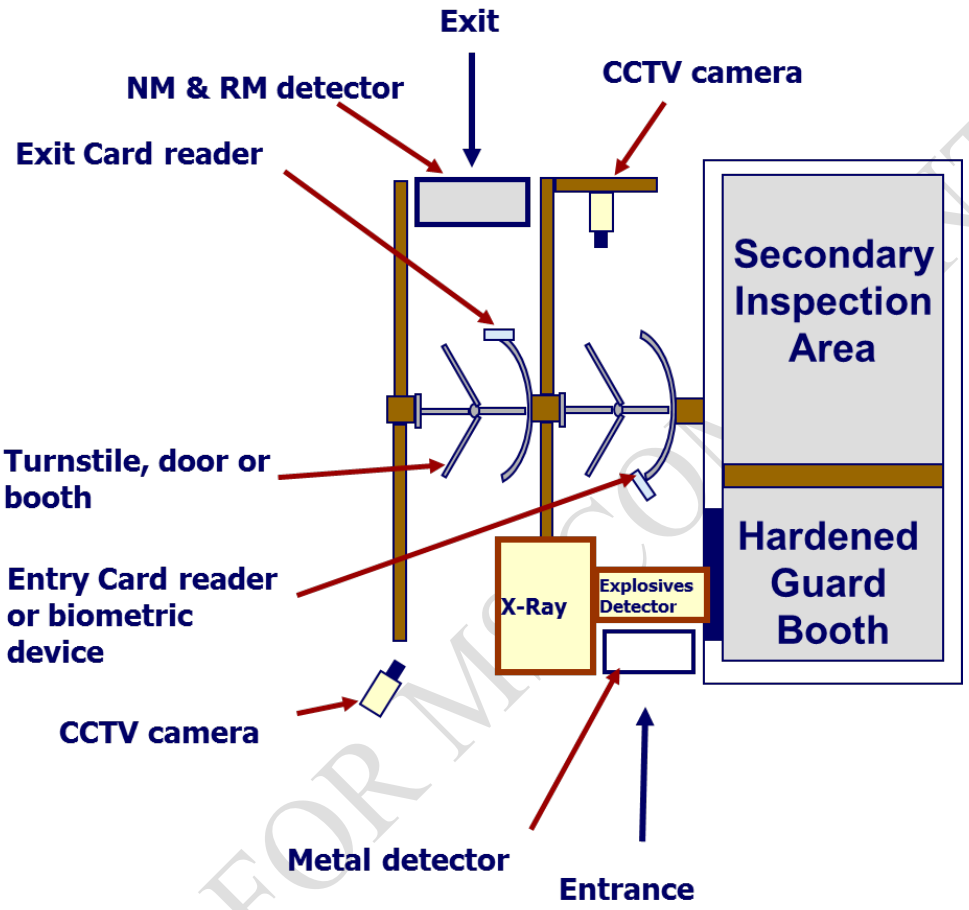

FIG. 25. Example of access control point components.

Personnel access control

4.270. A personnel access control system verifies the identity and authorization of the person seeking entry to a controlled area. Authorization is usually based on need for access to conduct authorized activities. For an automated electronic access control system, the person's data is placed on an access list, typically an electronic database. Modern access control devices have the capability to store the most recent authorized personnel access data so they can operate in backup mode when networks are interrupted. The following is a summary of personnel access control measures.

Credentials

4.271. Identity verification is based on a combination of one or more of the three criteria to identify individuals: something the person has (credentials, such as a badge or card), something the person knows (i.e. password or personal identification number) and something unique to the individual (i.e. a physical trait that can be measured, such as fingerprints, or other biometric attribute). The automated system then makes a decision to grant or deny entry to the area once identity and authorization is verified. The first three credentials (photo badge, badge exchange, stored image) require a visual check by a guard. Some badges contain coded credentials that can be used in automated access control systems. If these badges are used to operate an access control system, to open a door, a turnstile, or a gate for example, the management and control of them should be established in a similar manner to a lock and key control system described below.

4.272. The credentials methods below are ordered from least secure to most secure.

4.273. The photo identification badge is a common credential used for personnel access control, but it 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 in an effort to gain improper entry. Also, since this kind of badge is manually checked, human error (e.g. guard inattentiveness) can reduce its effectiveness, especially at times when large numbers of people are entering a facility. Typically these badges remain in the possession of the person outside working hours.

4.274. A badge exchange system requires that separate badges be held at the access control point. When s person presents a badge and requests entry, a guard compares the individual to the photo on the corresponding exchange badge held at the access control point. If the two match, the guard exchanges the badges and allows entry. The person's badge is held at the access control point until the employee leaves the area, at which time the badges are again exchanged. The exchanged badge worn within the security area is never allowed to leave the area. This minimizes the possibility of a badge being counterfeited, lost, or stolen but does not prevent someone from altering their appearance to match the image on a lost or stolen badge in order to gain unauthorized entry.

4.275. The use of a stored-image system requires a guard to verify 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 to be a form of biometric verification. However, they have an advantage over manual photo identification systems in that it is difficult to tamper with the stored image in the protected database.

4.276. A coded credential, such as a badge, has a method of storing information in or on the credential that can be read by an electronic access control system. Systems that use coded credentials are commercially available with a wide range of capabilities; including provisions to read unique

authorizations codes, time-expired access authorization, and record every passage through each access point and can provide access for specific periods of time and for several levels of entry authorization. Examples for coded credentials are:

(a) Magnetic stripe encoding is used widely in commercial credit card systems. A strip of magnetic material located along one edge of the badge is encoded with data. These data are read as the magnetic strip is moved through a slotted magnetic stripe reader or when inserted into an insertion reader. Magnetic stripe technology is the most popular technique because of its relatively low cost and high reliability. The Wiegand signal is an example of technology that uses a credential code produced by a series of parallel, embedded wires that have special magnetic properties. The wires are typically arranged in two rows. Encoding is 'fixed' during card manufacture. Cards are 'swiped' through a slotted card reader, similar to the way magnetic stripe cards are read. This technology has seen a high degree of acceptance and use in the access control industry.

(b) The barcode, widely used in retail trade to automatically identify products at the point of sale, is sometimes used on coded credentials. The varying widths of the bars and spaces between them establish the code. To read the card, an optical sensor scans the bar code and transmits the information to a decoding unit. Bar codes are easily reproduced using a computer printer. Two-dimensional (2-D) barcodes are also used on security credentials and are capable of storing more information than one-dimensional barcodes. The 2-D barcode is also more difficult to duplicate.

4.277. A proximity badge can be read without the badge being physically placed into a reader device. The electronic proximity identification badge is a small radio frequency transponder (transmitter) and must be powered in some way. The passive proximity badge draws its power from the reader unit through the radio frequency signal as it enters the interrogation field. The active proximity badge is powered by a long-life battery packaged within the unit powers active badges. This active technology has generally been replaced by passive proximity technology. In the past, the technology was a read-only badge, which contains a specific code usually fixed at the time of manufacture and could not be changed. Newer, programmable proximity badges have been developed. With these newer credentials, the system manager can programme the read/write badge according to the system's needs.

4.278. The smart card, also known as a chip card, or integrated circuit card, is the size of a standard bank credit card with an integrated circuit embedded in the card. Gold contacts on the surface of the card allow for communication with a reading device or can be interfaced through low power radio frequency communications (contactless smart card). A smart card includes a microprocessor that gives the card considerable capability. Smart cards can be cost effective since they can also

incorporate other information, for example, financial transactions, personnel training, health care records, or property control functions.

Personal identification numbers

4.279. Many access control systems require users to enter a memorized number, called a personal identification number (PIN) to gain entry. In a 'PIN only' system, the user enters his PIN on a keypad to gain entry. The PIN does not uniquely identify the individual, but rather matches the PIN entered by the individual to any PIN in the system data base. The use of a PIN alone as a method of identity verification does not provide a high level of security. An adversary could observe the PIN or the PIN could be obtained by coercion. Also, unless the system prevents entry of repeated incorrect PINs, the system may be vulnerable.

4.280. A better system uses a PIN in combination with one of the credentials listed above. As an example, an individual requesting access inserts their coded credential into the system and then enters their memorized number via a keypad. This number is compared to the one stored in the access file for that person. If the numbers are the same (and the person has the appropriate authority), the person is granted entry. It does have weaknesses; an individual could pass the PIN and credential to an unauthorized individual.

Personnel tracking

4.281. Many access control systems provide the capability to track personnel by recording data read from credentials at entry and monitoring points. It can be used to track the movement and location of personnel within a facility as they pass through doorways, gates, or other portals. The system records the locations and areas visited by personnel each day and can restrict access to certain locations during off-shift hours. The personnel tracking system helps protect against procedural violations, such as removing or exchanging credentials, detects violations of a two-person rule, and eliminates the risk of credential pass back. In addition personnel tracking maybe used to restrict entry of an individual to some but not all safety systems which provide important redundancy.

4.282. The data is stored in a permanent log and provides access to information by date, area, person or other parameters. Under most situations they provide a reasonable capability to track personnel. If appropriately recorded, access control records can be used during the investigation of a malicious act to determine a list of possible suspects or to ensure guards are performing their assigned patrol duties properly. Awareness that a facility has a tracking system may deter personnel from unauthorized actions. It is advisable that requests for authorized access to security areas or systems important to safety or security, whether approved or disapproved, be reviewed regularly to confirm continued need for access and to help identify potential insider malicious activity.

Two-person rule for access control

4.283. The two-person rule is a well-defined and established security measure to counter potential malicious acts by an insider working alone in high security areas (e.g. vital areas, inner areas, CAS).

4.284. Some automated access control systems require two sets of credentials and/or biometric characteristics to be entered prior to the system prior to granting authorized access to an area. This would apply to entry and egress to/from the high security area to ensure a single person is not left alone in a high security area (e.g. nuclear material storage location). Two-person rule access controls may be implemented when opening security equipment alarm cabinets and controller processing rooms during maintenance activities. A two-person rule can be implemented for certain CAS operator functions such as remotely opening a security door and other sensitive operations.

Vehicle access control

4.285. Vehicles may be subject to access controls when entering or exiting security areas. In some cases, verification of authorization of the driver and occupants only is used rather than authorization of the vehicle. In higher security areas, a vehicle registration system may be used to allow only authorized vehicles to enter.

4.286. Depending on the facility requirements and size, vehicle access control methods can consist of automated and/or manual methods. For a small facility a manual list of approved vehicles may be developed to limit vehicle access to security areas. For large and complex facilities, an automated database for approved vehicles may be developed similar to personnel access control logs, or a system using automated vehicle identification or recognition technology may be used. Access control systems may include vehicle license number plate recognition or embedded chip technology for vehicle tracking and logging of access. Image databases may also be used to identify authorized vehicles and to determine if modifications have occurred as compared to the approved and pre-screened configuration.

Access control in emergency situations

4.287. In an emergency situation, methods should be developed to provide access by emergency personnel. It may consist of procedures to escort emergency personnel into nuclear facilities by authorized individuals. Further guidance on this topic is provided in Ref. [2].

Locks and keys

4.288. A lock is a mechanical latching device for securing a physical barrier and consists of a mechanism that is used to withdraw a latching system. Locks are important components of a PPS, and provide both access control and delay against unauthorized access. Since a barrier, such as a door may

be penetrated either by breaking down the door or by defeating the locking mechanism, lock selection should consider hardware that provides delay as close as practical to the rest of the barrier. A lock and key management system for access points may consist of a two-person-rule for sensitive areas and therefore may limit collusion opportunities. Locks are commonly categorized by the mechanism used to withdraw the latching system. These include combination locks, keyed locks, and electronic locks.

4.289. Combination locks are designed as either a case lock, in which a combination lock is mounted on or into a barrier, or a padlock. Combination locks include multiple-dial locks, pushbutton locks, single dial locks, or electronic combination locks. A multiple-dial lock uses several rotating disks, and is commonly used on small containers, briefcases, and bicycle locks, and can be easily defeated. A mechanical pushbutton lock uses pushbuttons that activate linkages that connect a gate with 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 combination is discovered. A single dial combination lock is a mechanical lock with a spin dial, which interacts with several parallel discs or cams. Customarily, a lock of this type is opened by rotating the dial clockwise to the first numeral, counter-clockwise to the second, and so on in an alternating fashion until the last numeral is reached. The cams typically have an indentation or notch, and when the correct combination is entered, the notches align, allowing the latch to fit into them and open the lock. Depending on the quality of the lock, some single-dial combination locks can be defeated relatively easily, but there are high security designs that are difficult to defeat. Electronic combination locks are also available, and offer many features unavailable with other types of combination locks. Depending on the type, they can be defeated as with other combination locks, but they are typically more difficult to defeat.

4.290. Keyed locks can be categorized as warded locks, wafer (or disk) locks, lever locks, and pin-tumbler locks. The most common type of keyed lock is the pin-tumbler. As in the case of combination locks, a key lock should normally be capable of being set for a large number of different keys. Beyond basic pin-tumbler locks, several high-security lock cylinders are available. These provide considerably increased resistance to covert and surreptitious attack. They also offer greater key control capability because manufacturers offer restricted keyways. A restricted keyway is a special non-stock hardware set aside by the manufacturer for limited use. A letter of authorization is typically required to process orders for keys, blanks and cylinders. Restricted keyways offer a higher level of security because of the restrictions in making copies of keys. Keyed locks offer the capability for master keying, having separate keys that only open one lock, with a master key that can be used to open all the locks of that type. It is advisable that extra controls be implemented when using a master key system because if a master key is lost or stolen, it can be used to open all the locks at the facility using that keyway.

4.291. An electronic lock is a system comprised of 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 correct token is presented. A range of technologies are available in such systems, as described in this section, including biometric, magnetic-stripe card, proximity cards, smart cards, and combination entry. An electronic lock offers a number of advantages, including isolation of the lock part containing the code from the exposed part of the lock, versatility of programming, and ease of integration 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 egress from the secure side is possible. Many electronic locks are equipped with a case lock in the door. There is often a physical key to its cylinder, the emergency override key, which can be used to gain access to areas during a power outage.

4.292. A facility should implement a lock and key control system, and define roles and responsibilities for control of locks, keys, and other access control devices or measures. A lock and key control system should include all locking devices used at a facility. The following paragraphs describe some of the components of a lock and key control programme.

4.293. A lock and key hierarchy should normally be developed, to group locks, keys, and other access control devices into groups based on a graded approach. Locks, keys, and other access control devices used as part of the physical protection of assets and facilities may be categorized as security locks and keys to distinguish them from administrative locks and keys.

4.294. Lock and key control and protection measures should be developed for security locks, keys and other devices with appropriate measures based on the consequence of their loss or compromise. As an example, all keys used to gain access to a vital area should be strictly controlled and protected to ensure they cannot be used by an unauthorized person to gain access, whereas a key to an administrative office door may have minimal control or protection. Spare security locks, cores, keys, key blanks, and cards/credentials should be stored in a secure location.

4.295. An authorized access list (for example, identifying personnel authorized to have access to security keys) may be used. Keys and combinations should be issued only to individuals who are authorized users and require use of the security key/combination. A lock and key control system should include procedures for verifying the identity of the individual requesting the keys or combinations and determining the individual is authorized access to all areas unlocked by the keys or combinations provided.

4.296. An inventory management system should be developed to provide accountability for security lock, keys, and key/cards/credentials in use, and spares in storage. To implement an inventory system, security locks and keys should have a unique characteristic, such as a unique identification number. A record of all locks, cores, keys, key blanks, and cards/credentials should be maintained and kept in a

secured location. The records should identify the number of keys for each lock and their location and should note when a lock was changed, rekeyed, or rotated. At a defined frequency, inventories of all the security locks, keys, and other devices should be conducted. Measures should be established to address lost or stolen items to include activities such as re-keying, changing of locks, or changing of combinations or codes as necessary. A notification process should be established for reporting lost or stolen security locks and keys.

4.297. A combination and PIN management system should be developed to control issuance to authorized personnel. Records of combinations and PINs should be appropriately protected. Records should also be maintained of personnel with authorized knowledge of combinations and PINS, when lock combinations or PINs were last changed, and when they are required to be changed. A good practice is to periodically change combinations and PINs, and to change combinations or PINs when personnel with authorized knowledge no longer require a need for access, or there is evidence that they may have been compromised.

Biometric identity verification systems

4.298. Biometric identity verification systems use a unique physical or physiological biometric characteristic(s) of an individual to verify authorization. Commercial equipment is available that uses weight, hand or finger geometry, blood veins, fingerprints, facial verification, eye pattern and other physical characteristics. All personnel identity verification systems are concerned about the uniqueness of the feature used for identification, the variability of the characteristic, and the difficulty of implementing the system which processes the characteristic. Biometric systems can be used to validate other access controls credential or in 'recognize' mode where the entry of a secondary identifier is not required. In the first case, the system uses the first credential to identify the appropriate record, and then the system verifies the associated biometric data is correct. When used in recognize mode, the entire biometric enrolment database is potentially reviewed by the system until the appropriate record is located for authentication, which increases the verification processing time as the number of data entries is increased.

4.299. All technologies using biometrics characteristics have a segment of the population that cannot use the equipment, so alternate methods need to be implemented for that population. Additionally, in some nuclear facilities, as authorized personnel access higher security layers the potential for radioactive contamination exposure increases, and the need for personal protective equipment may be required. As a result of wearing equipment such as gloves, respirators, or other protection measures, proper selection of a workable access control measure must be determined. For example, if the authorized person must wear gloves, hand geometry or fingerprint recognition device may not be appropriate. Additionally, if a respirator is required, facial recognition, eye pattern or iris-based recognition systems may not be feasible.

4.300. The following is a summary of biometric access control measures.

4.301. Weight scales can be incorporated into personnel access control booths. The authorized person's weight is entered into the system for comparison during a facility access process. If the weight matches within a specified tolerance, combined with other access control measures such as cards and PINs provide increased assurance of positive identity verification. Weight scales also reduces the risk of credential pass back and unauthorized entry of more than one personnel simultaneously.

4.302. Hand geometry systems characterize the shape of the hand. The underlying technique measures three-dimensional (3D) features of the hand such as the widths and lengths of fingers and the thickness of the hand. A solid-state camera takes a picture of the hand that includes a side view (for hand thickness). The combination of infrared illumination and the reflective platen makes the image of the hand appear as a silhouette to the camera. The system measures lengths and widths of a number of hand parts and creates a numerical representation of the hand called a feature vector or template. During verification, the system compares the image with previous measurements (the template) obtained during enrolment. If the read image and the stored template match within an allowable tolerance, verification is successful.

4.303. Two-finger geometry is a similar system used to verify identity. This two-finger geometry system measures finger lengths and widths of the index/middle finger pair. The functional concept of this device is similar to the hand geometry system.

4.304. Blood vein pattern particularly in parts of the human hand are useful characteristics that can be used to verify identity. A number of companies have developed biometric identity verifiers based on the vein pattern in the palm, the finger and the back of the hand. Near infrared light can penetrate the skin to sufficient depth to clearly image the veins in parts of the hand when used in conjunction with any solid state camera.

4.305. Fingerprint systems typically use minutia points (fingerprint ridge endings and bifurcations) as the identifying features of the fingerprint, although some systems use the whole image for comparison purposes. All fingerprint identification systems require care in finger positioning and accurate print analysis and comparison for reliable identification. Current systems also incorporate a liveness/pulse check for added assurance. Direct imaging sensors that use solid-state devices are also available for acquiring fingerprint images. Capacitive, e-field, and thermal methods have been commercially developed. The devices are common for desktop applications such as secure computer logon.

(a) The ultrasound method images the lower layers of the skin where the fingerprint is not damaged. Therefore, this technique is not as susceptible to dry or worn fingerprints

taken from the top skin surface. Ultrasound imaging is not as fast as optical methods because of the raster scan required by the ultrasonic transducer.

(b) Optical methods using a prism and a solid-state camera are most often used to capture the fingerprint image. Dry or worn fingerprints have been difficult to image using optical methods, so special coatings have been applied to the optical platens to enhance the image quality. The purpose of these coatings is to ensure a good optical coupling between the platen and fingerprint.

4.306. 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 systems may also capture thermal images using an infrared imager. Distinguishing features are extracted from the image and compared with previously stored features. If the two images match within a specified tolerance, positive identity verification is determined. Developers have had to contend with two difficult problems: (1) wide variations in the presentation of the face and (2) lighting variations.

4.307. Eye pattern features are as unique as fingerprints. Successful commercial systems have been developed based on 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. The intensity of the reflected light versus beam position during the scan indicates the unique location of the retinal blood vessels.

4.308. Iris-based biometric systems use a video camera to image the iris structure of the eye. The unique structure of an iris can be used to identify an individual. A distinct advantage is that the camera images the iris at a distance of about ten inches so no physical contact between the face and the scanner is required and there is no LED shining into the eyes (the eye is externally illuminated with visible light). Users favour iris scan technology over the retinal scanner. Possible disadvantages of iris-based biometric technology may include false rejection errors when the user wears eye glasses, transaction times from 4 or 5 seconds (by practiced users) up to 15 seconds (for new users), and about 2% of the population are unable to enrolled because of their iris colour and structure.

Seals or tamper indicating devices

4.309. Seals or tamper indicating devices (TIDs) can be used for example with locks and alarmed locations as an additional indicator of an unauthorized opening of a container. When used, periodic checks should be implemented to confirm that seals and TIDs do not reveal irregularities.

DELAY

4.310. The role of barriers is to increase the adversary task time by introducing impediments along any path the adversary may choose, thereby providing the needed 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. Some barriers might deter or, if the adversary is unable to complete penetration, even defeat some threats. With the exception of a few barriers provided by natural elements such as rugged coastlines, high cliffs, mountaintops, and vast distances, delay should be provided by barriers that are carefully planned and positioned in the path of the adversary. The degree of delay afforded depends on the nature of the physical obstacles employed and the level of threat considered. In addition to being used for delay, barriers can be used to mitigate the consequences of a stand-off attack. Guidance on physical barriers is given in Ref. [2].

4.311. Barriers should be considered in relation to the adversary's objective (theft, sabotage) and the capabilities of the adversary as defined in the threat assessment or DBT. If the objective is theft of material, barriers which are penetrated or destroyed on the way into the facility may not provide delay for departure from the facility. Some barriers, such as emergency exits, may provide some delay from the outside, but due to safety requirements, allow rapid exit from the inside.

4.312. Table 4 provides an overview of the types of barriers 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.

TABLE 4. BARRIER TYPES

Type	**Placement**	**Function**	**Limitations**	**Possible Compensatory measures**	**Ensure the integrity**
Low security barriers	Facility boundaries	Demarcate boundary	No delay	Guard patrol	Visual inspection
Security fence	Facility boundary, security areas	Demarcate boundary, Assist detection and assessment by delay, might be part of detection system.	Limited delay	Guard post	Visual inspection, may have sensors
Vehicle barrier	Usually at security area boundaries	Prevent unauthorized vehicle entry	Barriers are designed for a maximum weight and speed of a vehicle.	Temporary devices or obstacles.	Visual inspection
Structural barriers	May be used as the	Provide delay	No stand-off, some	Guards, response forces,	Visual inspection, may have sensors

(buildings)	boundary of a security area		elements may need to be hardened for balance (e.g., installing grills or grates on windows)	moveable obstacles	
Turnstiles and Doors	At or within security area boundaries.	Used to allow authorized entry into a security area.	May be difficult to balance delay with associated barrier.	Guards, response forces, moveable obstacles	Visual inspection, may have sensors
Boundary penetration barriers	Specific locations	Provide balanced delay	May be difficult to balance delay with associated barrier.	Guards, response forces, moveable obstacles	Visual inspection, may have sensors
Specialized Barriers (blocks and tie-downs)	Specific locations, such as target locations, to increase delay	Provide balanced delay	Safety/ Operational impact	Guards, response forces, moveable obstacles	Visual inspection
Dispensable Barriers	Target locations	Provide delay	Safety, limited use, confined space issues	Guards	Maintenance and testing
Marine Barriers	Waterway boundaries	Provide delay against attack from waterways	May be difficult to design and deploy (tides, current, etc.)	Guards	Visual inspection

4.313. Different barriers designs can be used to create certain delay functions and 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 serves to delay the adversary at the point of detection and increases the probability of accurate assessment (see also Evaluation in Section 9).

4.314. A balanced barrier design ensures that each aspect of a barrier configuration affords equivalent delay as much as practical. The following design considerations should be considered for a balanced delay system:

(a) Locate vehicle barriers at the outermost detection zones to:

— limit the adversary use of vehicles near the target location,

— force the adversary on foot to hand-carry tools or breaching aids, and

— eliminate the use of a vehicle as a ramming device at the target location.

(b) Use barriers to maximize delay time closest to the target.

(c) Use barriers consisting of different materials requiring multiple defeat methods and tools.

(d) Use barriers in confined spaces to minimize the adversary work space and create difficult working environment for the adversaries.

Low security barriers

4.315. Low security barriers are typically used the outermost boundary of a facility for safety purposes, for example for construction projects, and offer minimal delay to an adversary. They are however frequently used to demarcate boundaries, keep animals out of the detection zone, or used for criminal prosecution purposes. Typical low security barriers include wooden fencing, fabric fencing, and wire fencing.

Security fences

4.316. Security fences are installed at security area boundaries. They provide deterrence, some delay and are often used in conjunction with intrusion detection systems. They can be used to support the functions of detection and assessment. As an 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.

4.317. A security fence usually consists of panels, uprights, hardware, and foundations. As seen in Figures 26 to 31, typical examples for security fence panels include: chain link fence, welded mesh, expanded metal (normal or flattened), metal palisade; woven metal, reinforced concrete.

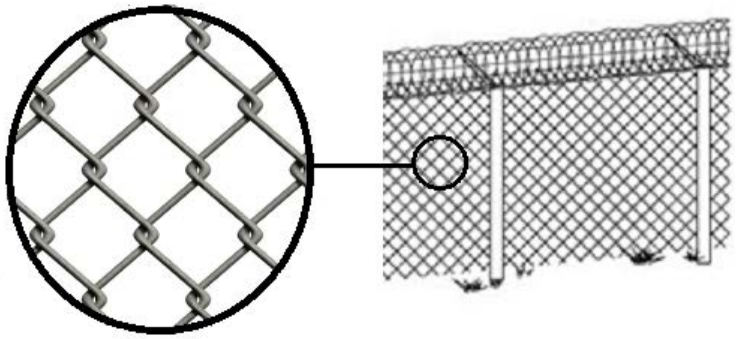

FIG. 26. Example of chain link fence fabric.

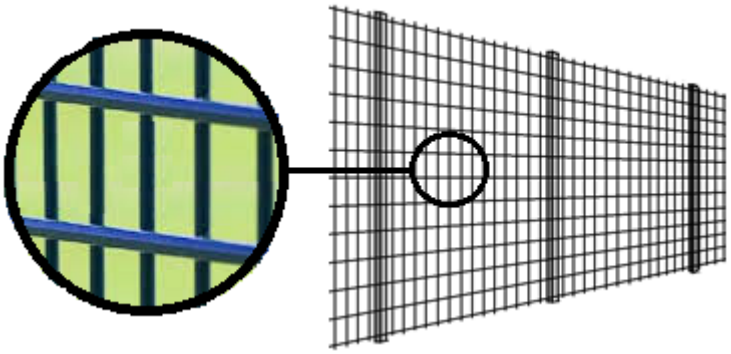

FIG. 27. Example of welded mesh.

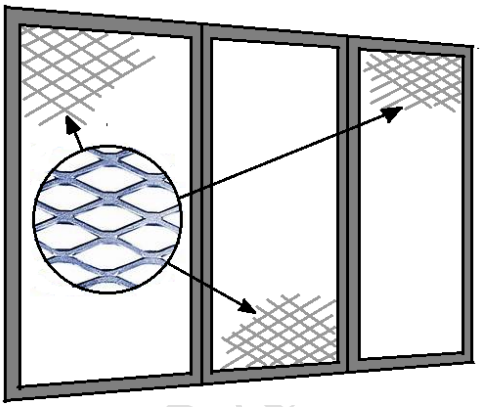

FIG. 28. Example of expanded metal fabric.

FIG. 29. Example of a metal palisade barrier.

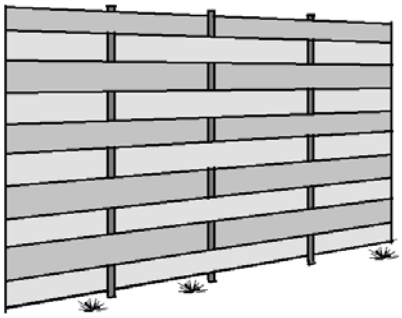

FIG. 30. Example of woven metal fence.

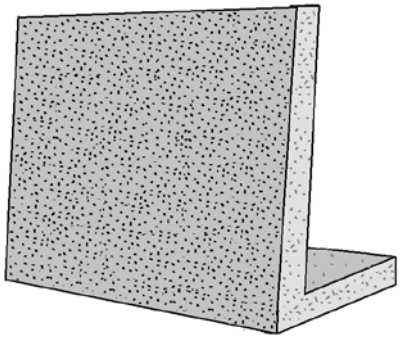

FIG. 31. Example of reinforced concrete barrier.

4.318. Security fence construction should also prevent tunnelling under the fence. This can typically be achieved by extending the foundation into the ground or by concrete grounding.

4.319. Security fence design should consider the associated detection systems and adversary capability. When selecting a fencing material, especially when replacing existing security fences, the impact on patrolling strategies and CCTV coverage will need to be considered, as different fencing materials may change visibility through the fence. For specific purposes other materials (for example security glass) may be used as fencing material. All fence types need to be designed for the specific delay desired use considering the threat assessment or DBT but also the requirements of the intrusion detection and assessment system.

4.320. Security fences might be used as part of the detection system itself. Examples include fences with mounted fibre optic cables, strain sensitive sensors fences and fence mounted vibration sensors. Fig. 32 illustrates examples of fence mounted fibre optic cables and vibration sensor cable.

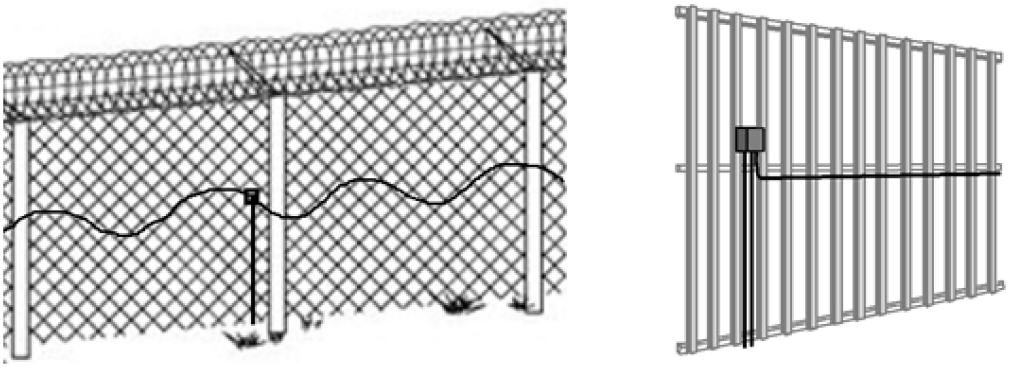

FIG. 32. Example of security fencing with sensors.

4.321. Security fences should be subject to regular visual inspection to ensure their delay function. Typical compensatory measures include the placement of guard posts to restore the delay and detection function, as necessary.

Use of barbed tape coil

4.322. Placing rolls of barbed tape coil (BTC) on or near standard fences can enhance their capability to delay intruders. Some examples for the placement of BTC are shown below. Barbed tape coil added to the top of an existing security fence can be an effective addition as an intruder will need to bring additional aids or equipment to climb over the fence (Figures 33–36). If used, a facility will need to consider the threat assessment or DBT, environmental conditions, safety impacts or legal implications, and the structural capability of the existing barrier.

4.323. Figures 33 to 36 show another enhancement that involves placing barbed tape rolls either horizontally on the ground, against the fence fabric, or between the fences. The barbed tape rolls are placed between the two perimeter fences to prevent accidental injury to the casual passer-by from outside and inside the facility. When the barbed tape rolls are placed horizontally, they should be staked to the ground and care taken to prevent excessive plant growth and collection of debris in the rolls.

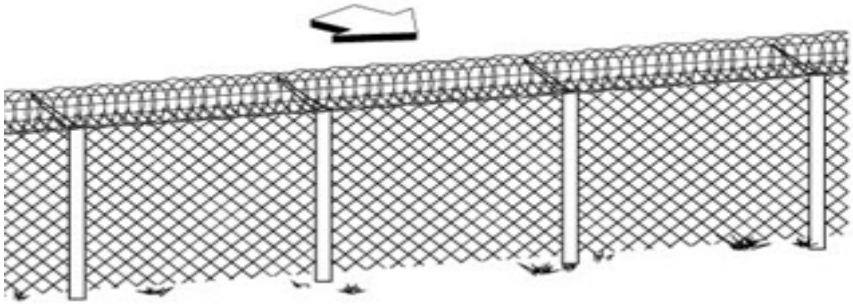

FIG. 33. Security fence topped with a single roll of BTC.

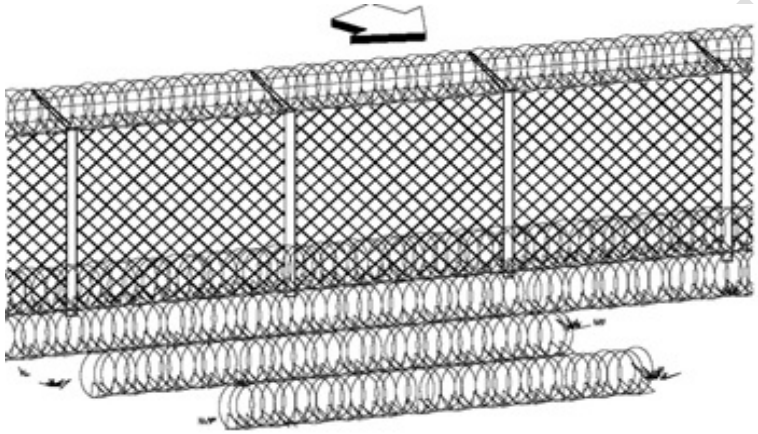

FIG. 34. Security fence with five rolls of BTC.

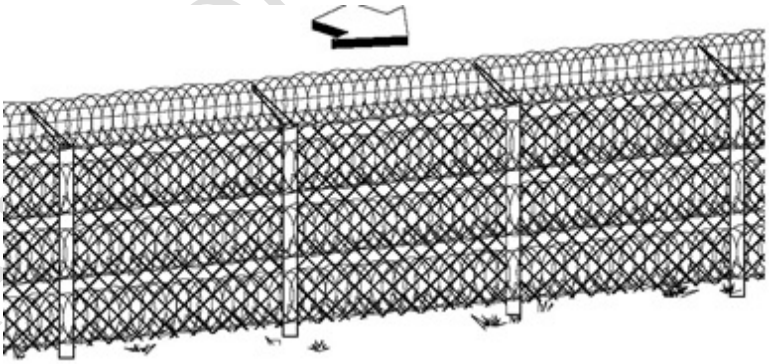

FIG. 35. Security fence with four rolls of BTC.

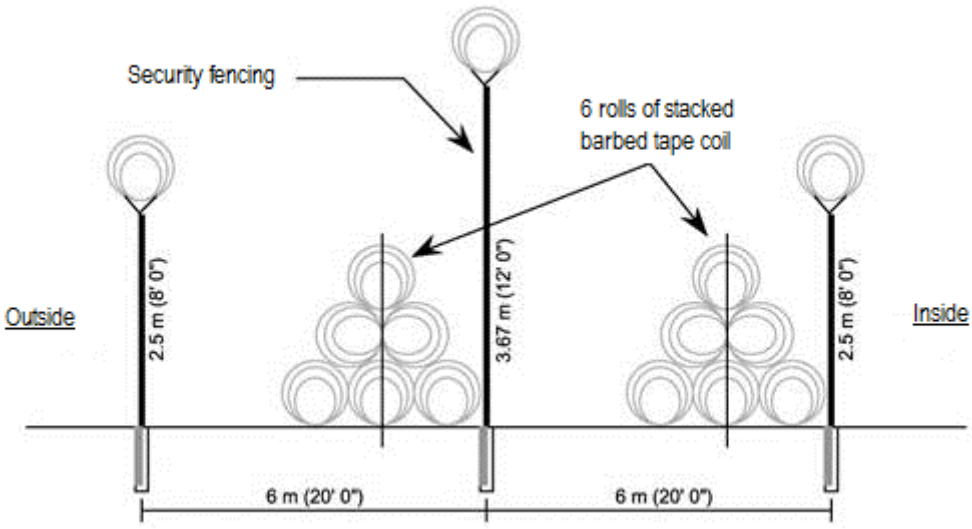

FIG. 36. Additional security fence configuration with BTC.

Vehicle barriers

4.324. Vehicle barriers are designed to prevent unauthorized access of vehicles to a facility. They can either be permanent structures that are built in-line with security fences or movable components at vehicular driveways and rail gates. In order for the vehicle to be stopped, the vehicle's kinetic energy must be dissipated. A well-designed vehicle barrier system should be capable of stopping a defined vehicle 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 vehicle barrier line.

4.325. For vehicle barriers, penetration is achieved when a vehicle passes through the barrier and is still functional. Penetration is also achieved when the vehicle barrier is removed or bridged allowing a vehicle to pass through. Penetration may also be achieved when a first vehicle causes an opening allowing a second vehicle to be driven through the breached barrier.

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

(a) Define the threat (using the DBT) that the barrier system is intended to stop (including the type, size and weight of vehicle, impact velocity, and other physical characteristics).

(b) Understand facility operating conditions (vehicle throughput).

(c) Evaluate limitations of vehicle barriers to protect against unusual vehicle types (e.g. small delivery vans, motor bikes or construction vehicles).

(d) Determine the areas to be protected before selecting the optimal locations to install vehicle barriers.

(e) Examine the site-specific considerations such as terrain, road layout in and around controlled areas, potential avenues of approach, and environmental conditions.

4.327. Select the barriers that are best suited to protect against the vehicle threat. In order to provide full penetration resistance, barriers should be selected to fit the particular situation and be installed properly.

(a) Barriers that are installed outside a detection zone should be designed to be difficult for an adversary to defeat. This, coupled with routine patrols, will make it difficult for an adversary to remove the barriers without detection and a response. For example, deeply buried, concrete-filled pipes could reduce the need for surveillance of an area.

(b) Vehicle barriers that can easily be defeated surreptitiously should be located inside a detection zone to detect tampering of the barrier.

(c) Consider the height at which the vehicle barrier will impact the vehicle. The optimum height for any barrier depends on its construction and the anticipated vehicle threat.

4.328. Most permanent vehicle barriers are designed to stop vehicles through one or a combination of the following methods:

(a) A vehicle arrestor absorbs virtually all of a vehicle's kinetic energy and applies a low to moderate resistive force to gradually stop a vehicle in a relatively long distance. Examples are weights that are dragged by a penetrating vehicle and accumulate with distance travelled, or cables attached to braking systems to dissipate the vehicle energy.

(b) A crash cushion absorbs a large portion of a vehicle's kinetic energy and provides a stiff resistive force to stop a vehicle in a reasonable distance. Examples are liquid-filled plastic containers and arrays of empty steel barrels that are backed by strong supports.

(c) An inertia device exchanges momentum and kinetic energy with a vehicle during impact. This device provides a stiff resistive force to stop a vehicle in a reasonable distance. Examples are relatively small concrete shapes and sand-filled barrels that are not anchored.

(d) A rigid device provides a high resistive force to stop vehicles in very short distances. 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. Train derailleurs are a type of rigid device.

4.329. Vehicle barriers are potentially vulnerable at the access points. Vehicle driveways are often aimed directly toward an access point, making it susceptible to ramming by a vehicle. The orientation of vehicle gates and driveways could reduce the probability of breaching with vehicles. Driveways

constructed with multiple turns and barriers (e.g. chicanes) on each side of the access point area and/or on the driveway will reduce the approach and departure speed of vehicles. Adding a serpentine path into a protected area in front of a vehicle barrier can reduce both the potential impact velocity and its kinetic energy.

4.330. A good practice at access points is the installation of interlocking movable vehicle barriers. This requires one movable vehicle barrier to be closed and locked before the other could be released and opened. The area between the vehicle barriers provides a holding area to allow search processes to occur prior to persons attempting entry or exit. Other methods (e.g. using vehicles, containers or heavy construction bags) as temporary vehicle barriers may be considered.

4.331. Typical movable vehicle barriers are designed to stop unauthorized vehicles, but are designed to be moved to allow authorized vehicles to enter. There are many different types of moveable vehicle barriers. Some examples include raised bollards, pop-up, and raised boom, see Figs 37–39.

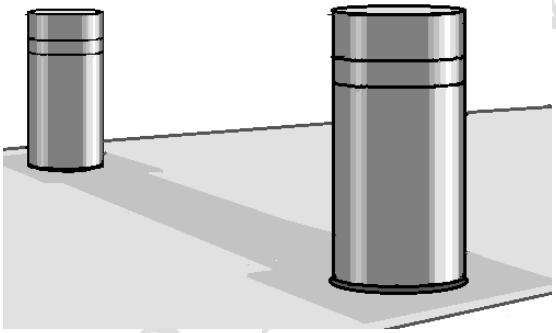

FIG. 37. Automated or manual raised bollards vehicle barrier.

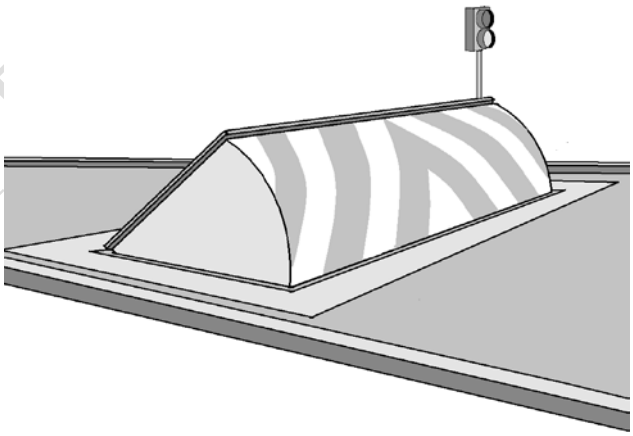

FIG. 38. Example of a pop-up vehicle barrier.

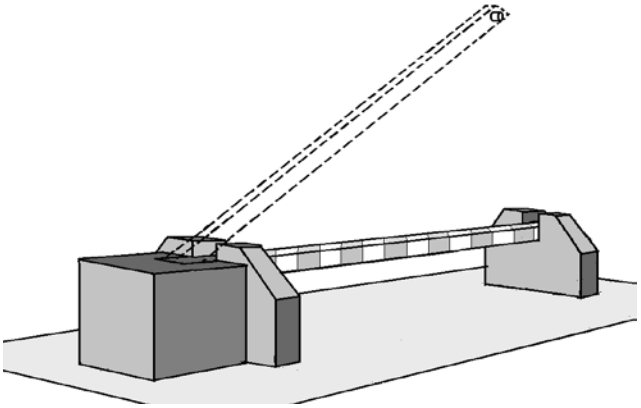

FIG. 39. Example of moveable boom vehicle barrier.

Structural barriers

4.332. Structural barriers are building components that include concrete walls, floor, ceiling and roofs. Structural barriers may also include interior freestanding structures that offer additional delay along the adversary path. In addition to the delay function, structural barriers may also be used for guard or response force protection.

4.333. Concrete walls, floors, roofs and ceilings are designed to support structural loads and, except for vault walls, are not necessarily designed specifically to delay penetration. Conventional wall construction includes wood framing, brick, block, or concrete. In concrete wall construction, strength and thickness of concrete and size and spacing of reinforcing (rebar) materials are determined based on structural requirements. However in order to meet the delay time requirements for physical protection, structural barriers may need to be designed above industrial construction standards or reinforced. In addition, protection against stand-off attacks should be considered when developing wall specifications.

4.334. Specifications for structural barriers should take into consideration the capabilities of the threats defined in the threat assessment or DBT. Typically, penetration methods an adversary may use to defeat a structural barrier include hand, power and thermal tools, and explosives, used alone or in combination.

4.335. If possible, one consideration when designing a new facility is to build a facility with inherently large delay. This not only protects against current threats, but may provide protection against new and emerging threat capabilities. New structural barriers can be designed with large amounts of delay. In some cases, existing structures can be made more robust by adding features to increase delay. Methods to increase delay of structural barriers are:

(a) The construction of two or more reinforced concrete walls in series close to each other provides a longer penetration delay times than one wall of equal thickness. Penetration

of multiple walls requires multiple individual efforts and the transport of tools through preceding walls.

(b) The construction of two or more reinforced concrete walls with fill material (such as rock) between the walls.

(c) The use of multiple materials to construct a composite wall, such as steel plating encasing both sides of the concrete wall will increase the delay time and complexity of task to defeat the barrier.

(d) Use of roof enhancements such as the installation of membranes with embedded screen, several inches of rigid insulation, reinforced concrete with deformed steel bars and expanded steel mesh, and large rebar placed into multiple rows or layers in reinforced concrete.

(e) Wall rebar reinforcement in a concrete wall can extend the penetration delay time in most designs. Even though the concrete is penetrated by the explosion, the reinforcing material usually remains intact so that it needs to be removed before entry can be accomplished. Removing the rebar often requires more time than is needed to remove the concrete; therefore, using additional rebar, increasing rebar size, or decreasing centre-to-centre rebar spacing can be advantageous.

(f) The use of earth cover or other overburden to delay access to the wall itself is a good enhancement.

(g) Barriers placed below and spate from the roof may be more effective against penetration than those in the roof itself. Such barriers may 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 may require a second penetration attempt. This second penetration may also be constrained as it would take place in a confined area and could force the use of tools from other tool classes in order to complete penetration. A suggested optimum distance below the roof is approximately 30 cm. This distance may restrict subsequent adversary breaching actions due to the debris. The enhancement materials may include quarry screen, expanded steel, bank vault mesh or floor gratings.

4.336. When used as protection for guards and response, barrier design should consider ballistics and explosive effects to enhance human survivability. Used as a fighting position, the design may include gun ports (or openings) and bullet resistance glazing, among other protective and operational features.

Turnstiles and doors

4.337. For a balanced barrier design the penetration delay time of access points within a barrier line should equal the delay time of the surrounding barrier structure. Examples of personnel access points with delay functions at a security area boundary include: metal turnstile, hardened turnstile, personnel portal or sally port (a booth with interlocking door), hardened steel grated door, and hardened steel barrier door. See Figures 40-43.

FIG. 40. Example of a metal turnstile.

FIG. 41. Example of a hardened turnstile configuration.

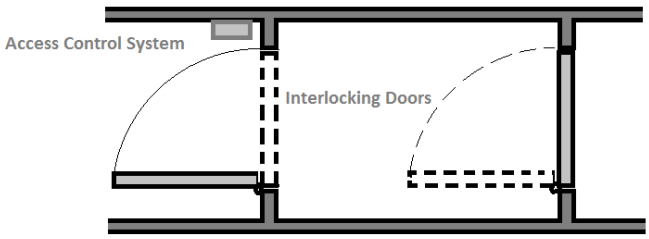

FIG. 42. Example of a personnel portal or sally port configuration.

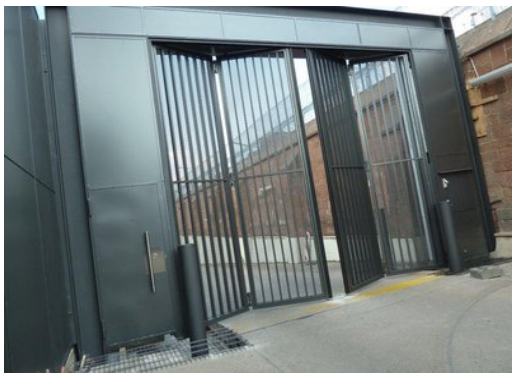

FIG. 43. Hardened steel grated door (may be guarded or unguarded).

4.338. The barrier value of a wall should not be reduced by the use of standard doors, frames, and hinges and other openings. Penetration delay times through access points can be increased with thicker or composite materials. In addition hardened and explosive as well as bullet-resistant doors and grills are available and may offer a substantial increase in penetration resistance. Doors and their associated frames, hinges, bolts, and locks should be strengthened to afford the same delay as provided by the floors, walls, and ceilings of the parent structure. High-strength vaults for the storage of Category I material for example need to have high-strength vaults doors.

4.339. The interaction of safety and security functions is a specific challenge for access points that are part of emergency pathways and also have delay functions.

4.340. In addition, measure like remote lockdown (temporary blockade of emergency hand gears for emergency doors) in case of an assessed alarm and visual supervision of the situation may be considered. Other solutions may 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 are rather expensive, the number should be reduced to a minimum.

4.342. Standard personnel doors that are usually lightweight sheet steel doors which penetration time may vary depending on the attack tools used. Generally these doors provide little delay. Therefore an upgrade of existing doors may be considered to increase their penetration delay time and balance the overall door structure, including the door face, frame, hinges, exit devices, louvers, glazing, and locks, and protect it against forcible penetration attempts with hand, power, or thermal tools. The following methods can be used:

(a) Eliminate all unnecessary louvers, external knobs, keyways and other openings.

(b) Add steel plates to door surfaces to increase the penetration resistance of a door.

(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. Cover the holes with a plate, which is welded into place.

(h) Weld the pin top to the hinge to extend penetration times.

(i) Use hinges with a stud-in-hole feature;

(j) Prevent hinge-side door removal by using a Z-strip made from steel, bolted or welded to the rear face of the door. This strip is formed so that if the door hinges are removed and an attempt is made to pry the door from its frame, one leg of the Z-strip will come in 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 to extend its penetration delay time. The metal plate with a drill-resistant steel component fastened to it prevents chiselling and wire hooking of the panic bar. The drill-resistance extends 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 would virtually eliminate prying attacks.

4.343. At new facilities or when complete door replacement is needed, high-security, attack-resistant doors should be used with respect to the requirements derived from the national threat assessment or DBT.

Boundary penetration barriers

4.344. Many boundaries, such as the wall to a building, are designed with openings for windows and utility penetrations. Since these by nature 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. Window upgrades should follow the balanced design principle so that they are not the weak link in a barrier system. Standard windows provide no penetration delay to adversaries and require enhancement to provide significant penetration resistance. If a window is operable, the locking mechanism may constitute a weak link that if forced, may be opened. Where windows are installed in doors, the metal strips separating the glass have proven to be weak. The location of the window

affects the upgrading required. Windows relatively close to the ground level require more hardening than windows located several metres high. The position and operation of the locking mechanism of a window vary with type and manufacturer. The mechanism should be located so that it is not readily accessible from the exterior. The installation of more substantial locking devices or fixed windows could be considered as possible upgrade options.

4.346. The strength and weight of the frame material of a window vary widely with class of window and manufacturer. Several special window frames contain concealed materials that resist cutting tools. The frame attachment to the structure may be improved by the use of additional or heavier fasteners or by welding the frame fin, but these techniques may not affect the delay time through the window unless additional upgrades are made to the glazing materials and protective coverings.

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

4.348. Where a higher level of penetration resistance is required, thick security glass can be used. Laminated glass is manufactured as a “safety and security glass” but may not be appropriate for use in security areas. 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 are combustible and their use is restricted by fire codes. 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 is increased against forcible entry of steel tools. The impact resistance of polycarbonates approaches the same performance level as that of ‘bullet-resistant’ glass. Possible upgrades include the addition of a screen or a bar grid to the interior of the louver or glazing.

4.349. Utility ports include all types of unattended framed openings other than doors and windows. Nuclear facilities have many unattended structural openings, such as ventilating ducts, utility tunnels, crawl spaces, conveyor openings, roof access hatches, exhaust fans, and service openings that can be used as intrusion paths by adversaries. Additionally, nuclear power plant openings can also include submerged intake and discharge channels (structures) that need to be protected. Utility ports may have lift-off covers that can function as a concealed pathway and should be barricaded and alarmed. Often utility ports contain grills installed for safety or ornamental reasons that also function as barriers. The penetration resistance of utility ports may be increased by the installation of protective coverings, such as grills, bars, expanded-metal mesh, or screens. Similarly, grids and grates constructed 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 crawling through the port. Also, nested ducting or tubing can be used to preclude access into air handling ducting, culverts, or large water lines.

Specialized barriers

4.350. Specific barrier applications include temporary barrier elements that are placed during repair and maintenance or around areas that need to be protected for a limited amount of time (e.g. intermediate storage areas). Temporary barriers may include massive modular blocks (see Fig. 44), cargo containers and even parked vehicles as a vehicle barrier.

FIG. 44. Massive modular blocks.

4.351. Other specific barrier applications can offer **additional delay** directly at theft and sabotage targets and/or support the detection of sabotage attempts. These include high-strength storage room doors, double layer steel cage for nuclear materials storage/delay and specialized tie-downs; see Figures 45–48.

FIG. 45. Example of a high strength storage room door.

FIG. 46. Example of a double layer steel cage for nuclear material storage.

FIG. 47. Specialized cage tie-down device.

FIG. 48. Additional example of a tie-down device using chains.

Dispensable barriers

4.352. The two types of dispensable barriers are active and passive. Dispensable barriers may provide additional delay by increasing the adversary task time to defeat a physical barrier by complicating the tasks and can significantly increase the probability that the overall PPS will perform as desired. The dispensable material is normally stored in a compact form, and through a chemical or physical reaction, is expanded to fill the opening or space during an attack. The properties of compact

storage and rapid expansion make dispensable barriers systems attractive in certain applications. Two examples of dispensable barriers are pyrotechnic smoke obscurant (Fig. 49) and the aqueous foam system (Fig. 50).

FIG. 49. Pyrotechnic smoke obscurant.

FIG. 50. Aqueous foam system.

4.353. Active dispensable barrier systems should be reliable to operate when required, protected against disablement by the adversary and designed to eliminate accidental activation during other periods (i.e. maintenance). The system should provide a high assurance of activation during an adversary attack (reliability) and assurance of a low probability of inadvertent activation (premature activation). Health and safety issues will need to be considered related to the use of active delay systems in confined work spaces and well as other state specific safety restrictions. The deployment

of a dense obscurant in combination with concertina or razor wire can significantly increase the delay time as compared to the use of the razor wire alone. Lastly, it may be possible to benefit from the use of certain safety systems as security dispensable systems (i.e. an aqueous foam fire-fighting system may also be used as a security obscurant dispensable system).

4.354. Passive dispensable barriers installed in doors or other locations do not require remote or external activation and are attractive due to their simplicity, commercial availability and low cost.

4.355. Dispensable barriers used without other physical barriers provide minimal multiplication of the existing delay times and should normally be used with significant physical barriers to maximize delay at the target location. Dispensable barriers may provide increased delay multiplication factors for theft scenarios than for sabotage scenarios.

4.356. Any use of dispensable barriers, especially activated applications, should be closely coordinated with nuclear facility safety disciplines for installation, testing and maintenance activities to ensure personnel safety at all times.

Airborne barriers

4.357. Strategic positioning of poles, cabling or other physical barriers such as rolls of barbed tape can restrict some types of airborne threats from landing at the nuclear facility. These types of barriers can be located on the facility grounds and on building roof tops.

Marine barriers

4.358. Marine barriers may be considered to protect against the intrusion of unauthorized waterborne crafts approaching the waterway boundaries of nuclear facilities. Marine barriers may 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, which can be combined in a series to make any length. These devices are also used to identify the nuclear facility boundary. An example of a single engineered floating barrier configuration is shown in Fig. 51.

FIG. 51. Single floating barrier configuration

4.359. The engineered floating barriers can be configured in a variety of barriers and equipped with additional security devices (surface barriers, underwater nets and detection devices), see Fig. 52.

FIG. 52. Double floating barrier configuration with above surface barrier and detection.

4.360. The deployable underwater barrier may be controlled by an electric winch from remote location or central alarm station or by manual methods. These barriers can consist of screens, mesh, or other fencing materials, see Fig. 53. The underwater barrier enhances protection against penetration.

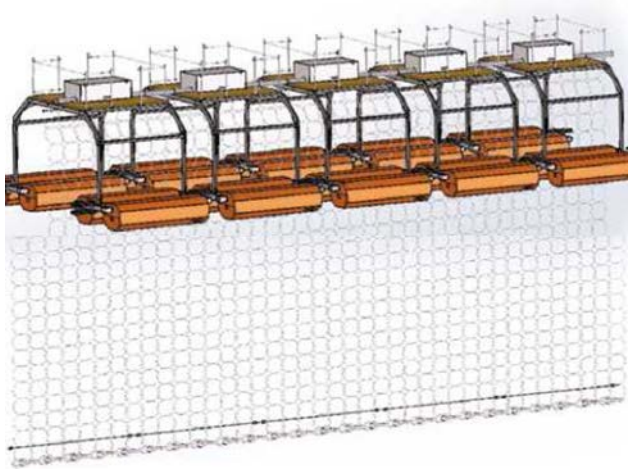

FIG. 53. Double floating barrier configuration with deployable underwater barrier.

4.361. Engineered floating barriers should normally be installed so that the barrier is fixed to the moorings on the shore and, if necessary, to seabed anchors. Due to the potential for a considerably lengthy barrier, multiple intermediate anchoring is required to adequately secure the barrier in place. The installation configuration depends on operating conditions including the depths of the water in the area around the site, wind directions and tidal conditions. Engineered floating barriers can be installed on rivers, lakes, channels, off-shore zones and other water areas. Particular attention should be given to anchoring when installing near or at the intake or discharge channels due to heavy current.

4.362. Other marine barriers may be fixed structures anchored to the shore with underwater barriers and/or detection capability, see Fig. 54. Some reinforced concrete sea walls or tsunami walls may be used as marine barriers.

FIG. 54. Marine barrier anchored to the shoreline.

Role of barriers for stand-off sabotage attacks

4.363. Mitigation measures for stand-off sabotage attacks should take into account the robustness of the engineered safety and operational features (such as reactor containment, redundancy and physical separation of vital equipment), fire protection, radiation protection and emergency preparedness measures already in place in the facility. Increased guard and response patrols may also be used at potential stand-off locations to deter and disrupt threats may be considered in addition to the use of barriers. When existing measures are not sufficient to adequately address stand-off attack, the following additional protection measures should be considered:

(a) Increasing the stand-off distance by expanding the limited access area or create larger clear zones outside the perimeter and eliminate areas of concealment.

(b) Installing structures or screens in locations to obscure line of sight between potential attack locations and the targets, thereby reducing the adversary's ability to conduct surveillance, pinpoint their planned targets, identify specific vulnerable areas, and provide the response force cover and concealment.

(c) Installation of physical barriers near or at the target to mitigate the consequences of a stand-off attack. Barriers may consist of layers of materials of different densities to make the shockwave from an explosive attack less efficient. Adding multiple spaced barrier layers outside or inside the structure may be used to cause pre-detonation, forcing adversaries to use multiple accurate attacks to achieve the desired consequences.

(d) Modifying layouts and hardening facilities by:

— Construction or relocating target storage locations underground;
— Relocation of targets within a very hardened material storage room within a weaker outer structure that when attacked collapses and entombs the inner hardened storage room; and
— Addition of thick earthen overburden to existing or planned facilities.

5. RESPONSE

EQUIPMENT

5.1. Guards and response force personnel should have the equipment necessary to perform both routine and response functions. The selection of the appropriate guard and response force equipment is based on many factors, such as the functions they are required to perform, operational or safety requirements of the facility (e.g. requirements for the use of personal protective equipment), environmental factors, and importantly, the equipment necessary to achieve the objective of preventing unauthorized removal of nuclear material or sabotage of the nuclear facility.

5.2. Depending on the threats defined in the threat assessment or DBT, other equipment may be required by a response force, which could include high calibre weapons, aircraft or vehicles equipped with weapons systems.

5.3. Other equipment that may be considered includes response force tracking systems. Tracking system technologies allow a tactical commander and response force personnel to monitor the locations of the response force and vehicles remotely. Several types of systems are in use today. These systems generally consist of a computer processer and display, a satellite terminal and antenna and transmitters and receivers. These systems include command-and-control and mapping software that displays the location of response personnel and vehicles on a computer's terrain-map display. Identification technology, known as Friend or Foe, is composed of interrogation systems to identify vehicles or personnel as friendly and determine their bearing and range from the interrogator. These also have the benefit that they can identify where security elements are during normal operations.

5.4. In addition, consideration should be given to equipment to aid in the survivability of the response force, such as hardened posts and armoured vehicles. Hardened fighting positions can be used to slow adversary forces down, but if used, care should be taken to protect positions so that they are not overrun and captured before the responders can man them. Vehicles such as aircraft or ground vehicles are valuable for reducing response time and as stable weapons platforms. If armoured appropriately, they can also protect off-site responders from certain adversary weapons.

QUALIFICATIONS

5.5. The State should provide minimum qualifications requirements for guards and response force members that are provided by the operator (as opposed to local law enforcement or military organizations). Organizations should ensure that guards and response force personnel (including candidates in training) meet qualifications that may include health, physical fitness, firearms accuracy and proficiency, procedural and policy knowledge and oral and written communications.

5.6. Training and evaluation are important programmes to ensure 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 force in interrupting and neutralizing adversaries defined in the threat assessment or DBT (see also Evaluation in Section 9).

5.7. Training should be based on established requirement, plans and procedures and be conducted in as realistic an environment as possible. This training should use a range of scenarios linked to capabilities defined the threat assessment or DBT. Training, table-top exercises, limited scope and full scope exercises (e.g., force on force exercises) are all useful tools to measure the readiness of the guards and response forces, identify areas needing improvement, and ensure plans and procedures are appropriate and effective. Training exercises should normally have elements of:

(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; and

(e) Adversary tracking.

6. NEW AND EMERGING TECHNOLOGIES

6.1. The rapid pace of technology development, coupled with new and emerging threats, necessitates the creation of a process for evaluating and implementing new and emerging technologies. If successful, the process facilitates implementation of technology that reduces cost, improves effectiveness, mitigates risk associated with new and emerging threats, and improves overall PPS functionality and capability (detection, delay, response).

6.2. Implementation of new PPS technology can be unsuccessful if personnel do not identify the best available technology to solve a problem, attempt to use a technology beyond its original design capabilities, fail to effectively integrate different technologies, or attempt to incorporate advanced technologies that are not yet mature. Technology is often acquired based on manufacturer’s assertions, but the claims can be misleading, false, or based on application in a different environment. In some cases, promising technologies are not utilized because of insufficient processes and mechanisms to identify them to fill a need or a gap, evaluate their usefulness, and expedite their deployment.

6.3. This section provides guidance for evaluating technology needs or gaps in an existing PPS, identifying candidate technologies to address needs or gaps and evaluate them prior to 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.

6.4. A State or a nuclear facility may develop a structured technology management framework to ensure new and emerging PPS technologies are seamlessly integrated with existing systems. The objective would be to identify, develop, and ensure that new/emerging security technologies are mature, work in the desired environment, and are available for use.

6.5. It is advisable that the framework:

(a) Identify research and development investments or new commercial or government technologies that will help address emerging threats and common needs,

(b) Identify technologies that best address a defined need and have undergone sufficient test and evaluation,

(c) Integrate PPS technologies at a nuclear facility to achieve overall system objectives, and

(d) Ensure the new technology is ready to be fielded at a nuclear facility.

6.6. A suggested framework for new/emerging technology management includes formalized processes for conducting needs assessments, conducting tests and evaluation activities and technology deployment, see Fig. 55. Within the proposed framework, a needs assessment is used to identify areas where technology may address existing gaps or issues, and drive research and development investments. Using a combination of market research, to identify possible technologies, and research and development investments will result in a suite of potential technologies to address future needs and threats. The next part of the framework includes processes to screen candidate technologies, and identify technologies that can be developed into or used in their current state as mature, viable, high value solutions to defined needs. The final piece of the framework includes a process to accept mature security technologies that are ready to transition to facilities as needed and that can integrate seamlessly with other security technologies.

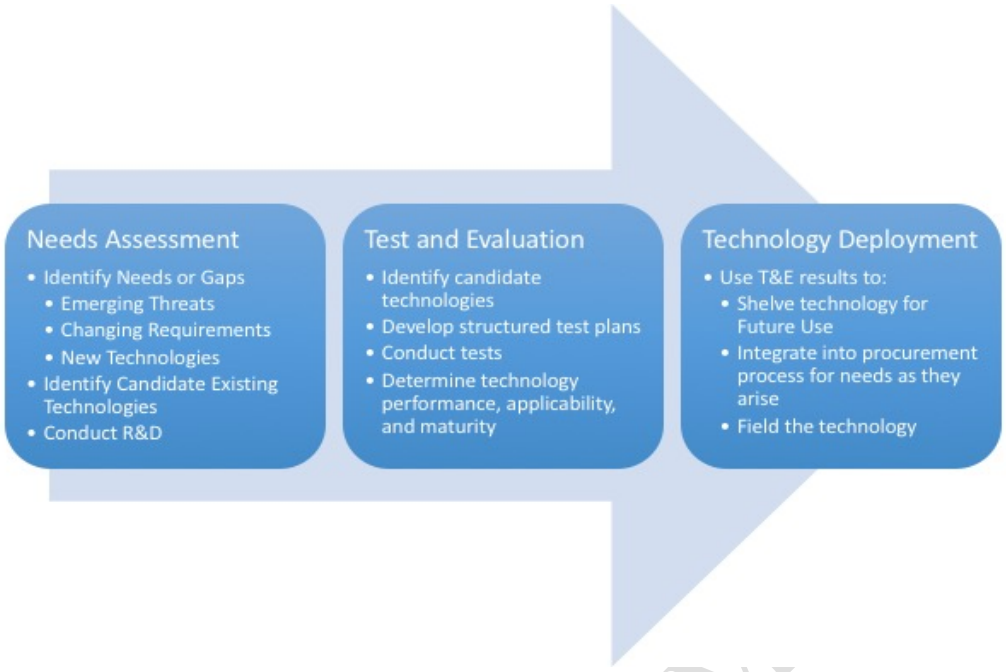

FIG. 55. Proposed technology management framework.

6.7. A formal technology management programme within a State will help ensure that new/emerging security technologies are identified, examined, and proven mature to address common needs and emerging threats. It will result in efficiencies in acquiring technologies, installing them, and maintaining them.

NEEDS ASSESSMENT

6.8. As illustrated in Fig. 56, a needs assessment is a systematic process used to determine needs, examine their nature and causes, and set priorities for future action. It focuses on the end goals or outcomes rather than the means to achieve the end. The end goals may be driven by many factors, such as changes in the threats, changes in 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 determine criteria for solutions so that decision makers can make sound decisions. It is also used to determine how best to allocate available money, people, facilities, and other resources.

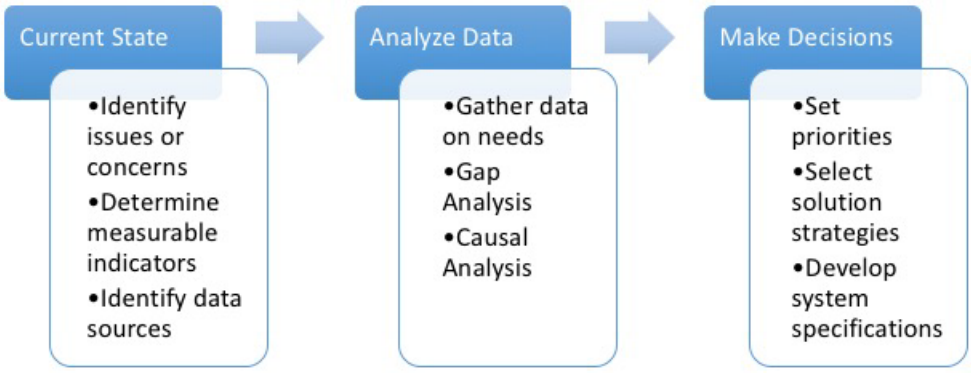

FIG. 56. Needs assessment process.

6.9. The first step in a needs assessment is determining the current state of the existing PPS and the threat. Issues or concerns are identified from a number of sources, which may include issues resulting from assessments or evaluations, from analyses of the performance of a PPS, or from changes in threat, requirements, or nuclear facility operations. It is good to develop measurable indicators regarding the issue to aid in the needs assessment. For example, the issue may be that a sensor has a tested detection probability of 0.75, and the desired performance of the sensor is a detection probability of 0.80. Sources of data necessary to analyse the issue in detail are identified.

6.10. Data are gathered for each issue in order to analyse the problem. An important component of a needs assessment is a gap analysis. A gap analysis is a technique to identify a specific area in any system in need of improvement to find gaps between a current state and a desired end state. A causal analysis is a structured analysis to determine what led do the identified issue or gap, to ensure solutions solve the real cause of the issue not just a symptom associated with the issue. For example, the sensor in the example above may have a low sensing probability due to communication issues between the sensor and the alarm communication and display system, and not due to issues with the sensor hardware itself. Replacing the sensor in this case will not address the root cause of the issue. A root cause is the basic reason why an issue or gap exists and can be quite distant from the original symptom.

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

TESTING AND EVALUATION

6.12. The fundamental purpose of testing and evaluation is to provide essential information to decision makers by verifying and validating performance capabilities documented as requirements,

assess how well a technology meets technical performance parameters, and to determine whether systems are mature, operationally effective, and suitable for intended use. During the early phases of evaluation of a new technology, testing and evaluation is conducted to demonstrate the feasibility of conceptual approaches, evaluate design risk, identify design alternatives, compare and analyse trade-offs, and estimate the ability to meet operational requirements. As a new technology undergoes design and development, the iterative process of testing gradually moves from design testing and evaluation, which is concerned chiefly with attainment of engineering design goals and verification of technical specifications, to operational testing and evaluation, which focuses on questions of operational effectiveness and suitability to address a defined need.

6.13. Formalized testing and evaluation processes originated in the testing of hardware, but the advent of computer based, software-intensive systems brings new challenges to testing that have to be addressed to conduct effective tests. Whether testing hardware or software, the constant throughout the testing and evaluation process is the need for thorough, logical, systematic, and early test planning followed by feedback of well-documented and unbiased testing and evaluation results to system developers, users, and decision makers.

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

(a) Develop test objectives;

(b) Develop pre-test plan (used to develop expected outcomes from the tests).

(c) Conduct tests, including:

— Develop detailed test plans,

— Gather test data,

— Analyse test data, and

— Document test results.

(d) Conduct and document post-test analysis.

6.15. The first step in the process is to develop test objectives. Test objectives are developed based on the results of the needs analysis, and may describe objectives related to parameters 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.

6.16. The second step in the process is a pre-test analysis of the evaluation objectives from the first step to determine the types and quantities of data needed, the results expected or anticipated from the tests, and the analytical tools needed to conduct the tests and evaluations. Considerations during the pre-test analysis can aid in determining how to design test scenarios, how to set up the test

environment, how to properly record the test, how to staff and control resources, how best to sequence the tests, and how to estimate test outcomes.

6.17. The third step is the actual conduct of the tests, and involves development of specific test plans, conduct of the tests, data gathering, data analysis, and documentation of the test results. The tests should normally be planned and executed to accumulate sufficient data to support analysis. The data should be reviewed for completeness, accuracy, and validity before being used for the final step in the process.

6.18. The final step in the process is a post-test evaluation, which is the comparison of the measured outcomes (test data) from the previous step with the expected outcomes from the second step, tempered with technical and operational judgment. This is where data are evaluated. 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 were they the result of test conditions, such as lack of fidelity in computer simulation [2], insufficient or incorrect test assets, instrumentation error, or faulty test processes. Parameters for operational environment, systems performance, and logistics support should be carefully chosen, fully described, and documented prior to test. Modelling and simulation may be used during the data analysis to support the evaluation of performance effectiveness and suitability.

TECHNOLOGY DEPLOYMENT

6.19. Technology deployment is the process used to add a new or improved technology to an existing system. The overall goal is to have a process that streamlines the deployment of PPS technology to meet requirements in a reasonable time and at the lowest possible total cost. The goals of a technology deployment programme are to use available resources to:

(a) Use the best technology available from both commercial and government sources, as applicable;

(b) Rapidly deploy the technology after selection;

(c) Refresh the technology, as needed, to maintain an effective PPS throughout the life of the system.

6.20. A technology deployment programme addresses two different objectives. The first objective is to improve/refresh an existing PPS as needed. This is intended to maintain functionality of systems or components of a PPS by updating technologies to prevent obsolescence in an existing system. The second objective is to enhance the functionality of systems or components of a PPS by upgrading functionality of a technology or adding new functionality to enhance the capability of the existing PPS.

6.21. A technology deployment programme helps address the need to sustain, add to, or enhance existing PPS capabilities to meet new requirements, address new or changing threats, or to prevent obsolescence in systems or components.

7. PPS NETWORK AND SUPPORT SYSTEMS

PPS NETWORKS

7.1. Requirements for PPS networks should be identified during the design stage and whenever modifications are planned. The design of the communication networks, power supply and other support systems, should be integrated into the PPS design. A typical PPS network overview is shown in Fig. 57. The PPS should be resistant to and provide detection of computer security attacks.

7.2. Integration of PPS networks should be done in a secure manner; however, integration and linking increases complexity of the network and may increase the methods an adversary can use to attempt to compromise the PPS network. Therefore computer security requirements for computer based systems, networks and digital systems should be taken into account from the start of the PPS network design process. Ref. [7 and 13-18] provides guidance on computer security.

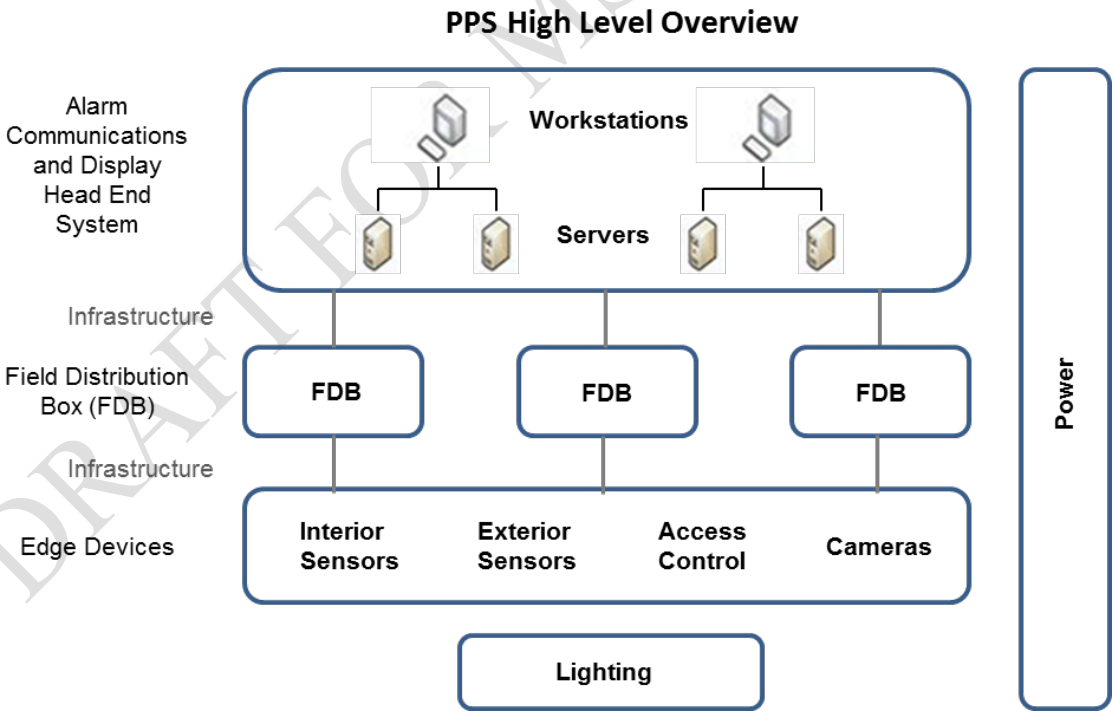

FIG. 57. Overview of a typical PPS Network and Associated Devices.

7.3. Computer systems and networks requiring protection as recommended in Ref. [1] include those used for the PPS to protect against unauthorized removal of nuclear material or sabotage, as well as those used for NMAC and safety systems. Such attacks may be aimed at acquiring sensitive

information held on these systems (see also Section 3), compromising the integrity of information held on these systems (e.g. altering NMAC records to disguise a theft of nuclear material), denying the availability of the system (e.g. disable a system important to the PPS, or preventing an alarm from reaching the CAS) or misuse a system function (e.g. unlocking a remotely operated door lock).

7.4. An important consideration in regards to PPS computers and networks is a scenario in which a system is penetrated as a precursor to a physical attack. The penetration may have occurred potentially months or years before the actual attack. If a penetration of a PPS computer system or network is detected, measures should be taken to determine if the penetration was intended to alter the system for the potential exploitation in conjunction with a physical attack at a future date.

7.5. It is important to note that there are striking differences between the types of computer systems typically used in a nuclear facility PPS; such as: information communications technology systems (which hold and transmit, inter alia, sensitive information), embedded computer systems, and instrumentation and control systems (which only contain software codes but whose integrity and availability can be very important for ensuring safety). The PPS normally interfaces with operations, NMAC, and safety, including emergency preparedness. IAEA guidance is provided for an integrated PPS [2] and for the protection of computer-based systems, including guidance on establishing an effective computer security programme at nuclear facilities [7]. Further guidance on the protection of computer based and instrumentation and control systems is given in Ref. [18].

Network design principles

7.6. PPS network designs vary depending on the size and requirements of the nuclear facility. There are many variables to consider when designing a network that will allow for flexibility and growth. Some of the most important engineering principles to take into account include:

(a) Hierarchy: Designing a hierarchical network model allows the designer to break the complex problem of network design into smaller and manageable pieces or areas. It can also aid in the design of a reliable network infrastructure which may provide a computer security benefit

(b) Modularity: By separating the different functions that exist on a network into modules, the network is easier to design. Modularity may also lead to a more stable operability so that failure of one functional area (for example a zone or function) will not lead to the total system failure.

(c) Resiliency: The network should remain available for use and perform a required function under given environmental and operational conditions (both normal and abnormal) for a stated period of time. Normal conditions include normal or expected traffic flows and traffic patterns, as well as scheduled events such as maintenance windows. Abnormal

conditions include hardware or software failures, extreme traffic loads, unusual traffic patterns, denial-of-service events, whether intentional or unintentional, and other unplanned events.

(d) Flexibility: The ability to modify portions of the network, add new services, increase future network capacity without going through a major upgrade (i.e., replacing major hardware devices), or to allow for potential changes in the operation process.

(e) Network integrity: Network components should have limited tactic-technical possibilities and service life. At the same time, maintenance of network integrity helps ensure that the system continues to provide its security and is not changed without approval. Methods of integrity maintenance include the features of the design for: denying the access to the equipment and denying and detection of access to information.

(f) Complexity: The degree of complexity of the network should be balanced with requirements of the nuclear facility regarding the protection requirements and the existing organization resources

7.7. During PPS network design, the requirements of information security and physical protection of communication lines and network nodes should be considered. The system should have means of detection and registration both of explicit and implicit failure of components (devices, algorithms, signals) [7]. Special attention should be given to the protection measures at the respective zone boundary (such as firewalls and limitation of data traffic) as well as physical and administrative controls.

7.8. The system design should consider the quality and the operating environment rating of the components to be installed within manufacturer's specifications. Failure modes should be evaluated to understand the extent of the outage due to potential failure(s). For example, in a 'tree network' all components attached to a 'branch' are affected, while the other branches remain unaffected. Installing redundant equipment on the same network branch would result in both sets of equipment being affected by the same outage.

7.9. Data communication networks use different types of topology, or architectures, to transmit information from one device to another. Network topology is a method for connecting devices in a single computer network. The type of topology selected determines the cost, robustness and reliability of the network. Different network topologies are available to address different needs or requirements.

Communications network

7.10. PPS communication (data) networks and devices should interact with the overall PPS. An automated PPS design should separate critical functions such as perimeter intrusion detection,

perimeter monitoring, and access control from other facility networks. The separation of functions will provide for the necessary architecture that improves computer security measures.

7.11. An automated facility PPS may consist of:

(a) Alarm data acquisition and processing system (display and assessment equipment) used for intrusion detection system control;

(b) Access control system including automated systems for assigning authentication and identification of 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.

7.12. The PPS subsystem devices mentioned above generate, receive and process a range of types of signal (sensor annunciation, video for assessment, access control communications, and overall system status). For PPS subsystems, all the communication elements can be integrated in a single or several networks. Integration into a network permits the transfer of information from periphery devices to computers that perform the function of servers for processing input data.

7.13. Data communication networks may consist of:

(a) Physical protection devices (detectors, cameras, alarms);

(b) Periphery devices interacting with users (biometrics, electromagnetic door locks);

(c) Controllers of devices providing signal processing from several detectors;

(d) Distribution devices (switchers and routers);

(e) Database servers that process the signals from intermediate distribution devices; and

(f) PPS equipment workstations (CAS, guards and other response).

7.14. Redundant and diverse data communication paths are a good practice, where systems are commonly designed such that the second system can automatically assume control upon loss of the primary system. Redundancy provides a more secure communications system by forcing an adversary to defeat or compromise two separate communications paths instead of one.

Encryption methods

7.15. Data encryption may be necessary if physical access to PPS cable or communications lines cannot be controlled. However, encryption can present a significant drawback due to the communication delay for signal encryption and decryption. Risks arising due to increased response

communication time 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 the computer systems according to importance [17].

Transmission technology

7.16. The wiring sub-systems of a PPS are divided into signal networks and power supply networks. The PPS and lighting sub-systems should be operated using an uninterruptible operation approach; i.e., alternate or backup power sources are needed.

7.17. PPS data communication can be achieved using different equipment: wire, optical fibre or, in rare exceptions, wireless links (see Table 5 below). Cable/wire communication lines are currently used as the main method of data transfer. Wireless signals are extremely vulnerable to attack, especially denial of service (availability) [7].

7.18. There should normally be no wireless communication functions implemented in a PPS assigned to the highest security level as it is difficult to provide a secure boundary for such communications [7]. However, ultra-high reliable wireless networks are an emerging technology, becoming more robust and reliable and may become a more viable option for future use. A typical wireless sensor system consists of one or multiple sensor/transmitter units and a receiver unit.

7.19. Some of the concerns when considering the use of a wireless sensor system include collisions, signal fade, interference and jamming. Collisions occur when two or more signals, such as state-of-health, are received simultaneously, resulting with neither message being read by the receiver. Signal fading can occur when the path between the transmitter and receiver is too far or is blocked by too much material which shields the signal, such as large metal objects or metallic building siding. Interference occurs when other sources transmitting in the same frequency range overpowers the signal sent by the sensor/transmitter unit. Jamming is similar to interference and can be initiated by an adversary so that alarm signals do not reach the receiver. In addition there is a large risk of interception and falsification of wireless signals.

TABLE 5.WIRE METHODS AND TYPES

Method	Type	Advantage/disadvantage For use in PPS network
Wire • Coaxial • Twisted pair	electrical pulses (voltage) e.g. RJ45 RS-232 (a communication standard) or Category 6 cable	Conventional method - Used in television and radio equipment - High degree of noise resistance and great mechanical strength RS-232 has a limited maximum cable length 15m (Standard Cable) to 300m (Special cable)
Optical fibre • Multimode • Single mode	light pulses Several rays or modes Single ray or mode	- 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 is 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 - Long cable runs may cause signal loss - 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 unavailable - 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

PPS SUPPORT SYSTEMS

Power and backup systems

7.20. The purpose of the power system is to provide a reliable power source for physical protection systems and subsystems during routine and emergency conditions. Redundancy allows components to fail without catastrophic consequence. Depending on power supply design requirements, electricity may be supplied by one or a combination of the following methods:

(a) Off-site commercially available power;

(b) Uninterruptible power supplies (UPSs) and batteries;

(c) Standby generators.

7.21. For the most sensitive facilities it may be desirable to have two separate off-site power feeds to reduce the likelihood of power interruption. The off-site power feeds should not be collocated to ensure that a single event does not result in power interruption. PPS power considerations include:

(a) Choosing the power supply and capabilities based on the power consumption requirements;

(b) Accounting for the power distribution network (power lines, distribution cabinets, connections, and conduits) including loading requirements for all PPS components and subsystems.

7.22. If off-site PPS power is lost, an UPS should provide near-instantaneous electrical power to support the continued operation of PPS equipment designated as critical; i.e. sensors, alarms, communication components, and surveillance cameras. An UPS, which is normally battery powered, provides temporary electrical supply to the PPS until the automatic transfer of the electrical load from normal power to the emergency power, usually consisting of an emergency generator(s). An audible and visual indication of power failure and subsequent restoration should be provided to the CAS or alarm station including indication of emergency generator status, when available. Perimeter lighting typically does not operate from the UPS or battery power sources. However, the UPS and backup generators provide a potential avenue to attack PPS systems and should be subject to protection measures, including computer security.

7.23. Protection considerations for standby power may include:

(a) Installation within a controlled area or hardened building inside the perimeter (in some cases a vital area);

(b) Installation of sensors to detect tampering and unauthorized access;

(c) Automatic start or energizing, upon failure of the primary power;

(d) Performing routine maintenance testing under load to ensure efficiency and effectiveness;

(e) Performing routine checks of output voltage to address the initial power surge;

(f) Monitoring of UPS batteries and charging systems from the CAS or alarm station, including battery recharging time;

(g) Defining safe load and time required for the PPS equipment to operate on backup power; (adequate fuel storage and supply)

(h) Providing adequate capacity to power the PPS, CAS and backup station; and

(i) Providing power to computer security equipment to ensure continued operation.

7.24. Network backup switching capability provides redundancy for PPS network equipment operation in case of damage to a network element. The backup network capability mitigates the 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, as opposed to redundant systems that typically use identical equipment and software, which are more likely to have common vulnerabilities.

Location and protection requirements for stationary equipment

7.25. Maintenance workstations used for PPS equipment and network devices (server) should be located in an access controlled area; e.g., located in locked, alarmed and controlled cabinets or rooms. A two-person rule is suggested for access to network servers and workstations to provide administrative protection of equipment and to ensure configuration management.

Protection considerations of network cables

7.26. All PPS signal cables or lines should be located within the secure side of the protected area boundary in order to restrict access, if possible. 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, it is advisable to enclose or bury conduits underground.. Normally cables will be exposed at both terminal locations and this is where the cabling is most vulnerable to attack.

7.27. The communications cables and lines used for transmitting sensitive information should also be controlled and monitored by computer security measures to ensure signal and line integrity is maintained and to provide an indication of potential malicious activity or component failure [7].

Tamper protection

7.28. Tamper protection should be incorporated in the hardware and system design; e.g., sensors to detect an intruder approach to the equipment or lines. Tamper protection and/or line supervision should be utilized for the following applications:

(a) sensor electronics and junction box enclosures, with tamper switches that alarm if opened,

(b) alarm communication lines, with some type of line supervision to detect lines that have been cut, disconnected, short-circuited, or bypassed; and

PPS network maintenance and testing

7.29. PPS network devices are continuously exposed to operational conditions that can reduce the life of the components (e.g. weather conditions, mechanical impact, voltage variations and radiation fields). Periodic preventive maintenance of the physical protection network will increase PPS availability (service) and extend the operational life. An in-service PPS should also be subject to computer security measures.

7.30. PPS network maintenance can be preventive (scheduled) or emergency (unscheduled, or associated with an outage or deviation from specifications of system elements). To monitor performance, periodic maintenance and operability tests are necessary to ensure continued operability, reliability, availability and effectiveness of the network to collect and communicate the data from the automated physical protection subsystems.

7.31. Each facility should establish procedures and schedules for the preventative maintenance of PPS network systems based on the type of equipment installed, conditions under which the equipment operates and the maintenance history of equipment.

7.32. Consideration of the life-cycle of PPS network components and systems should be performed to ensure that components are replaced before end-of-life failure, with the schedule of the end-of-life failures based upon the stated or historical operational lifetime. The following activities facilitate recovery in case of unpredicted failures:

(a) Modular design to allow for rapid replacement and return to service.

(b) Frequent back up of the databases and system configuration;

(c) Documented recovery procedures to return the network to full operability after an outage; and

(d) Availability of original or compatible spare parts and equipment (monitor vendor changes).

8. PERIODIC EQUIPMENT TESTING

TYPES OF TESTING

8.1. Periodic equipment testing includes acceptance and sustainability testing. Several types of periodic equipment tests will be described here that serve these need including:

(a) Pre-acceptance testing, performed during installation to ensure that all hardware and software components are operational and interacting,

(b) Acceptance tests, performed to demonstrate that installed components or systems have been implemented as designed and will operate as designed,

(c) Operability tests, performed to indicate that physical protection components are functional, and

(d) Maintenance and calibration tests, performed to determine whether the PPS components and subsystems are correctly installed, aligned, and calibrated.

8.2. These different types of tests may be performed as separate and distinct processes, be combined to as part of a comprehensive testing and maintenance process or support a quality assurance programme as part of an integrated management system (see Section 11). For example, operability tests may be performed once a day on a certain PPS element as a distinct process. At the same time, the same element may undergo operability and calibration testing after maintenance, prior to acceptance testing. If the element passes all tests it would be placed back into operation. The following sections describe the types of tests in more detail.

PRE-ACCEPTANCE TESTING

8.3. Following the installation of new physical protection systems and sub-systems, all physical protection components should undergo pre-acceptance testing to ensure that all hardware and software components are operational and interacting. This process includes point-to-point testing along the entire network to ensure that all alarm communications are functioning and report to a central alarm station or other location, as necessary. The process would include all hardware, software, voice and data communications, lighting, power and backup systems. This testing is typically part of the construction phase and is conducted prior to formal handoff to the facility organizations.

ACCEPTANCE TESTING

8.4. Acceptance tests should be performed to ensure that the PPS elements are fully functional in all aspects of operation and meet design specifications prior to acceptance by the operator. Testing should include all system and sub-system components of the PPS. Acceptance testing is the most encompassing testing because proper installation should be checked while at the same time baseline performance and operability should be determined and documented. Acceptance tests are intended to uncover operational and functionality issues that should be addressed to ensure system operation in accordance with design specifications and requirements. This type of testing would include all PPS hardware and software, voice and data communications, lighting, power and backup systems.

8.5. Acceptance testing activities should be thoroughly planned and documented in an acceptance testing plan that defines the testing objectives, scope of testing, approvals for testing, responsibilities, testing approach, fault and data recording, resource specifications, testing environment and

identification of each planned test. Test plans should be developed to include specifications, a description of the test, initial hardware/software testing conditions, detailed test procedure, expected results, and any special instructions as necessary. An effective acceptance test plan requires design specifications that have been clearly defined, measurable, and readily tested.

OPERABILITY TESTING

8.6. Operability tests are intended to ensure that PPS elements such as components and subsystems initially function upon installation and subsequently continue to function and operate properly. During operability testing, there is no intent to defeat the PPS component/subsystem or to determine how well the component works, but simply to confirm operation.

8.7. As an example, guards might be assigned to periodically walk through a portal metal monitor to determine whether or not metal items they normally carry cause a visual and audible signal, as required. Another operability test is that of a door balanced magnetic switch that might involve assigning a guard to open the door and to confirm an alarm is received. Operability tests may also be applied to subsystems. For example, a guard patrolling a barrier monitored by a volumetric intrusion sensor with CCTV may be assigned to walk into the area covered by the sensor to confirm an alarm is received. Personnel in the CAS would then determine if the sensor alarmed, if the appropriate camera was activated and whether the quality of the camera image displayed was sufficient to determine that a human set off the alarm.

8.8. Operability tests should normally be performed on a fairly frequent schedule, perhaps as often as once every shift or as infrequently as once per week as appropriate, to ensure continuous operation of those components and subsystems. Problems identified by operability tests should be promptly corrected.

8.9. Operability tests can be performed manually by a human tester, or by using remote or self-testing capabilities. An example of a manual test is the balanced magnetic switch test described above. Another manual test might involve a technician inspecting a perimeter after a storm to determine if sensors or cameras have been damaged or appear to have been moved out of alignment.

8.10. Manual testing of PPS components is strongly preferred, but in certain instances, due to manpower limitations or remoteness of intrusion detection systems, manual testing may not be possible or practical. In such cases a capability for remote or self-testing might be used where the functionality to test the trigger/initiating signals are provided by the alarm communication and control system itself As an example, a self-test might begin with the intrusion detection system generating a test trigger to a specific sensor at a random time. The sensor would then be expected to respond with an alarm. The intrusion detection system would subsequently check that the alarm occurred within a specified time and was properly cleared by the operator within a specified time. Failure to pass a

remote or self-test should produce an alarm message, indicating possible hardware failure or tampering. Current remote or self-test techniques may identify that the sensor is still working, but do not test the sensor to verify proper calibration or alignment. In this case, a remote self-test should supplement, not replace, other forms of manual testing.

MAINTENANCE AND CALIBRATION TESTS

8.11. Maintenance and calibration tests are conducted to determine whether the PPS components and subsystems are correctly installed, aligned, and calibrated based on requirements and specifications. Such testing would also be conducted as part of, or in conjunction with, initial acceptance testing or following P maintenance activities. As an example, a maintenance/calibration test of a metal or radiation portal monitor may involve a series of walk-throughs using a specified test source to demonstrate that the detector has an acceptable detection probability against the source. Another example may involve using a trained technician to perform 30 tests of a perimeter sensor using a combination of walking, running, running, jumping, bridging or crawling (as appropriate) techniques to meet a requirement that the sensor provide a probability of sensing of 90 percent with a 95 percent confidence level. Still another test might involve a technician mapping out the sensing area of an interior sensor by slowly walking towards the sensor at 15 degree intervals.

8.12. Properly 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 may have been tampered with. A key requirement for maintenance and calibration tests is that they can be conducted in a consistent, repeatable fashion. The consistency/repeatability is important to ensure that the reason a device passed the test on one day but failed the test the next day was due to some degradation of the device performance as opposed to some variation in how the test was conducted. Consistency and repeatability may be achieved by providing a detailed set of procedures and training programme for the tester and/or by use of an approved testing device that simulates an intruder crossing the sensor (for example, using a tool to tug at fence fabric with a consistent force to simulate a climber).

ON-SITE TESTING

8.13. Due to unique facility design or environmental conditions the facility should conduct on-site performance testing to establish and/or validate the values used in effectiveness assessments, see Section 9. If the facility is active, detailed coordination is required between facility operations and security to ensure protection measures are maintained during the testing period, including through previously approved compensatory measures. If a deficiency is identified through testing or a protection element is defeated as part of a test (i.e. fence is cut), as soon as testing is completed,

compensatory measures should be implemented and corrective actions initiated. The compensatory measures should remain in place until corrective actions are completed.

USE OF DEDICATED TEST BEDS

8.14. Performance testing performed through the use of dedicated test beds located at the facility or at another testing location. Test beds are useful to determine and/or validate PPS component effectiveness over a wide range of conditions and defeat mechanisms. A dedicated test bed allows testing under realistic conditions without impacting facility operations or security. The test bed may include facilities to test interior and exterior PPS systems and an infrastructure to support sensor testing, data gathering, and data recording. The test bed may include access control systems, delay systems, contraband detection, lighting, assessment, power distribution, as well as alarm communications, monitoring and recording systems.

8.15. One benefit of using a test bed located at a facility is the feasibility of testing and monitoring PPS measures under facility-specific environment 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 weather conditions.

8.16. A dedicated test bed may also be used to determine 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 proper site-specific maintenance and calibration tests. Dedicated test beds are also useful when defeat testing of a barrier or intrusion detection system may be prohibited due to cost or facility constraints where personnel safety is a concern, such as high radiation or contamination areas. Such tests provide the data required to develop specific physical barrier delay times.

8.17. 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 breaching techniques from hand tools, power tools, explosives, and vehicles, as applicable.

9. PPS EVALUATION

9.1. A PPS evaluation is conducted to determine whether the PPS meets prescriptive requirements and/or performance objectives. The methods and programmes used to gather, analyse and manage the data directly influence the validity of the PPS evaluation. During a PPS evaluation, all physical protection measures including people, plans, procedures, and equipment, should be included to

determine if 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 may be specified differently by a State, but generally include:

(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 measure(s) are in place. For example, "a 2.4 metre chain-link fence is required on the boundary of the limited access area." Note that the prescriptive requirement may also include performance standards that are measured in technical terms, not in terms of effectiveness against the threat assessment or DBT.

(b) A performance-based regulatory approach where a requirement is specified in terms of the overall objectives of the entire PPS against the threat defined in the threat assessment or DBT. As an example, a performance-based requirement could be to prevent theft of category I nuclear material from a specific threat with rifles, bulk explosives, and a commercial vehicle. Another example may be a requirement to detect an intrusion of a facility containing a category III quantity of nuclear material and report to the local police immediately and the competent authority within 24 hours.

(c) A combined regulatory approach, where some requirements may be defined in terms of effectiveness against the threat assessment or DBT, and some may be defined in terms of presence or absence of one or more specific measures that the State requires (perhaps meeting associated technical standards). Some requirements may also have a combination of these two aspects.

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

9.4. Measuring the effectiveness of a PPS designed to meet performance requirements, in many cases, requires the conduct of performance tests, such as exercises [2]. Performance testing is not possible for a facility under design; so other methods, such as the use of simulations may be used. The evaluation of performance requirements may include both direct comparative reviews along with independent testing to validate that the 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 may be necessary, along with notification to the competent authority, as required. A PPS evaluation can also be used to:

(a) Improve the PPS by increasing effectiveness through identifying efficiencies and deficiencies;

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

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

9.6. An IAEA-sponsored activity, such as an International Physical Protection Advisory Service, or other independent review could also be considered to support a facility PPS evaluation programme.

PRESCRIPTIVE VERIFICATION

9.7. Using the prescriptive method, the State establishes specific physical protection requirements to meet its defined physical protection objectives for each category of nuclear material and each level of URC [2]. These requirements provide a set of ‘baseline’ provisions or criteria for the operator to apply to each category of material and each level of URC.

9.8. Prescriptive requirements can generally be evaluated by direct observation, measurement or examination of records and PPS element testing. Examples of prescriptive requirements include:

(a) A specific feature (e.g. wall, fence, and camera) must be present.

(b) A physical protection measure must meet directly measurable parameters (e.g. wall thickness is more than X cm; fence height is more than Y m.).

(c) Physical protection equipment must receive some type of certificate or other officially recognized documentation to confirm its specification.

(d) Guards must have certain qualifications, possess specific types of equipment and are knowledgeable in their use.

(e) A perimeter sensor should be designed, operated and periodically tested to ensure that it provides a probability of sensing of X% with Y% confidence against a person walking or running.

9.9. An evaluation of a PPS against prescriptive requirements should always be performed before other required evaluations can proceed; e.g., 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 or specifications, gathering information, and then comparing the information against the requirements to determine compliance. The following evaluation 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 with designing, operating, managing, and maintaining the PPS. Interviews may 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 regarding 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 may also be required where a prescribed measure must meet some technical quality level or specification.

9.12. Determining which PPS component/measure to performance test may be based on facility operation, testing schedules or a requirement by a competent authority. In addition, specific measures may be tested based on lessons learned, results of previous assessments, security incidents, or other information indicating a potential weakness in the PPS.

9.13. There are different reasons for performance tests of individual physical protection measures or a combination of PPS measures, including:

(a) Tests to determine performance metrics (such as detection probabilities and delay times) representing how well physical protection measures perform against adversaries with varying levels of capabilities, as specified in the threat assessment or DBT;

(b) Tests to determine defeat methods of technical measures and subsystems (may be used to support fault tree analyses to understand how the measures and subsystems can be defeated).

9.14. Other factors to consider for the performance test/exercise programme supporting a PPS evaluation include:

(a) Developing a plan to validate compliance with requirements and performance of the PPS. The plan should provide a basis for the design, frequency and criteria for the performance testing programme and the evaluation. The plan should ensure the evaluation verifies that criteria for reliability, operability, readiness, and performance are met.

(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 facility organizations (emergency response, facility personnel, and control room staff) into the exercise to add realism and determine if these different disciplines can work together during a security event.

(d) Documenting results of the evaluations, including corrective actions, and where appropriate reporting the results and findings to the competent authority.

(e) Engaging with other nuclear facilities to share lessons learned and best practices, including the process of conducting evaluations and the results.

9.15. A nuclear facility should implement a PPS performance testing programme that makes use of other ongoing testing programmes conducted by nuclear facility maintenance personnel, as part of the quality assurance programme, to make efficient use of available data. A Performance testing programme should have elements to coordinate the test design, planning, conduct and management of the data derived from the tests, including:

(a) Integrating data from other testing programmes, such as maintenance and training to determine common testing objectives and methods to maximize the utility and relevance of test data.

(b) Ensuring the necessary resources are integrated with the facility operational schedules to minimize disruption.

(c) Documenting test plans to establish the objectives, standards, methods and procedures 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 and with the appropriate established procedure.

(f) Preforming 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) Identifying and documenting a data management plan to guide the effective collection, analyses and maintenance of the test data.

9.16. Performance tests should be repeatable and impartial. To be valid, testing by different experts using the same test plan should yield comparable results. Test methodology should be well structured to ensure the most efficient and accurate use of individual test results and observations. Use of established international standards, such as ISO/TC 69, Applications of Statistical Methods, provides additional best practices in the appropriate use of data sampling and test design.

Performance evaluation methods

9.17. Performance tests used for evaluation include limited scope and full scope exercises (e.g., force on force exercises) are designed to determine whether personnel, procedures, and equipment provide required levels of performance. These tests may be designed to examine performance of a single physical protection component, or of a larger subsystem of the overall PPS. An example of a limited scope test would be an exercise to collect response and assessment times for a particular target. Another limited scope test might be designed to validate that an alarm station operator can interact with the intrusion detection system to properly identify the source of an alarm in a storage area within a designated time.

9.18. When practical, multiple performance tests may be conducted for each physical protection element to gather a range of test data to ensure that a representative sample is collected. As an example, three exercises might be performed to determine response times, one for each of the three shifts of responders. The use of video can be very useful to record test data.

9.19. Performance testing data may be maintained in a data library which can then be used as a basis to justify probabilities of detection and assessment, delay and response times used in physical protection evaluations. See also Section 8 for further information on collecting test data.

Limited scope performance tests

9.20. Limited scope performance tests may be conducted to test any operation or procedure, verify the performance of a policy, or verify a requisite knowledge or skill. While other evaluation techniques such as observations and interviews may not require a test plan(s), limited scope performance tests should be formally documented and approved prior to conduct. 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 may be

either scheduled or unannounced. During any evaluation process it is best to use multiple testing techniques to determine if personnel assigned to PPS activities are performing their assigned functions effectively.

9.21. One advantage of limited scope performance tests is that many PPS measures can be evaluated without the disruption of facility operations or without large resources and personnel. Limited scope performance tests can include the direct observation of a specific activity or process or can include the evaluation of specific actions or response to an anomalous condition. Limited scope performance tests can also provide an indication of a specific protection capability, while multiple tests for a series of actions can provide an 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. A full scope performance test, or force-on-force exercise, is a major, integrated test designed to evaluate all the elements employed in response to an attack from a specific threat at a facility. Full scope exercises are the best method to realistically evaluate and verify 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 to identify areas requiring improvement.

9.24. Full scope exercises require extensive planning and coordination with all organizations at a nuclear facility including management, facility operations, those with physical protection responsibilities, as well as with emergency and off site response entities. They are also demanding and costly, so careful planning and coordination are required to maximize the benefit. An effective tool for full scope exercises is the use of simulated weapons to collect adversary and response force engagement data during the exercise. An overall exercise plan should be used to plan, coordinate, implement and record meaningful data of a force-on-force exercise. While there are numerous topics that may be included, a force-on-force exercise plan should normally include the following topics:

(a) Clear test objectives;

(b) General and specific attack scenario descriptions;

(c) Specific adversary threat (from threat assessment or DBT);

(d) Facility(ies) involved and exercise boundaries;

(e) Compensatory measures to protect the facility during the test, including a shadow force (additional actual armed response force in standby), if required;

(f) Measures to ensure sufficient protection of 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; and

(i) Schedule.

Scenario Development

9.25. This section provides an overview of a scenario development process used for specific scenarios in performance testing and during analyses to determine the effectiveness of the PPS against a defined threat. A force-on-force exercise needs development of a specific attack scenario. During this process, the intent is to use subject matter experts to develop a range of scenarios to address the threats defined in the threat assessment or DBT. These scenarios may include external threats, insider threats or external threats in collusion with insider threats. Information used to develop scenarios is derived from many sources, including:

(a) Characteristics of the nuclear facility;

(b) Characteristics of the specific theft or sabotage targets;

(c) Characteristics and capabilities of the threat;

(d) Results of previously completed analyses, such as the results of a path analysis; and

(e) Other factors as applicable.

9.26. Some considerations for developing adversary scenarios include:, the capabilities of the adversaries, which is a combination of tactics to be used, such as force, stealth, or deceit; different facility operating conditions at the time of the attack (e.g., nuclear material vault open or closed); the amount of information an adversary force may have; and actions of an insider in a collusion scenario.

9.27. Once a range of scenarios have been developed, a process should be used to select a scenario or scenarios that will be tested in a force-on-force exercise or during the PPS evaluation. Considerations for selection include identifying: a ‘worst case’ scenario; bounding scenarios (e.g. scenario B is a more difficult test of the PPS, and includes elements tested in scenarios A and C); or selecting a scenario to test a specific feature of the PPS or testing a range of scenarios over time. It is important to ensure that no matter which scenario is selected, the testing objectives can be met.

9.28. Selecting the scenario to test is very important, as the results provide information regarding the PPS effectiveness. In some cases, a PPS may perform better against attack scenarios that appear

more challenging, and not perform as well against scenarios that appear to be less challenging. For this reason, evaluating a range of scenarios provides a better indicator of the effectiveness of the system. Other methods to conduct scenarios evaluations include table-top exercises and computer simulations.

10. PPS ANALYSIS

10.1. This section describes the analysis process and methods used in terms of evaluating the results of performance tests, models and simulations to determine the effectiveness of a PPS in meeting established performance requirements including:

(a) Path analysis – a method of evaluating potential adversary paths and determining the probability a response force can interrupt the adversaries before their goal is accomplished.

(b) Neutralization analysis - a method of determining the probability a response force can stop an adversary before their goal is accomplished or by causing an adversary to abandon the attempt.

(c) Insider analysis – a method of determining the effectiveness of the PPS against a malicious act by a person with authorized access at a nuclear facility.

(d) Scenario analysis – a method where a specific attack plan (scenario) is developed and the PPS is evaluated to determine its effectiveness against it.

10.2. The ultimate objective of an analysis of the effectiveness of a PPS is to determine the likelihood that it will protect appropriately against theft of nuclear material or sabotage of the nuclear facility. Performance testing is the most important method to acquire information regarding the effectiveness of a PPS, and the results can be used to support the analysis methods defined in this section. As an example, performance testing can be used to determine the probability of detection of a perimeter intrusion detection system at a nuclear facility. This data can then be used to conduct a path analysis [2], which is a comprehensive analysis of all potential paths from outside the nuclear facility to the target. There are other methods, such as force on force results that can be used along with the results of performance tests to determine the effectiveness of a PPS against defined threats.

10.3. The primary objective of the PPS functions of detection and delay are to facilitate a timely response to a malicious act. The objective of the response function is to interrupt and neutralize or 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). System effectiveness takes on the form of the following Eq. (1):

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

where:

— P_E is the measure of the probability the PPS meets its performance requirements.

— P_I is the probability that the response interrupts the adversary, where interruption is defined as the event when a sufficient number of appropriately trained and equipped members of the response force arrive at the appropriate location in time to stop the adversary's progress toward completing a malicious act.

— P_N is the conditional probability that the PPS defeats the adversary given that interruption occurs.

10.4. Path analysis focuses on evaluating P_I, where P_I depends upon the relationship between detection capabilities, delay times, and the time between first sensing of the adversary and a timely response to evaluate whether these forces are in position to interrupt the adversary. Neutralization analysis focuses on evaluating P_N, which depends on response force weapons, training, and equipment compared to the adversary weapons, training, and equipment. Neutralization analyses are heavily influenced by legal and regulatory requirements as well as the quality of response plans. Path and neutralization analyses each consider a variety of factors to determine potential or real weaknesses; assess whether performance requirements for P_I and P_N are met; and determine if there is defence in depth and balanced protection.

PATH ANALYSIS

10.5. Path analysis determines P_I for each credible adversary path to the target to assess whether there is high assurance that an adversary attack along any of these paths will be detected while there is enough time remaining in the adversary task time for the response force to interrupt the adversary. The path analysis process identifies adversary paths having the lowest P_I; such a path is called a most-vulnerable path or critical path. The effectiveness of the PPS design in providing interruption is measured as P_I for a most-vulnerable path. If P_I is inadequate along the most-vulnerable path then the PPS design will be considered inadequate. P_I is determined for a single path using timelines such as those shown in Fig. 58.

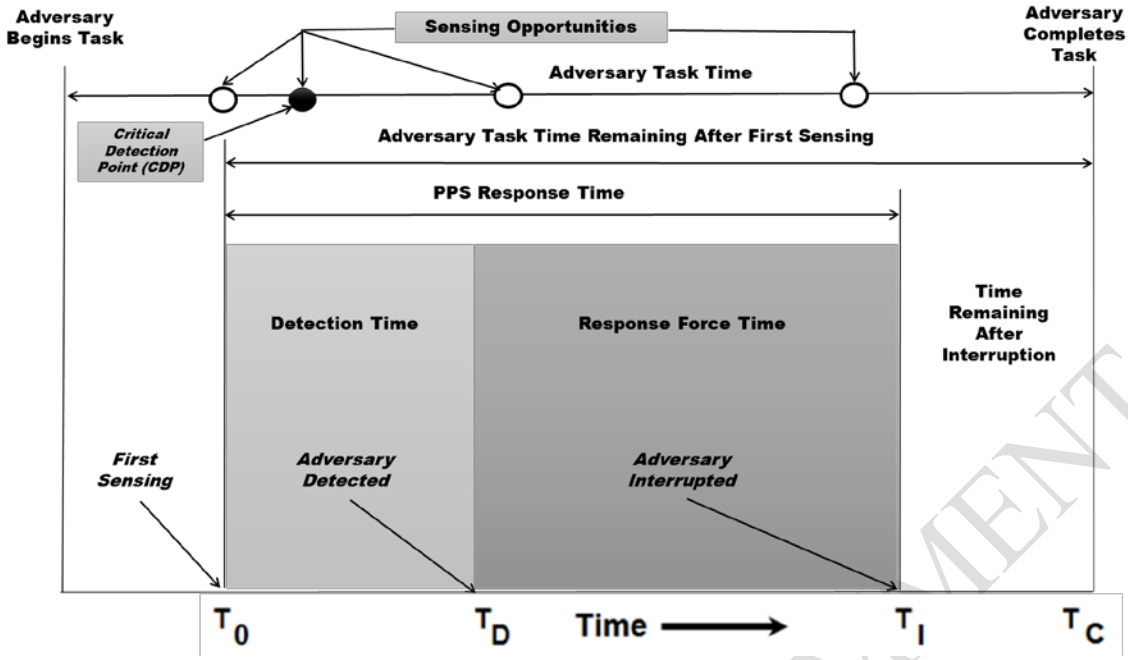

FIG. 58. Comparison of adversary and response force timelines.

10.6. Figure 58 shows the adversary 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 may cause 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. Note that the last timely sensing opportunity is called the critical detection point. Below the adversary timeline is a comparison between the PPS response time and the adversary task time remaining on the path after first sensing at each possible sensing opportunity. The adversary task times 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 to be timely if the PPS response time is less than the adversary task time remaining after first sensing; otherwise the sensing opportunity is not timely. In Fig 58 the first two sensing opportunities are timely. Probability of Interruption, P_I, is computed as the probability that the adversary is detected at one or more of the timely sensing opportunities on the specified path. If there are K timely sensing opportunities then P_I is calculated from the following Eq. (2):

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

where:

— P_{Di} is the probability of detection associated with the sensing opportunity.

— K is the number of timely sensing opportunities.

— i is a single timely sensing opportunity.

10.8. Path analysis applies this P_I calculation conceptually to every path to the target. The set of paths to be evaluated are defined in terms of concentric layers of protection around a particular target. As an example, Fig. 59 depicts a hypothetical facility with two layers of protection around a single target.

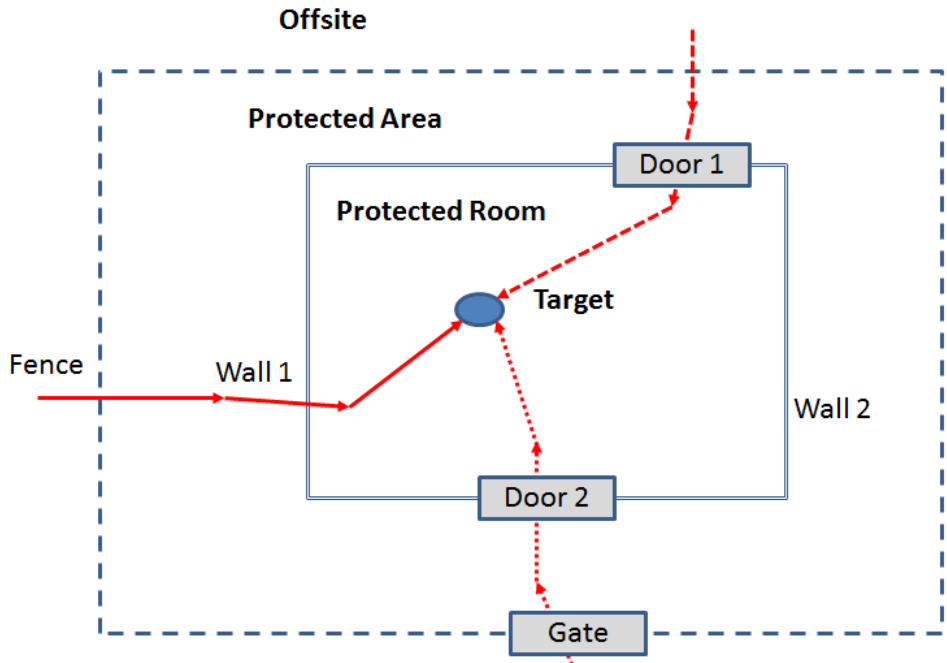

FIG. 59. Three adversary paths indicated on a hypothetical facility with two protection layers.

10.9. The protected area layer consists of two elements, a gate and a fence, while the second protection layer consists of 4 elements: Door 1, Door 2, Wall 1, and Wall 2. There are then 8 paths to the target starting with path {Fence, Wall 1, and Target} and finishing with {Gate, Door 2, and Target}. During path analysis of this hypothetical facility P_I for each of these 8 paths would be computed and the path with the lowest P_I would be identified as the most-vulnerable path. If that P_I value was sufficiently high then this PPS might be deemed to provide effective interruption capability at this target.

10.10. Besides 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 fall before or at the critical detection point on all paths. For example, the hypothetical facility in Fig. 59 may not have defence in depth if only one layer is timely; that is, only the fence and gate on the perimeter boundary are timely but the four Protected Room boundary elements are not. Alternatively, if the hypothetical facility in Fig. 59 has the critical detection point at the Protected 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 focus on evaluating P_N as a measure of the effectiveness of the response force. The determination of this probability will require information about the response forces, the threat, the PPS, as well as the choice of methodology. P_N is evaluated based on engagements that are defined as a set of events where two opposing forces (response force vs. adversaries) use weapons and tactics in an attempt to achieve their respective goals. Obviously, because many random variables are involved in an engagement, there are many possible outcomes. A PPS win is defined as one of the following theoretical outcomes: the adversary force is killed, captured, or abandons the attack. The probability of neutralization, P_N, can be defined by the following Eq. (3):

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

10.12. For the Eq. (3) to hold, the number of engagements in the denominator should be assumed to be an arbitrarily large number in accordance with the Law of Large Numbers. This law states that as the number of times that an event, in this case an engagement, is repeated, the proportion of successful outcomes, measured as a response force win, will tend to come to the actual probability of that event. In using Eq. (3) in an analysis process, the analyst should keep in mind that all engagements should use identical assumptions, such as the same initial conditions, and there are only two possible outcomes per engagement, either a win or a loss. Methods for determining P_N include:

(a) Expert judgment;

(b) Mathematical models;

(c) Simulations; and

(d) Analysing the results of real security incidents (actual malicious acts).

10.13. Each method has its advantages and disadvantages, primarily in terms of time, cost, and accuracy. Some methods can analyse a few factors, while some can analyse many more. No method is able to account for all the factors that affect the outcome of a single engagement, but can provide insight into the strength of a response force.

10.14. Simple methods, like expert judgement, may only require data regarding the number of personnel and weapon types on either side, along with the time that different numbers of each side arrive to an engagement. More complex models, such as simulations, may require a significant amount of data, including:

(a) Initial locations of response forces and adversaries;

(b) Response force deployment routes and final locations;

(c) Adversary path;

(d) Adversary scenario;

(e) Terrain;

(f) Building schematics; and

(g) PPS characteristics (e.g., barrier delays).

10.15. When used as part of the design process, neutralization analysis will include some combination of expert judgment, mathematical models, and simulations. The analysis may consider general response planning issues such as comparing contingency plan options, response numbers and weapons, and training against requirements found in regulations. A neutralization analysis may also include a performance-based component that would also examine, in some detail, the performance of response forces against adversary scenarios under different conditions.

10.16. Under the latter approach, a number of scenarios are created and each scenario combines information and assumptions about the target(s) to be attacked. These assumptions include; the PPS (and the response force), the adversary characterization, the adversary attack plan that includes a sequence of postulated adversary actions and one or more adversary paths. Note that the scenarios to be evaluated may be known at the beginning of the neutralization analysis or may be created as the analysis proceeds.

10.17. The neutralization analysis focuses on response aspects of the PPS so assumptions are typically made about the element or protection layer on the adversary path that first leads to adversary detection. This element might be chosen because it is the critical detection point or it might be the first timely element/layer that the analyst determines provides the first significantly large probability of detection. Effectiveness exercises, either limited scope or force-on-force exercises, or simulations then begin/kick-off at that element/layer.

10.18. Because it is often difficult to conduct a large number of tests, especially force-on-force exercises, methods may be used and documented to estimate P_N from the available sample size. One method to estimate P_N is to use the simplistic formula Eq. (4), which is an approximation with small sample sizes and does not meet the Law of Large Numbers. Other methods of determining estimates of probabilities from small sample sizes exist.

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

DETERMINING THE PROBABILITY OF EFFECTIVENESS OF A PPS

10.19. When determining the probability of the effectiveness of a PPS, one method is to evaluate the $P_{E,}$ using the P_I x P_N formula by determining the P_I of a given path, and then the location of the critical

detection point of the most vulnerable path, and then conduct P_N scenarios starting with the adversaries at the critical detection point. A disadvantage of this approach is that the critical detection point at a facility is at or near the target location, and it is not always credible that detection would not occur until this point.

10.20. Another method to evaluate the $P_{E,}$ using the P_I x P_N formula, is to select a location on a path before, at or after the critical detection point, and then conduct P_N scenarios with the adversaries starting at that location. In this case, P_I is the cumulative detection of the sensing opportunities on that path up to the selected location. Under this approach, the scenario is analysed using the most probable point of detection. In this method P_E is also estimated using Eq. (1).

10.21. Note that this P_E value may not equal the value defined if the chosen element/protection layer is not the critical detection point. In such a situation, P_I may not be equal to the cumulative P_D at the chosen layer/element.

INSIDER ANALYSIS

10.22. IAEA provides guidance on measures that might be used to protect against the insider threat [13]. This section describes a method to analyse a PPS against insider threats when acting alone or when working in collusion with external threats. Methods widely used to analyse insider threats include expert reviews and table-top analyses. Insiders are a challenging threat to a PPS because they have detailed information not available to external threats and are capable of using defeat methods not available to external threats. Unlike external threats, the insider threat has unique:

(a) Access – authorized access to nuclear facilities, such as access into an inner or limited area.

(b) Authority – defined authority to influence or control others. For example, a guard force supervisor may 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. Information that may include facility characterization and operations, or PPS measures, capabilities, and operation, and target information.

10.23. The process used to analyse the insider threat identifies and groups nuclear facility personnel into threat groups based on common access, authorities, and knowledge. The insider threat groups may then be prioritized, and those groups that may pose the biggest threat may be analysed further. For each insider threat group selected, the access, authority, and knowledge of personnel within the group is used to develop scenarios based on the type of threat defined in the threat assessment or DBT. Insider threats may be:

(a) Passive – to provide information to external threats, but not participate in an attack.

(b) Active –to act alone, collude with other insider threats or with external threats to commit a malicious act. An insider may or may not be willing to use violence during the attack.

10.24. An analysis of passive insider threats consists of determining what information an insider threat group would have to develop scenarios. The effectiveness of the PPS is determined by performance testing those scenarios and analysing external attack scenarios that exploit the information available from the specific insider threat group.

10.25. An analysis of the threat of an active insider alone involves using experts to develop scenarios that the insider would use to exploit their access, authority, and knowledge. Scenarios should also be developed for multiple insiders if required by the applicable threat assessment or DBT. The effectiveness of the PPS against these threats may be estimated by using experts, through the use of performance tests or the use of table-top exercises.

10.26. Insider collusion with an external threat can include direct and indirect actions to support the successful completion of a malicious act. An analysis of insiders working in collusion with an external threat involves developing scenarios representing the external threat that includes the access, authorities, and knowledge of a selected insider threat group in an active role supporting the attack. These attack scenarios are then evaluated as defined previously through the use of performance tests, path analyses, and neutralization analyses.

SCENARIO ANALYSIS

10.27. Scenario analysis involves: (1) creating a detailed representative set of adversary scenarios (attack plans); (2) configuring the response based on facility security plans, procedures, and tactical deployment of response forces; and (3) performing a simulation of the interaction between adversaries and the PPS that is conducted as realistically as possible.

10.28. Scenarios analysis is a method to determine the P_N, which requires details about the attack and the response. Scenario analysis is a PPS effectiveness evaluation technique that is based on postulating adversary attack scenarios and determining P_E directly without needing to calculate P_I in one tool and P_N in another. The emphasis is on selecting adversary paths that take advantage of possible PPS vulnerabilities. The process involves identifying PPS elements/components that may be susceptible to defeat due to installation specifics or operational procedures. This includes 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 table-top exercises, computer combat simulations, and/or force-on-force exercises.

10.29. The results of the scenario analysis can be used to derive the P_N value when the P_I x P_N formula described above is used. The results can also 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. To achieve the nuclear facility mission, specific types of systematic and directed work are conducted. 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 activities and evaluating work results. Management systems are methods, processes, and tools used by the management of a nuclear facility to create a framework to accomplish work in a safe and secure manner while ensuring the purpose, objectives, and goals of the nuclear facility are achieved within the legal and regulatory framework of the State.

11.2. Historically, work performed in certain nuclear disciplines with potentially severe consequences was not controlled formally, and poor or incorrect work led to failures due to human error. A concept termed conduct of operations was developed to implement increased formality in the operations of nuclear facilities. Implementing conduct of operations principles resulted in the development of management systems that employ deliberate and systematic work planning, formalized change-control processes and methods to assess the quality of work output to provide assurance that operational goals are achieved. This also led to improved regulatory oversight by competent authorities.

11.3. The increasing importance of physical protection has resulted in the application of many of these management systems into the physical protection discipline. Implementation of formal management systems at a nuclear facility to perform operational, administrative, and business related work is essential to achieving physical protection objectives.

11.4. 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 nuclear facility to:

(a) Meet competent authority and operator requirements with consistent policies, processes, and procedures.

(b) Improve overall efficiency by elimination of duplication.

(c) Make it easier to continually improve management systems.

(d) Foster change and encourage innovation by creating a framework for continuous improvement and performance on the basis of experience from each discipline and manage necessary changes.

(e) Make decisions that best address the overall needs of the facility in a coherent and disciplined manner.

(f) Bring together expertise from different disciplines, to address conflicting requirements and to optimize solutions best suited to address all requirements.

(g) Prevent risk reduction in one discipline, such as safety, from creating new risks in another discipline, such as physical protection.

(h) Ensure physical protection does not unduly impact facility operations or the accomplishment of its mission.

11.5. An integrated management system incorporates all management systems of a nuclear facility into one coherent system to achieve its purpose and mission, and tailor the core management principles and processes as necessary for each specific discipline (e.g.: physical protection, NMAC, safety and operations). Activities that have an effect on operational results or regulatory compliance should be part of the management system. An integrated management system provides a single framework for the policy, processes, procedures and change control necessary to address all the objectives of the nuclear facility operator, including the areas such as nuclear operations, quality, safety, environment, personnel, finance, nuclear security, and information management. 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 documents that describe these processes should be integrated into a single framework. Care should be taken to ensure sensitive information related to the PPS, as with other sensitive information, is appropriately protected and shared only on a need-to-know basis.

11.6. Nuclear facilities should use an integrated management system for all phases in the lifetime of a nuclear facility and new nuclear facilities should integrate an organization-wide management system in all activities [14]. In other cases, at an existing nuclear facility, if an integrated management system does not already exist, it can be developed by integrating the separate existing management systems, including quality management, into one system. The remainder of this section assumes that an integrated management system exists at a nuclear facility.

11.7. Duties and responsibilities for physical protection should be established within the framework of the management system, and quality assurance is one element of an integrated management system [2]. Operators should adopt through their management system an integrated and coordinated approach to reviewing proposed changes before implementation, to ensure that changes proposed do not result

in unintended degradation of arrangements in the either safety or physical protection. Additional information regarding an integrated management system is contained in the IAEA Safety Standards [19, 20]. IAEA guidance 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 physical protection culture and cooperate with other State entities having physical protection responsibilities, such as off-site response forces [2]. Ref. [21] notes that staff performance is influenced by the quality of management and contains provisions for expectations, requirements and standards for the conduct of work, training, documented procedures and information systems.

APPLICATION OF MANAGEMENT SYSTEMS TO THE PPS

11.8. An integrated management system is used by facility management to sustain, monitor, and control all phases of a nuclear facility, including the PPS. For purposes of this document, the term "operation of a PPS" includes all the activities associated with its use and sustainment, including maintenance and testing. Management system principles help ensure a PPS continues to meet its original design specifications and it is modified as necessary to address changes in requirements.

11.9. The elements of an integrated management system include: requirements management; work direction and control; resource management; assurance activities; and sustainment and continuous improvement. These elements are shaded in Fig 60.

11.10. The unshaded elements in Fig 60 reflect the input for design begins with prescriptive and/or performance requirements established by the State and the competent authority for a nuclear facility, along with other requirements related to facility mission in terms of PPS requirements, the PPS design installation/implementation of physical protection measures, and operation.

11.11. An integrated management system is used to achieve the physical protection objectives. Fig. 60 illustrates conceptually the application of Management Systems to the PPS.

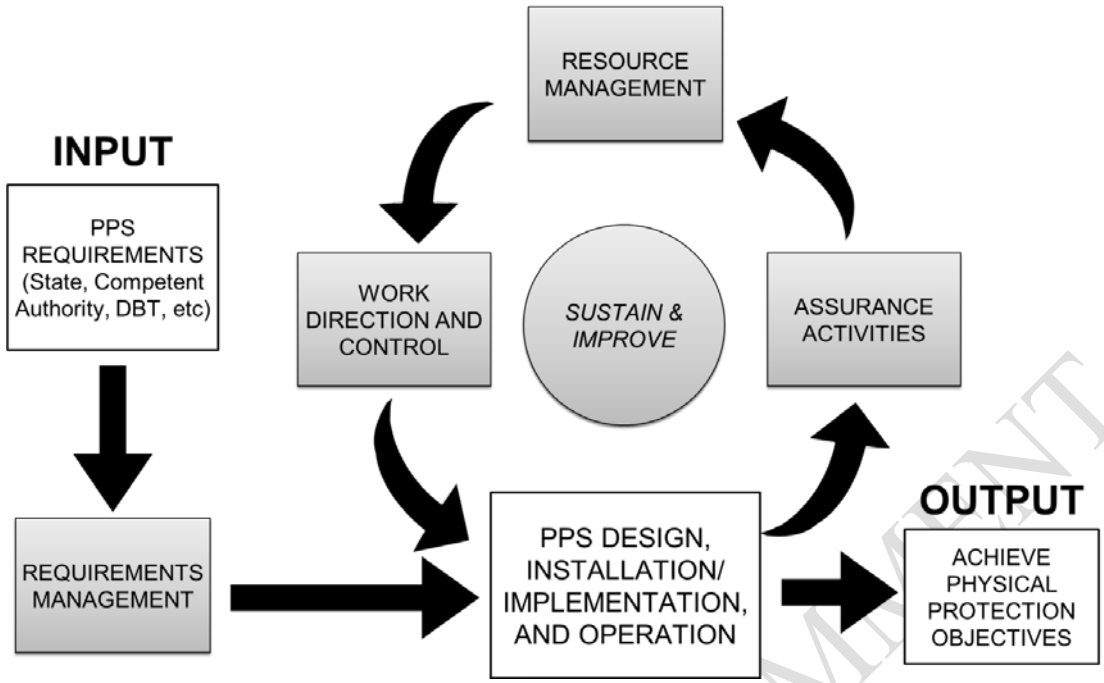

FIG. 60. Management systems applied to the PPS.

11.12. In many instances, some functions at a nuclear facility are provided by different organizations or government agencies; therefore, the facility management system will not address all of the PPS functions. As an example, the response force for a nuclear facility may be provided by the national police or military within a State. The operator management of the nuclear facility is responsible for operation of detection and delay components of the PPS, and may implement the overarching quality assurance processes that are part of the facility management system, but the national police or military will use internal quality assurance practices defined by their organization. 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, NMAC, and safety in development of standard programmes to cover all the disciplines, such as a quality assurance programme. Additionally, the operator should develop strong interfaces with all State and operator organizations involved in functions related to all phases of the design, development and installation of physical protection measures and operation of the PPS.

REQUIREMENTS MANAGEMENT

11.13. A PPS should be designed to meet a set of objectives, established by a State and its Competent Authority. These objectives may be in the form of prescriptive requirements, performance requirements, or most likely a combination of both, that 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 the PPS continues to meet the

requirements that become the basis for operation of the PPS. There are many methods and tools used to manage requirements., The following requirements management topics, as applied to a PPS, include:

(a) Assembling stakeholder requirements;

(b) Analysing the requirements;

(c) Verifying the requirements; and

(d) Documenting traceability of the requirements.

11.14. These activities may be performed sequentially as the design process proceeds or some may be performed in parallel. ISO/IEC/IEEE 29148 “Systems and software engineering - Life cycle processes - Requirements engineering, 2011”, provides more information regarding how stakeholder requirements can be collected and how a requirements analysis is performed.

Assembling stakeholder requirements

11.15. As part of the activities associated with design, the first step in the process is to determine all the applicable stakeholder requirements. These requirements may come from many sources, including the State, the competent authority and operational or safety requirements. During the design phase, these stakeholder requirements will be used to develop additional requirements, called derived requirements, which ultimately result in design specifications.

Analysing the requirements

11.16. Once all the applicable stakeholder requirements have been assembled, the second step of a requirements management process is to conduct an analysis to ensure the requirements are clear and understandable, to identify conflicting requirements and to transform the requirements into PPS derived requirements including design specifications for operating and maintaining the PPS using a risk management approach. Efforts should be taken to ensure that the derived requirements are clearly understood by the applicable stakeholders and properly reflect their view of the requirements.

11.17. Examples of how to develop a derived requirement:

(a) Requirement: “Inner areas should provide delay against unauthorized access to allow for a timely and appropriate response to an unauthorized removal.” [1] If this is a requirement from the competent authority, additional information would be required to develop design specifications. The requirement does not specify the amount of delay necessary for the inner area barrier, the response force time, or the threat capabilities that may be used to defeat the barrier. If the threat capabilities as defined in a threat assessment or DBT allow the use of explosives to defeat a barrier, for example, the

barrier would need to be more robust than a threat limited to the use of sledge hammers and pry bars. The analysis may result in a derived design requirement that the inner area wall provide 30 minutes of delay against forced penetration.

(b) Requirement: "Only authorized persons should have access to the inner area." [1] This is a requirement for the operator and a derived requirement should be developed so when the PPS becomes operational, plans, processes and procedures should be in place to determine:

- Job positions or personnel categories requiring access to the inner area to perform assigned job functions.
- How the authorization process to approve access for authorized persons into the inner area is controlled.
- The process to physically allow an authorized person access into the inner area.
- The necessary security related training required before personnel are granted access.

11.18. Another important step in the requirements management analysis is to identify potential conflicts in requirements. As an example, IAEA guidance states: "The number of access points to the inner areas should be kept to the minimum necessary (ideally only one)." [1] However, a safety requirement may state that an emergency exit must be provided within 25 meters of any location within a hazardous area. There may also be operational requirements to have access points at locations in the inner area to streamline nuclear material movements between other inner areas and reduce processing time. Meeting the recommendation for one access point would create a conflict with the other requirements. These conflicts should be resolved during the analysis step in a manner that balances the competing requirements.

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

Verifying the requirements

11.20. During the installation/implementation of physical protection measures, the stakeholder and derived requirements will be used as the basis for verification activities. Verification of the requirements ensures the design specifications and all requirements for operating and maintaining the PPS are implemented appropriately.

11.21. Verification may be in the form of performance tests, assessments, inspections, audits, or other means to provide assurance the formally documented requirements are in place. Verification

activities may be performed at the element, component, subsystem or PPS level. The linkage between verification activities and performance testing is important even during design.

Documenting traceability of the requirements

11.22. An important aspect of requirements management is to use a method to document how each formal stakeholder requirement can be traced by the creation of derived PPS requirements for the design, installation/implementation of physical protection measures and operation stages.

11.23. Requirements traceability serves two purposes, it provides evidence that the requirement has been met and it provides a mechanism to efficiently identify plans, processes, procedures and training that would need to be changed if the core requirement changes. For simple systems a common method for documenting requirement traceability is to create what is called a traceability matrix that lists the requirement, and all the associated plans, processes, and procedures, and records used to implement the requirement. As systems become more complex, use of traceability matrices becomes impractical, so formal tools and software are used.

11.24. As an example, there may be a regulatory requirement that personnel receive a certain type of security training once every six months to be allowed access into 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 some frequency.

(b) A process is developed within the facility for personnel requiring access to the inner area. It requires management to ensure training is scheduled for new personnel to grant them access into the area, ensure they receive the training before being authorized into the area, record a person's completion of training in a logbook, and send a copy of the log to designated security staff every time a person completes the training.

(c) Procedures are developed for security staff to build and manage a list of personnel with authorized access to the inner area, containing each name, their department, the date training was received, and the date the training expires. The procedures would be used to update the list on a monthly basis to require security staff to identify all the personnel on the list whose training certification will expire, will require refresher training that month, and mail memorandums to the appropriate departments. The procedure would also require security staff to write an interim memorandum to send to the access control point that lists personnel who have taken the training in between monthly updates.

(d) Procedures are developed for the guard working at an access control point to the inner area to verify the person is on the current list, prior to granting the person access to the inner area.

11.25. In this example, the single stakeholder requirement is reflected in the security plan, a training plan, training lesson plans, logbooks, and several procedures. A traceability matrix would list all of them, so when a change occurs, such as the required frequency of the training, all the necessary plans, processes, procedures and records can be updated to reflect the new requirement.

WORK DIRECTION AND CONTROL

11.26. Work direction involves determining what functions should be accomplished, establishing overarching security policies, establishing an organizational structure to accomplish those functions, defining roles, responsibilities, and accountabilities of departments and positions, developing strategic and tactical goals for organizations, and establishing criteria of performance for the PPS.

11.27. Determining what functions need to be accomplished to design, install, and maintain a PPS involves an understanding of the technical, administrative, and support functions necessary to perform the work. Some of the functions may exist within the facility security organization, and some of the functions exist in other departments of the facility. Example include, the:

(a) Design phase of a PPS may require involvement by security professionals, a design agent or agency, personnel responsible for the infrastructure of a nuclear facility, operational personnel, guard and response force representatives, safety representatives, IT representatives, and budget personnel.

(b) Installation of PPS facilities, barriers, or other systems requires construction and infrastructure personnel.

(c) Operation of a PPS requires personnel to operate and maintain the PPS elements, as well as supervisory personnel, and other security and non-guard personnel who provide functions such as training, assessments, performance testing, quality assurance, trustworthiness, records management, information protection, computer security, administration, budgeting, procurement, contract management.

11.28. A policy document is needed at a facility which states the commitment of management to physical protection. A best practice is for this security policy to be issued directly by the top management to make its importance quite clear and demonstrate its commitment for physical protection. There is a particular need to ensure that all personnel understand that adherence to this policy is expected of all personnel. This policy enforces management's direction regarding physical protection matters in all areas including the PPS.

11.29. Establishing an organizational structure to effectively manage a PPS involves defining the framework within which the physical protection department operates. There are many types of organizational structures, and the appropriate one for physical protection at a specific nuclear facility is based on many factors, but the objective is to develop an organizational structure that effectively manages the work necessary to design, install, and operate a PPS. There is no single structure that works in all situations, and the framework of the broader organization, the type of nuclear facility, State laws and requirement, cultural norms, and other factors influence which structure is appropriate for a given nuclear facility. Some common considerations when defining the organizational structure of a physical protection organization include:

(a) Establishing a clear chain of command, which is an unbroken line of authority that extends from the physical protection manager down to the individual personnel performing functions related to the PPS.

(b) Span of control refers to 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 both the personnel and the work can be effectively managed by a person.

(c) Centralization is a concept regarding how decisions are made within an organization, and what levels within the chain of command are 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. Many security organizations use an approach where the appropriate level for decision making is determined by factors such as the potential impacts of the decision to other organizations, risk, and costs.

(d) Division of labour involves how work activities or tasks are divided into individual jobs. Some jobs involved in operation of a PPS require specialized training, such as a locksmith or an armorer, and some require the skills of a generalist, such as a security planner responsible for developing security plans and procedures relevant to the PPS.

(e) Formalization of job functions within a security organization involves how jobs are structured. A guiding factor is the degree to which specific job tasks and activities are governed by processes and procedures.

(f) Departmentalization involves how specific jobs are grouped together in order to coordinate common activities and tasks. Some security organizations have a technical security group comprising personnel who can perform all the functions necessary 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 nuclear facility's IT group as needed for a specific activity.

11.30. 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 who is responsible for what in order to achieve the desired results. This goes beyond individual staff members understanding their roles and responsibilities for physical protection to ensuring that all managers within the facility are delegated responsibility for the physical protection of targets within their purview, including information and computer systems, as well as support tasks such as staff and training and implementing trustworthiness policy. Managers also need to be made responsible for ensuring that personnel employed by them understand their responsibility for physical protection, apply physical protection requirements and procedures as a contractual condition, and are appropriately supervised in this respect.

11.31. Establishing performance criteria for the PPS involves development of performance thresholds, 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 defines how well work is performed, how accurate it is performed, or how effective the final product is. An example of quantity performance metric 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 metric is the guards should respond to any alarm on the perimeter within five minutes.

11.32. Quantified measures of physical protection performance, with associated goals, are essential in establishing management expectations and in involving staff in achieving the desired results. It is suggested that management establish measurable physical protection objectives. 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 objectives 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 zero security incidents, personnel may not report such incidents so as not to be the one that ruins a clean record.

11.33. Work control involves providing leadership, oversight, and planning by developing a framework for work conduct and ensuring changes in the design or operation of the PPS occur in a deliberate, controlled, and integrated manner.

11.34. Management provides leadership by ensuring physical protection activities are accomplished appropriately by planning, assigning, and overseeing work activities associated with the PPS, and by setting a personal example. All work needs to be suitably planned in order to ensure that necessary functions are performed and physical protection is not compromised. Planning is accomplished for routine work as well as for non-routine activities or abnormal events, such as exercises, non-physical protection related maintenance work, equipment modification and replacement, outages, loss of power, failure of physical protection measures, and nuclear security incidents, in order to ensure the integrity of the PPS is maintained at all times. Some non-routine activities or abnormal events will require the planning of compensatory measures. Oversight is a supervisory function related to ensuring that personnel perform assigned functions according to plans and procedures, to meet the objectives of the function and performance metrics if applicable.

11.35. Work control also involves developing a framework for the conduct of work. The concept of conduct of operations involves activities such as development of shift activities, defining CAS activities, development of procedures to address; abnormal events, conditions, and trends, control of equipment and its status, use of compensatory measures, record keeping, shift turnover, use of procedures, and use of operator instructions.

11.36. Ensuring 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 documents the physical, procedural and training elements of an operating organization’s PPS. It serves as the repository for the design documents, standard operating procedures and governing guidelines for the PPS. Configuration management should be part of the sustainability programme of the operator and identifies and documents the characteristics of a facility's PPS, including relevant computer systems and software. It also ensures that changes to the PPS characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation. It also includes processes for coordinating changes to the facility’s systems or operations that may impact the effectiveness of the PPS. Furthermore, IAEA guidance suggests configuration management may 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 [2].

11.37. Configuration management ensures that changes to a PPS are properly developed, implemented, verified and documented. Having immediate access to this information can help the nuclear facility speed the recovery from hardware/software failures and ensure equipment is operating as intended when returned to service. In addition, access to accurate records regarding training, procedures, maintenance and logistics allows the operating organization to verify that these important aspects of a physical protection system are being met. The operating organization should:

(a) Ensure that the implications of changes in the PPS subject to configuration management are reviewed prior to implementation and are documented appropriately.

(b) Ensure that configuration management information is accurate, available in a timely manner and appropriately protected.

(c) Apply configuration management to document the physical layout, procedural operation and personnel training records of its PPS.

11.38. IAEA guidance highlights the importance of management programmes for configuration management of the PPS [2]. Other guidance suggests how 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 [20].

11.39. Change management can ensure any proposed significant change within the nuclear facility made by any department for whatever reason, whether of a structural, procedural or organizational nature, be they temporary or permanent, are analysed with regard to their implications for physical protection. It is important that no reduction in the effectiveness of physical protection is acceptable, even for short periods of time, without appropriate justification and management 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 safety and NMAC.

11.40. Preferably, one manager should approve each change and the change is then endorsed by those individuals whose area of responsibility is most affected. This review and approval process should be given particular importance when the activities that permit the change to be made are the responsibility of different parts of the organization. Evidence that the change satisfies physical protection requirements need to be made available and approved or authorized by the facility's security organization.

11.41. Adequate monitoring as the change is implemented needs to be carried out to provide early warning on any negative effects on PPS effectiveness, thereby ensuring that there is sufficient time to take remedial action as necessary. Examples of planned activities which could have a potential adverse impact on physical protection are:

(a) Activities that could cause a loss of primary power to physical protection equipment;

(b) Placement of vehicles or heavy equipment or installation/development of physical protection measures of barriers that could obstruct detection or assessment or increase response times; and

(c) Construction activities that remove or degrade physical barriers, thus allowing established access controls to be bypassed.

11.42. 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 its planned activities do not decrease the effectiveness of the security plan or PPS at the adjacent facility.

RESOURCE MANAGEMENT

11.43. Resource management includes topics such as training and qualifications programmes; selection of personnel for the functions necessary to support design, installation/implementation of physical protection measures, and operation of the PPS; procurement of products, goods, and services; and establishing a productive work environment.

11.44. Personnel selection is the methodical process used to select personnel to perform job functions related to the PPS, with the intent to identify people who have the knowledge, skills, ability, and other characteristics to make the most valuable contributions to the organization. Human resource processes at a nuclear facility are often part of an integrated management system, and physical protection management should work to recruit, hire, and retain the best personnel available within the constraints of the system. Personnel selection also includes ensuring personnel have all the qualifications necessary to perform a job function, and have trustworthiness checks prior to being employed in a position requiring such checks.

11.45. Effective physical protection depends upon staff having the necessary knowledge and skills to perform their functions to the desired standards. Managers need to ensure that their staff not only receive security training appropriate to their responsibilities but that they are also educated on the threat, the importance of each individual being responsible for physical protection and the need to report suspicious activity.

11.46. Procurement of goods and services is required to sustain an effective PPS. Some considerations include procuring PPS equipment from established vendors to ensure replacement parts are available for the expected lifetime of the equipment, performing testing and evaluation of new components to ensure they integrate into and are compatible with existing PPS components prior to a large procurement, and evaluating potential supply chain risks. The operator retains responsibility for physical protection when contracting any processes or procuring any goods and services. Management needs to retain the competence to specify the scope and standard of a required product or service and subsequently assess whether they meet the physical protection equipment requirements and specifications. Management system may include arrangements for:

(a) Qualification of vendors, contractors and suppliers of items, products and services;

(b) Selection of vendors, contractors and suppliers on the basis of the effectiveness of their managements systems and their performance;

(c) Verification that vendors, contractors and suppliers understand and comply with physical protection requirements (including security of sensitive information) relating to the items, products and services which they provide;

(d) Prior approval by the nuclear facility of any sub-contracting 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 suppliers and their staff;

(g) Periodic assessment of the management systems, including physical protection arrangements, of suppliers and their performance, using a graded approach; and

(h) Verification that items, products and services supplied meet the facility's physical protection specifications and are authentic.

11.47. The physical and physiological environment work environment has a large impact on how staff members perform their tasks and comply with physical protection requirements. It is important that physical protection procedures are not regarded as an excessive burden. Managers can involve personnel in reviewing physical protection guides and procedures to make sure they comprehend the documents, understand why these procedures are in place and are able to offer suggestions to make them more effective.

ASSURANCE ACTIVITIES

11.48. Assurance activities include implementation of quality assurance and assurance programmes to provide ensure the PPS performs as designed, meets requirements, and meets the defined standards of performance. An assurance programme establishes evaluation and testing activities with sufficient rigor to ensure that PPS elements are at all times operational, functioning as intended, and interacting in such a way as to identify and preclude the occurrence of adverse activity before physical protection is compromised.

11.49. Quality assurance is part of quality management focused on providing confidence that quality requirements will be fulfilled (which in turn should be part of the integrated management system). A quality management system can be defined as one that is a collection of business processes focused on achieving quality policy and quality objectives to meet regulatory requirements [2].

11.50. 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 elements that compose the total PPS at a nuclear facility. Consideration should be given to

development of schedules for assurance activities, how results of assurance activities are used, and 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 a wide range of assessment programmes, root cause analyses, performance indicators, lessons learned and corrective action tracking programmes that can be used for physical protection.

11.51. Assurance activities include regular evaluations to ensure the ability of a nuclear facility to sustain its PPS by identifying both strengths and areas for improvement. The rigor of these evaluations should be based on the graded approach, depending on the type of nuclear material or nuclear facility, the nature of the operations, as well as the measures that make up the PPS. Additional information on assurance activities can be found in Section 9.

SUSTAINABILITY AND CONTINUOUS IMPROVEMENT

11.52. Sustainability is the concept of maintaining the performance of people, procedures and equipment. This requires monitoring performance, motivation, and leadership to create organizations that collaborate, innovate and produce consistently superior results. Sustainability includes maintenance and testing programmes to keep PPS systems working as designed, and working to develop a culture that fosters high performing organizations and team who collaborate, innovate and produce consistently superior results [22]. High performing organizations have shared goals, shared leadership, collaboration, open communication, clear role expectations and group operating rules, early conflict resolution, and a strong sense of accountability and trust among its members.

11.53. To effectively maintain a PPS requires not only effectively sustaining the technology but also sustaining the people using the technology. It requires developing an organization’s vision, mission, values, and strategies, which is the foundation on which the expectation of high performance is built. Communicate to personnel what is important, what the organizational goals are, what gets rewarded, and what actions get disciplined. Most importantly, the entire employee population communicates to decision makers from the top to the bottom of the organization what they are expected to produce and what is acceptable in doing so. However, this will not add value unless management ensures they implement leadership practices that are consistent with the vision, mission, values, and strategies.

11.54. Sustainable high performance requires placing the right personnel in the right positions with the right leadership qualities. It also requires development of programmes to:

(a) Recruit the most qualified personnel available;

(b) Develop staff skills and abilities through training and qualifications programmes;

(c) Recognize and reward good behaviour;

(d) Retrain, transfer, or terminate low performing personnel; and

(e) Provide a safe work environment.

11.55. Continuous improvement is a process of identifying improvements in policy, programmes, processes, plans, procedures, equipment, or in management systems as a result of issues identified during assessment activities such as inspections, self-assessments, or performance tests, feedback from personnel or lessons learned, 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 incremental, unless a change such as a new or emerging 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 aging or obsolescence of equipment, reduced financial support, complacency or loss of motivation by personnel, and complacency by management. In this case, continuous improvement concepts may not identify ways to improve performance beyond its peak, but can be used to identify ways to sustain the performance of the PPS.

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities, Implementing Guide, under preparation (NST023).

[3] 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, GOV/INF/2005/10-GC(49)INF/6, IAEA, Vienna (2005).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations and Associated Administrative Measures, NST002, *implementing guide under development*

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Technical Guidance, Nuclear Security Series No 17, IAEA, (2012).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, Implementing Guide, IAEA Nuclear Security Series No.25-G, IAEA, (2015).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, NST044, *implementing guide under development*

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Technical Guidance, Nuclear Security Series No.16, IAEA, (2012).

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, Implementing Guide, under preparation (NST041, revision of NSS No.8)

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security during the Lifetime of a Nuclear Facility, Implementing Guide, under preparation (NST051)

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Technical Guidance, Nuclear Security Series No.4, IAEA (2007)

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Security Purposes at a Facility During Storage Use and Movement, Technical Guidance, under preparation (NST033)

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

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Technical Guidance, under preparation (NST036).

[19] 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).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, Implementing Guide, Nuclear Security Series No. 7, IAEA, (2008)

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, Implementing Guide, under preparation (NST020)

[23] AMERICAN NATIONAL STANDARDS INSTITUE, INTERNATIONAL SOCIETY FOR AUTOMATION, ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries, (2016).

ANNEX A: EXAMPLE NEEDS ASSESSMENT AND REQUIREMENTS ANALYSIS FOR A NEW TECHNOLOGY

A.1. This purpose of this hypothetical example is to provide a detailed overview of a needs assessment and a requirements analysis. In this example, facility management has 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 intruders away, again without exposing guard patrols.

A.2. One way to provide this capability is to using an unmanned aerial system (UAS). Alternate approaches might be to install cameras within the limited access area, perhaps mounted on guard patrol vehicles or installed throughout the limited access area. Data collected about UAS might provide the following information:

(a) UAS can be operated in several ways:

— Continuously over extended periods of time to provide intelligence, surveillance, and reconnaissance capability. Essentially, a persistent UAS presence over protected areas would be intended to almost always be available (subject to weather conditions) to direct intelligence, surveillance, and reconnaissance assets (cameras/infrared) at areas of concern. This operational approach either requires an airframe with long flight times (endurance), or requires the ability to hot-swap platforms in and out of service as batteries are recharged and/or fuel is replenished.

— Normal operation on a power and communications tether. Note that this system could be deployed from the tether and the tethered system could be moved. 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 be more limited in deployment options compared to continuous, untethered operations.

— Deployed periodically (e.g. once per hour) or on demand for assessment or determining intent.

(b) Very little reliable information, beyond vendor 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 thus has legal and policy limitations on operations that should be addressed.

A.3. As an example, assume that the operator would like to deploy a UAS on demand if there are indications that intruders are within the limited access area. Using system engineering concept, the

first step in exploring use of a UAS is to determine stakeholder requirements for this subsystem. Stakeholder requirements specify required system capabilities and functions as well as standards for quality, test and evaluation, and performance testing. Example stakeholder requirements may include:

(a) Operational effectiveness requirements: The UAS should be able to positively assess and challenge an intruder at least 30 seconds after detection at the boundary of the limited access area. The UAS should be available for deployment 75% of the time and cover 70% of those routes that the intruder 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, specify weight limits and operational limits for the UAS and also specify training requirements for UAS pilots. Also, hypothetically, UAS pilots are only allowed 8 hours or less of flying time within a 24 hour period. The competent authority may have requirements for the operator if they are a member of the response force.

(c) Operator requirements:

— Safety requirements: Operator safety policies specify that any physical protection subsystem operate within the constraints of a safety plan, protecting both operating facility personnel as well as the general public.

— Other required documents including: acceptance testing plans, maintenance plans and training plans for pilots and maintenance personnel.

(d) Cost requirements: No set cost limitations are specified at the beginning but there is a need to estimate rough initial and operating costs for deploying a UAS so that management can decide whether it is advisable 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. One of the first steps is to determine the concept of operations. The concept of operations describes the way the system works from the Operator perspective, includes the user description and summarizes the needs, goals, and characteristics of the system. A possible concept of operations for the UAS might involve the following steps:

1. Possible intruders would be observed within the limited access area using thermal imagers or by patrols using binoculars.
2. Vehicle patrols and waterside 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 command one or more selected patrol vehicles and boats to launch a UAS. The personnel in the vehicle or boat would determine if their UAS was operational, was in a location where it could be launched, and whether weather conditions were suitable for launch. If not the CAS would be told about this fact and other patrols may be queried to determine if any were in a position to launch a UAS.
4. The UAS may also be controlled by a pilot in the CAS to fly close enough to the vehicle or personnel to be able to determine if they are armed, are driving armoured vehicles, or are carrying suspicious-looking 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 intruders to instruct them to leave the limited access area or prohibited regions on the water side over a loudspeaker.

A.5. Both stakeholder requirements and concept of operations may lead to derived requirements such as the hypothetical requirements listed here:

(a) Steps 1-4 of the concept of operations should be performed while an intruder at least 30 seconds after detection at the boundary of the limited access area. Speeds and descriptions of the intruder vehicles/boats will be specified based on the threat assessment or DBT. Note that it may be necessary to collect performance data to create a timeline of UAS steps; the timeline would then be used to verify that these stakeholder requirements would be met against possible intruder timelines.

(b) The UAS should be available to be deployed 75% of the time based on weather conditions and system reliability constraints. Vendor UAS weight, size, and speed parameters will be compared to historic weather conditions such as rain, snow, hail, high winds and/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 should be available at night to see and track intruders. Given present technology, this capability will likely 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 define where on the facility map flight is allowed and also define how high 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 starts to fly away by itself.

(f) Training will be necessary to perform all their associated steps under the concept of operations. This includes the CAS operator, patrol vehicle/boats 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 the intruder 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 intruders away from the boundary of the limited access area. For example, one assumption might be: how many decibel of sound is needed to warn away an intruder under different weather conditions.

(i) To meet system maturity requirements, only those UAS makes and models will be evaluated for inclusion that have been operated at a nuclear facility for at least a year.