SANDIA REPORT
SAND2021-14561 TR
Printed November 2021

Sandia National Laboratories

Security Technology Testing and Evaluation Manual

Anthony Aragon, Greg Baum, Thomas Mack, JR Russell, Ben Stromberg

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

This manual was created by Sandia National Laboratories (SNL) to document a practical and methodical approach to test and evaluation, design, deployment, and maintenance of physical protection systems (PPS) for the protection of nuclear materials (NM) and other high value assets. SNL has developed an exceptional expertise in PPS for high value assets over decades of science, technology, and engineering research and development.

This Security Technology Testing and Evaluation Manual (STTEM) presents a systematic approach for a standardized test and evaluation process to evaluate new and existing security technologies, qualify security technologies that are deemed ready for deployment, and provide post-deployment testing methodologies to verify performance of the technologies has not degraded over time.

This manual is designed to be applicable to all stages of the testing and evaluation (T&E) lifecycle of a PPS, shown in Figure E-1. The STTEM is configured so individual sections can be extracted and used as standalone methodology references for each stage of the T&E lifecycle. This structure was adopted to allow international partners the latitude to draw from sections individually to meet their immediate needs.

The information is this manual is structured to follow the T&E lifecycle, starting with identification and understanding of pertinent requirements, then execution of a market survey to identify candidate security technologies, followed by component testing and evaluation. If the technologies meet requirements, they can be incorporated into the PPS design. After a PPS design is established, it is implemented and certified by the designated competent authority and/or sponsor, and the PPS is approved for operations to protect NM. After the PPS is approved to protect NM, it must be periodically tested (the operational sustainment and maintenance stage) to verify its performance has not degraded over time and that it performs as designed until retired or replaced due to age or obsolescence.

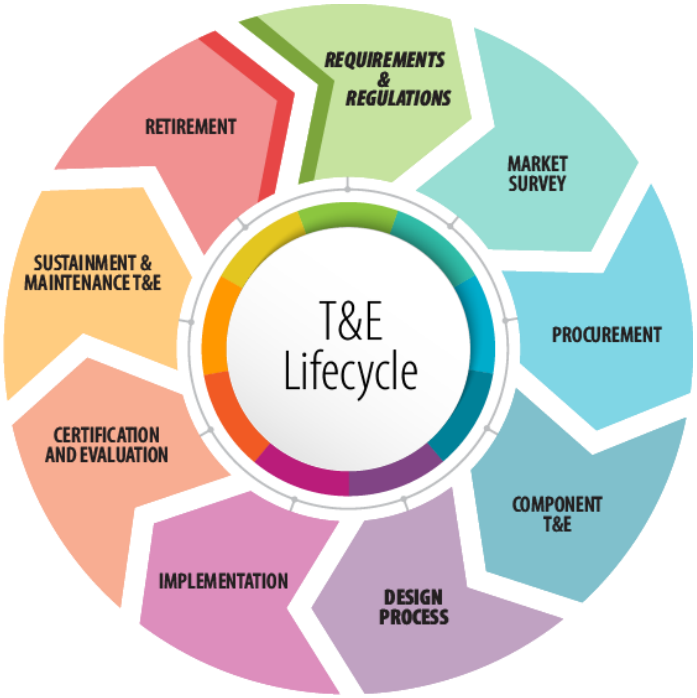


Figure E-1. PPS Testing and Evaluation Lifecycle

This page left blank

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
24/7	24 hours per day, seven days per week
AC&D	Alarm communication and display
AGL	Above ground level
CA	Competent authority
CAS	Central alarm station
CES	Consumer Electronics Show
CM	Corrective maintenance
CMMS	Computerized maintenance
CONOPS	Concept of operations
COTS	Commercial off the shelf
CUAS	Counter Unmanned Aircraft System
CUxS	Counter unmanned system
DA	Delegated agent
DEPO	Design Evaluation Process Outline
DOE	Department of Energy
DT	Design Team
DVR	Digital video recorder
ES&H	Environmental safety & health
FAR	False alarm rate
FCC	Federal Communications Commission
fps	Feet per second
Gp	Group
GT	Greater than
IAEA	International Atomic Energy Agency
IDS	Intrusion detection system
IH	Industrial hygiene
ISC	International Security Conference
LT	Less than
MTBF	Mean time between failure
MTTF	Mean time to failure
MTTR	Mean time to repair
NAR	Nuisance alarm rate
NEPA	National Environmental Policy Act
NM	Nuclear Material

Abbreviation	Definition
NNSA	National Nuclear Security Administration
NTIA	National Telecommunications and Information Administration
OPSEC	Operational security
POC	Point of contact
P_A	Probability of assessment
P_C	Probability of communication
P_D	Probability of detection
PIR	Passive infrared
PITCO	Pre-Installation Test and Check Out
PM	Preventative maintenance
PPS	Physical Protection System
P_S	Probability of sensing
P_T	Probability of communication
REQ	Requirements engineering
RF	Radio frequency
RFI	Request for information
RVTM	Requirements verification and traceability matrix
SAS	Secondary alarm station
SME	Subject matter expert
SNL	Sandia National Laboratories
STTEM	Security Technology Testing and Evaluation Manual
T&E	Testing and Evaluation
TADI	Testing, analysis, demonstration, and inspection
UAS	Unmanned aerial system
UL	Underwriters Laboratories
US	United States
USG	United States Government

1. INTRODUCTION

The Security Technology Testing and Evaluation Manual (STTEM) documents a process illustrated by the T&E Lifecycle, shown in Figure 1-1, the purpose of which is design, testing, and analysis of physical protection systems (PPSs) for nuclear material (NM). It is based on decades of experience from Sandia National Laboratories (SNL) physical security personnel.

1.1. Document Breakdown and Overview

The STTEM is intended for use by security personnel at any participating sites who may have, (1) knowledge related to PPS technologies ranging from minimal to substantial, (2) PPS technology needs ranging from basic to sophisticated, and (3) testing and evaluation (T&E) knowledge from individual PPS components to the entire system throughout the PPS lifecycle.

To meet the needs of such a diverse group, the manual provides information that spans the complete T&E lifecycle of a physical security system. Covered information includes pre-test activities, such as requirements definition, market surveys, and procurement. These activities may not be traditionally considered a part of the T&E lifecycle by some, but successful completion of these steps will have a significant impact on the test objectives, structure, cost, and schedule associated with actual testing activities. The ultimate success of the T&E program will depend on the accurate completion of these pre-test activities. Because of the dependency of the pre-test activities, they are included as part of the T&E lifecycle and this manual.

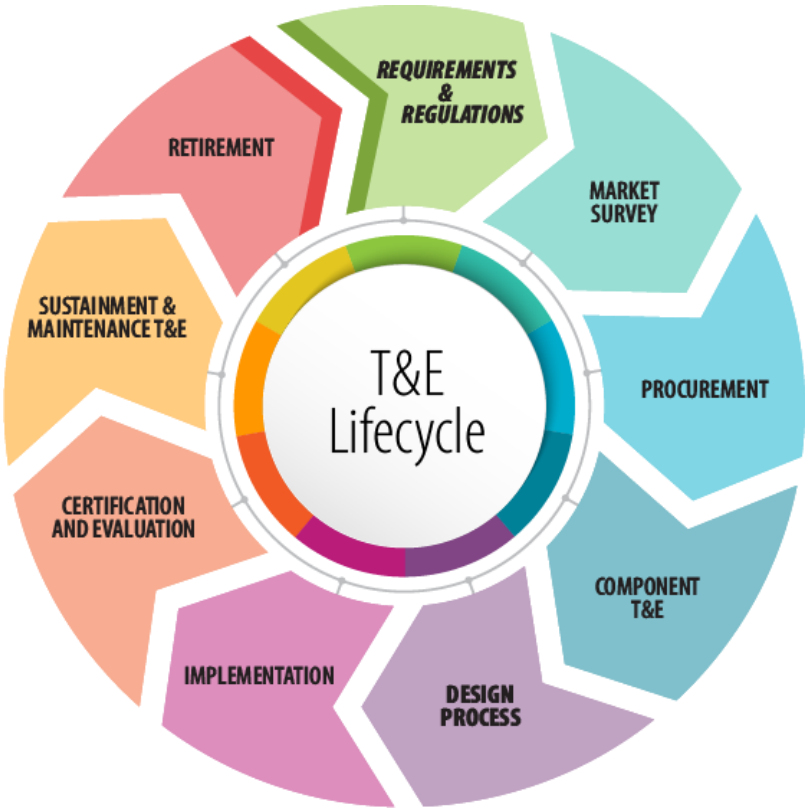


Figure 1-1. Physical Security Testing and Evaluation Lifecyle

The STTEM is organized into 10 chapters, listed below. The associated comments in italics provide a high-level objective for each chapter and a rationale for the information cited in.

Chapter 1: Introduction	Provides overview, background, purpose of this document.
Chapter 2: Requirements	Provides a basic understanding of requirements engineering and how requirements tie to all aspects of the PPS lifecycle.
Chapter 3: Market Survey	Describes a methodology for gathering information to determine the best commercial products available and make an informed selection of technologies to be tested. This assumes a sponsor is trying to find the best solution available and is not directing you to test a specific technology.
Chapter 4: Procurement	Describes the procurement process. An informed decision to procure a specific technology will follow the market survey. Although procurement of a technology may not be necessary to accomplish pre-deployment testing, it will be required for deployment.
Chapter 5: T&E Process	Covers the fundamentals of testing with a focus on pre-deployment testing of security components to ensure they can comply with prescribed performance requirements. After establishing testing fundamentals, they are applied to testing activities that support design, deployment (implementation), certification, and maintenance.
Chapter 6: Security Design Process	Includes descriptions of the Design Evaluation and Process Outline (DEPO) methodology as well as an explanation of the optional pre-installation and test check-out (PITCO) process.
Chapter 7: Implementation	Describes the implementation process. After the infrastructure at the site is in place, the PPS components are installed. Incremental/functional T&E is performed during installation of components, progressively verifying performance of installed components.
Chapter 8: Certification	Describes the certification process. After implementation and verification that the system works as expected, the official certification of the system is conducted. This test is overseen or conducted by the designated competent authority to verify performance of all elements of the security system meets requirements. The certification process also establishes baseline performance to compare against as the system ages.
Chapter 9: Sustainment	Describes the sustainment process. After the system is certified and officially approved to protect NM, sustainment

	testing is conducted to verify elements of the system have not degraded over time and continue to meet requirements.
Chapter 10: Retirement	Describes the retirement process. Data from sustainment testing will identify when system elements are reaching end-of-life and need to be replaced. It is important to begin the process to replace security elements several years prior to the estimated retirement date.

Organizations involved in the protection of NM face a challenging and fiscally constrained environment that requires collaboration in several physical security areas, including the physical security of NM, transport of materials, and security of associated facilities.

The physical security T&E processes outlined in this document provide a consistent, standardized approach to qualifying physical security technologies and equipment in order to support construction of new PPS facilities and upgrade existing PPSs.

The physical security T&E processes will establish and maintain standardized T&E processes based on the T&E lifecycle shown in Figure 1-1 and are intended to serve as an international resource that leverages proven methodologies across multiple organizations in the pursuit of high performance, cost effective, and timely physical security solutions for the protection of NM.

The physical security T&E processes apply to all physical security technologies employed within the nuclear communities, including the equipment and processes that perform the following essential functions:

- Intrusion detection
- Assessment
- Communications
- Counter unmanned aerial systems (CUAS)
- Alarm communication and display (AC&D)
- Delay
- Access control and contraband detection
- Response
- Cybersecurity

1.2. Purpose

The purpose of this manual is to provide an introduction and overview of the philosophy and methodologies used to establish a T&E program throughout the life of a security system that is protecting against malevolent attacks at nuclear sites. As an introductory overview document, this manual is not intended to develop expertise in PPS technologies, PPS T&E, PPS design, or PPS analysis.

To this end, the principal objectives of this manual include the following:

- Define the elements of the T&E lifecycle

- Identify T&E methodologies of PPS technologies
- Document the different processes of the T&E lifecycle
- Provide a central source of information on T&E methodologies for use by test engineers and designers

1.3. Comment on Use of an Integrator

This document is written with the assumption that testing, design, and installation is not performed using a commercial integrator. It is not our intention to sway the audience for this document to use or not use an integrator and it will be up to the organization responsible for the design and installation of the PPS to decide if employing an integrator makes sense.

When faced with the task of providing physical security to protect a facility from theft or sabotage of nuclear or radiological material it is necessary to first decide whether the facility has the resources (qualified man-power, knowledge and expertise, funding, and desire) to follow this entire STTEM process to successfully accomplish the objective. This manual provides the necessary guidelines for a facility to follow this process. However, in many cases it can be more efficient and productive to hire a physical security integrator to provide these services, which will include many of the elements in the T&E lifecycle.

A security systems integrator specializes in bringing together subsystems into a whole and ensuring those subsystems function together to provide a system that complies with the facility's performance and regulatory requirements. These subsystems can include intrusion detection, video assessment and surveillance, access control, contraband detection, communications and monitoring, etc.

The integrator can bring to the table much experience and knowledge of existing and new technologies available in the market to provide effective solutions that can meet the needs of the facility. This could save significant time and effort in going through the exhaustive process of a formal market survey. It can also save time and effort in accomplishing initial testing and evaluation of systems to determine viable technologies and manufacturers using this STTEM process.

A qualified integrator can provide a wide range of services to assist the facility. These services can range from simply providing recommendations on viable physical security hardware solutions that comply with performance requirements to total involvement from the evaluation of requirements, proposing and providing subsystems, design and implementation, through testing to ensure proper functionality for certification. Qualified integrators can also manage and maintain the systems as well as train the people that will manage the system at the facility, while providing continuous assessments, upgrades, maintenance, and ongoing service.

Some additional benefits of engaging the services of a full-service system integrator include the understanding and knowledge of your system they will have because of their involvement from conception to completion. Partnering with a single team provides one point of contact to ensure history and continuity throughout the lifecycle, which allows the integrator to be aware of and receptive to the facility's ongoing needs.

Given the level of knowledge the integrator will need to have of the facility and its physical security systems in order to be the most effective, choosing an integrator will obviously necessitate a thorough vetting of the companies considered.

If an integrator is not involved in the STTEM process, it will up to the facility to ensure a successful outcome by performing all the functions outlined in the T&E lifecycle.

2. REQUIREMENTS AND REGULATIONS OVERVIEW

2.1. Introduction

Good requirements are crucial to project success. Requirements directly drive costs, schedule, and ultimately the performance and effectiveness of the security element or system being tested.

Because this T&E document is primarily intended for use by security personnel at a nuclear site or physical protection system equipment test facility, it is assumed that the audience for this document will be provided high level requirements, documented in regulations provided by the Regulatory or Competent Authority in the country for the protection of nuclear facilities.

The actual organization that provides and identifies the specifications that the security component or system being tested must meet security requirements will vary among countries. For purposes of this document, the requirements organization will be referred to as the Design Team (DT). It is assumed that the DT providing the requirements is also the authority that accepts the performance of the security element or system being evaluated.

2.1.1. Requirements, Roles, and Responsibilities Throughout the T&E Life Cycle

It is essential that the DT stay involved with every step of the T&E lifecycle. Requirements-related activities and responsibilities are discussed in the following section and are enumerated in the T&E lifecycle shown in Figure 2-1.

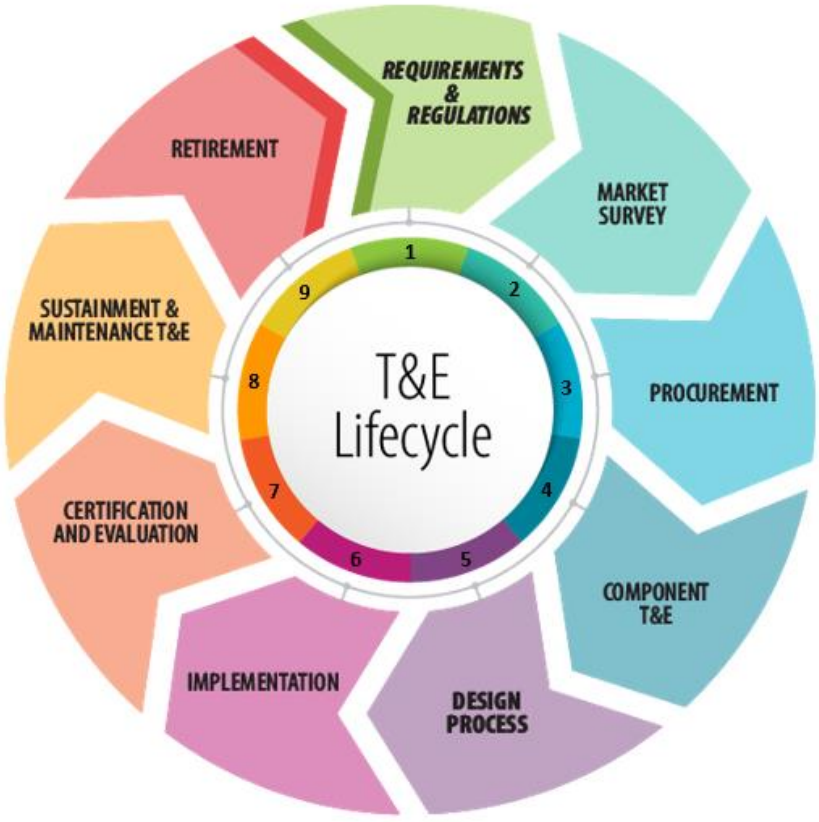


Figure 2-1. Activities Associated with Requirements and the T&E Lifecycle

Ideally, each numbered activity in the following text will be completed or resolved before advancing to the next activity.

Activity 1: Requirements and Regulations

- The DT is responsible for providing security requirements and specifications of the security element or system necessary to pass acceptance criteria
- The role of the competent authority (CA) in the design, certification, and test and evaluation stages of a physical protection system will vary from country to country depending on the regulations and role of the competent authority in each country
- The T&E team will review the requirements, ensuring they are complete, clear, and verifiable
- The T&E team will identify any regulatory requirements from other agencies within the country that may conflict or possibly take precedence over the DT requirements
    - For example, the DT could specify radio frequency (RF) jamming to neutralize an unauthorized unmanned aerial system (UAS) that will also jam nearby airport communications; the frequency coordination regulations from the airport authorities may take precedence over the DT requirements, so this issue would need to be discussed and resolved
    - The frequency coordination issue would also impact how neutralization of an unauthorized UAS will be tested during component performance testing, certification, and operations/sustainment
- If issues or questions do develop, the T&E team will work with the DT to resolve the issues and update/document the requirements as appropriate, including the date when the requirement was changed

Activity 2: Market Survey

- Assuming the DT has not defined a specific technology to be evaluated, the T&E team will seek to identify the best commercially off the shelf (COTS) technologies available that can meet the DT requirements
- The T&E team is responsible for providing COTS vendors with key security performance and environmental requirements the technology must be capable of meeting
    - Before sending out notices to COTS vendors, the T&E team should list and prioritize the requirements
    - It will be necessary to define a method to quantify and prioritize requirements to rank vendor responses, which will be covered in more detail in Section 3
    - It is worth mentioning that some vendors may say their technology will meet a requirement, but in truth they really don't know; the main objective of the component performance testing phase of the T&E lifecycle, Section 5, is to experimentally show what a technology can or can't do
- If a COTS technology does not exist that can meet the DT requirements, this issue should be presented to the DT and resolved; possible resolution options include:
    - The DT resolves the conflicting regulatory requirements described in the frequency coordination example, allowing the use of RF jamming when in proximity to an

airport under certain conditions (note the "certain conditions" agreed to will impact the T&E of the technology), or

- The DT could modify the requirement, for example allowing shorter sector lengths in a perimeter design for which COTS solutions do exist.

Activity 3: Procurement

- After a down-select from the market survey of COTS technologies, the top candidate technologies are procured
- The number of technologies to be purchased for T&E will be limited by the budget and schedule allotted by the funding agency; allotted budget or cost is not a technical performance requirement, but will likely be one of the most important requirements specified by the sponsor for this activity
- There may be security requirements from the DT or import regulations restricting import of technologies from specific countries that must be considered
- Some countries may have restrictions on "sole source" purchases; this restriction is imposed to allow any qualified vendor to have an equal opportunity to sell their technology, enforcing a "fairness of opportunity" regulation
- Procurement may not mean purchase; there may be options to lease or "borrow" a technology for a limited time to conduct preliminary T&E

Activity 4: Component Performance T&E

- The T&E team will consider all DT performance requirements, specifications, regulatory requirements, safety requirements, and cost/schedule when creating a test plan
- The DT will typically approve the T&E plan before testing begins
- The DT design team will also review the T&E plan to make sure they can design the PPS based on the data and performance metrics (metrics used to verify a requirement) that result from tests scoped in the T&E plan

Activity 5: Security Design Process

- The security design process follows a methodology defined as the Design Evaluation Process Outline (DEPO) that encompasses the first several elements of the lifecycle wheel; the steps in the outline include:
    - The DT will take the defined PPS requirements (as outlined in activity 1) and ensure all relevant requirements applicable to the project are identified, defined, and understood
    - Next, the DT will conduct or oversee the identification of qualified PPS technologies that may meet the requirements; for some facilities, this may be carried out by an integrator
    - The final steps in the DEPO process include the evaluation of the PPS technologies to ensure all performance and other prescriptive requirements are satisfied, which will be accomplished by the T&E team or the integrator. If the design analysis shows the design requirements were met, it will be formally documented and the process advances to implementation. If the design does not meet requirements, a second design iteration will be needed to make the necessary corrections.

- In many cases it will be advantageous to conduct a Pre-Installation Test and Check Out (PITCO), which involves providing a test bed to verify software configurations, connectivity for power, communications protocols, data rates, and latency requirements can be met as designed and built
    - If a PITCO test bed is warranted, the DT and/or T&E team will determine who accomplishes this task
    - This activity is meant to identify inter-system compatibility issues prior to installation at the site; compatibility issues can be caused by insufficient detail or mistakes in requirements or specifications, and it is the responsibility of the design team to specify inter-system compatibility requirements during the design phase of a PPS, but iterations on interface requirements and component specifications may occur between the design phase and implementation
- It is the responsibility of the T&E team to test and verify that subsystems have the appropriate interface definitions and requirements and report back to the design team and the sponsor

Activity 6: <u>Implementation</u>

- Implementation or construction of a PPS can be a complex undertaking and may involve numerous requirements. Depending on the size and complexity of the project, it may be necessary for the DT to identify a team of inspectors, representing the interests of the DT, to verify requirements are met for multiple areas that may not be considered part of the specific technology, including:
    - Power distribution and backup power
    - Fiber communications, copper communications, wireless communications
    - Geotechnical and soil
    - Structural requirements for facilities such as entry control facilities, the central alarm station (CAS), the secondary alarm station (SAS), guard towers, etc.
    - Drainage
    - Fencing
    - Lighting
- It will be necessary to ensure the appropriate infrastructure is properly installed and meets requirements; this will be accomplished by the design team or integrator, as appropriate
- Ideally, when the site infrastructure is in place the PPS implementation team can begin to install the PPS elements
    - As various security technologies are installed, they should be tested to verify they meet the requirements, and should be consistent with the result recorded in the component performance T&E
    - Members from the T&E team are normally on site to test security elements as they are installed

    - It is useful to list methods or tests in the form of a checklist during installation of security technologies, verifying requirements that will be assessed during the certification and acceptance tests are met
    - The implementation team and the T&E team are responsible for checking that all requirements are met prior to entering the certification phase

- After implementation testing is completed, a burn in time (continuous operation of a newly installed technology that is intended to detect any early failures) specified by the DT will be conducted; the longer the burn in time the better. Thirty days is a typical burn in time.
- Prior to entering the certification phase, the DT may require a readiness to test document that shows all the results from the installation tests, proving the system will be able to meet the certification and acceptance requirements

Activity 7: Certification and Acceptance

- Some consider the certification and acceptance testing to be the most important phase of testing because it decides whether the DT will declare the PPS worthy of protecting NM, but if T&E in the previous steps is conducted in a rigorous and meticulous manner, there should be no surprises, and all requirements should be met
- These tests will be conducted at the request of the DT to show requirements have been met; the T&E team, or integrator, is responsible for conducting the certification testing at the request of the DT. The DT may invite the CA to observe the testing if that is a regulatory requirement
- If done properly, the checklist used during implementation testing and documented in the readiness to test report will identically match the checklist used in the certification tests (verification that requirements are met); the DT will specify whether a checklist is required
- Certification often includes an additional 30-day burn in period in the operational environment to verify:
    - The technology part of the PPS meets requirements
    - The security force knows how to properly operate the system
    - Early component failure is not going to occur
- The DT may employ subject matter experts (SMEs) to assess the results of the acceptance tests and will likely require a report documenting that requirements have been met; this report also serves as a baseline for system performance at the time the DT accepts the system
- The DT has the ultimate responsibility for declaring that the PPS technologies are ready for full operational capability

Activity 8: Sustainment and Maintenance T&E

- The security personnel are responsible for conducting periodic tests to verify the system continues to perform (meet requirements) as documented in the acceptance test results
    - Periodic tests may be structured such that the security personnel will test all elements of the PPS on a pre-defined, periodic basis

- Maintenance testing will identify when a security component or subsystem is failing to meet requirements, warranting repair or replacement
- Maintenance tests will resemble tests conducted during acceptance testing.
- The Competent Authority may require periodic physical force-on-force exercises or table-top force-on-force exercises to show the site can effectively use the security technologies to properly respond to different attack scenarios; this type of testing will challenge the PPS technologies, training, CONOPS (concept of operation), and response force capabilities to protect NM from simulated attackers.

Activity 9: Retirement

- When technology failures occur during normal operations, or maintenance testing shows that components are failing due to end-of-design-life limitations, site security personnel will make recommendations to resolve these issues to site security management by suggesting a PPS upgrade or replacement
- At this point, the site security management may authorize the recommended repairs, upgrades, or replacements
- A change in threat definition constitutes a change in requirements, which will be incorporated into the requirements phase of the next round of the T&E lifecycle.

2.1.2. Requirements and Component T&E

The component T&E is the first opportunity for the T&E team to experimentally verify security performance claimed by the vendors and to verify the component's ability to meet DT security requirements. The T&E team will be provided requirements, regulations, and specifications, but it cannot be assumed the requirements provided have been reviewed and analyzed for clarity, completeness, and that they are measurable. It is incumbent on the T&E team to review and analyze requirements prior to writing a test plan.

From the perspective of the T&E team evaluating a security component (a sensor, camera, etc.), the component being tested has already been designed, manufactured, and is hopefully a COTS product.

By the time the security component has matured to a COTS product, a significant amount of effort (maybe several years) has been invested in the development of the product, including definition of vendor requirements, design, manufacture, establishing technical support (an important requirement to consider, which may not be specified in the security requirements provided), and sale of the product. A considerable amount of testing to show the vendor's requirements have been met has already been completed.

The T&E team's task is to write a test plan that addresses the security requirements and specifications provided by the DT and regulatory requirements that will be imposed on the testing and operation of the security component. The task of writing a test plan will be discussed in some detail in Section 5.

2.2. Review and Analysis of Requirements

A requirement is a precise statement of a need. After receiving a set of requirements, it is vital for the T&E team to spend time reviewing and analyzing the requirements. The process of reviewing and analyzing requirements should start with making sure the team understands the requirements. A

good understanding of the requirements is critical before attempting to estimate the cost, scope, and schedule associated with a test plan or program.

2.2.1. Objectives of Requirements Review and Analysis

The objectives of the review and analysis of requirements include:

- Producing clear, understandable requirements
- Eliminating inconsistencies or conflicting requirements
- Prioritizing requirements (if requirements are conflicting)—threshold vs. objective, shall vs. should, etc.
- Identifying interfaces between subsystems and associated requirements
- Identifying requirements for the entire lifecycle of the security element
- Identifying gaps or missing requirements
- Removing any unnecessary requirements
- Ensuring requirements are verifiable, and assessing the verification technique required
- Identifying assumptions built into the requirements

The T&E team should critically challenge each requirement, making sure the objectives listed above can be satisfied. This effort may require multiple iterations internally with members from the T&E team, the DT, and the implementation team. The following sections further detail the objectives of the requirements review and analysis process.

2.2.1.1. Ensure Requirements are Clear and Understandable

A clear requirement will not be misunderstood or misinterpreted. It should identify a single and concise thought. The team should be able to understand it and be able to quickly explain it to others, such as managers and sponsors.

Clear requirements will use consistent terminology, and any key terms will be defined. Examples of key terms in the security arena are probability of sense, probability of detection, and nuisance alarm rate (NAR). Terms such as these should be documented in a Glossary of Terms that can be accessed by anybody reviewing or trying to understand the requirements. All acronyms should be defined and understandable.

Requirements should be stated positively, i.e. the intrusion detection sensor shall be capable of detecting walkers, crawlers, and runners.

Requirements should be written to avoid using ambiguous terms such as "the sensor should support the response force in detecting intruders" or "the sensor should be made of high-quality materials." Phrases like these indicate authors either do not know exactly what the product will need to do, or they have not sufficiently thought through the requirement.

The requirement should state the need, not the solution. Good requirements clearly state what the need is and do not specify the solution. Returning to a previous example of a need, "the intrusion detection sensor shall be capable of detecting walkers, crawlers, and runners" as opposed to saying, "radar and video analytics shall be used to detect intruders." This type of requirement may drive the design team to pursue a solution that is not attainable.

2.2.1.2. Eliminate Inconsistent Requirements

Inconsistent requirements can be difficult to identify during reviews and are often due to requirements embedded in a subsystem that prevent a higher-level system requirement from being met. They can be identified during the design phase because they will create design difficulties. T&E of a system or component will also identify inconsistent requirements. An example of inconsistent requirements is:

- Higher Level Requirement: the cause of an alarm shall be assessed within 2 seconds from time the sensor declares an intrusion alarm
- Lower Level Requirement: camera images of a perimeter sector receiving a sensor alarm shall be automatically displayed within 3 seconds from the time the sensor declares an intrusion alarm

In this example, it is not possible to assess the cause of an alarm within the 2-second period if the images from the cameras are displayed 3 seconds from the time the sensor declares an alarm.

2.2.1.3. Eliminate Conflicting Requirements

Conflicting requirements can be the result of requirements that can be traced back to different requirements sources. For example, the requirements provided by the DT could state that RF neutralization shall be used to defeat incoming unauthorized UASs. A requirement from a country's frequency coordination regulations may state it is not legal to use RF directed energy to neutralize UASs. In this hypothetical example, a conflict exists between the requirement supplied by the DT and the laws of country.

2.2.1.4. Identify Lifecycle Considerations

Lifecycle considerations require the reviewers to put themselves in the position of the security personnel who will be required to maintain the security component. These types of issues are not readily identified by the design team or the T&E team. To address lifecycle issues, input from personnel who will maintain the system or have experience maintaining the system is advised. An example of a lifecycle need or requirement is:

- Higher Level Requirement: damaged sensors in the field shall be repaired within a 24-hour period of identification of sensor failure

This requirement could be decomposed into lower level requirements such as:

- Lower Level Requirement: the site shall maintain an inventory of sensor replacement parts onsite, allowing replacement of failing technologies within a 24-hour period
- Lower Level Requirement: maintenance personnel shall be trained in replacing failed sensor part

If replacement parts cannot be provided by the vendor or the maintainers cannot be trained, this set of requirements cannot be met.

Another Lifecycle consideration is upgrading software. For example, over time vendors will identify and correct issues associated with sensors installed in the field; software upgrades that address bugs will be sent out. Important questions to address are:

- Are the maintainers expected to upgrade the software?

- Are there configuration management procedures and documentation in place to track upgrades?
- What cybersecurity measures are imposed that will dictate how software upgrades are implemented?

2.2.1.5. Identify Missing Requirements

Engineers tend to focus on requirements for product function and performance and are more apt to miss requirements associated with maintenance, training, safety, or legal/regulatory expectations. Because of the damaging impact from missing requirements on a testing program, it is important to include reviewers with responsibility in these areas. If these requirements are not specified, they cannot be expected to be reflected in the component or system. The hardest requirements to meet are the ones that are not identified.

2.2.1.6. Remove Unnecessary Requirements and Assumptions

When reviewing requirements, each reviewer should mentally challenge each requirement and determine if it is needed and verifiable. If the answer is no to either of these questions, contemplate rewriting the requirement such that it is verifiable, or consider deleting it. Unnecessary requirements can stem from "wish lists." Wish lists can easily lead to scope creep in a project, increasing complexity, costs, schedule, and risk. Reviewers should seek to clearly understand what the goal or function of the system is and what data or performance is mandatory. Identify features that are "nice to have" vs. features that are mandatory for the intended functionality. Removal of unnecessary features (requirements) will make the system simpler, meaning fewer things can go wrong, and easier to maintain.

An example of an unnecessary requirement is the addition of extra fields in a screen presented to alarm operators that allows the operator to provide more details when describing the cause of a nuisance alarm. The more detailed information, requiring the extra fields, is not mandatory for the goals or the system functionality. It could take the operator an excessive amount of time to fill out the fields, distracting them enough that it could delay assessment of an actual intrusion alarm.

2.2.1.7. Identify Requirements Assumptions

Humans are not perfect, and anyone can make incorrect assumptions when developing and reviewing requirements. One of the difficult tasks for reviewers is to identify undocumented assumptions imbedded in the requirements. A useful approach to identify assumptions is to understand and discuss the reason or rationale behind each requirement. This discussion should include viewpoints from the users, maintainers, safety, cybersecurity, installers, the DT, and the customer who is paying for the system. If the rationale behind each requirement doesn't make sense to the reviewers, based on the collective rationale of the team, the assumption may not be valid.

It is likely it will be necessary to make assumptions while developing and reviewing requirements, and it is important to identify and document these assumptions and discuss them with the DT or other reviewers to determine if they are valid. The earlier the review team can validate assumptions, the better.

Sometimes, people do not ask critical questions because they think they are supposed to know the answer already (which may result from reluctance to reveal a lack of knowledge). This is the exact opposite behavior needed to uncover assumptions. The person leading the review team discussion

should encourage ideas and dialogue from all participants. Promoting an open discussion environment will result in more effective results in identifying assumptions.

A customer may specify a solution because they believe it is the best technical solution. Unfortunately, this happens too often. In this example, when the customer is specifying a solution rather than a need, they are assuming they understand what the best technical solution is. It is important to recognize the best technical solution is not necessarily the best overall PPS solution. There are other factors that must be considered, beyond the technical. As noted earlier, one key factor is budget. If the customer is correct and the solution they specified is the best technical solution, it may be too expensive, thereby exceeding a cost requirement. This is an example of an assumption leading to conflicting requirements.

When going through the process of challenging a requirement and asking for the reason or rationale behind the requirement, sometimes the answer may be "we don't know," or "this is how we have always done it." The team should recognize that answers like this indicate further review is necessary and an effort should be made to determine why "they always did it that way." There may be a good reason behind this tradition or decision, and it is important to document this reason and the rationale behind the assumption. Understanding "why" a decision is made can be just as important as "what" the decision is when reviewing requirements and documenting this information will serve to maintain corporate knowledge for the next generation of engineers.

Sometimes unnecessary requirements are caused by assumptions. As described in the previous example (2.2.1.6), the author(s) of the requirements assumed the addition of extra fields to allow more details on the cause of nuisance alarms would be a good thing. This assumption was not critically challenged by comparing the value of the additional information and the time required to enter the information to the mandatory function of the system, which is to detect intruders. There was also a disconnect between the requirement and the operational environment. Having an alarm operator review the requirement would have likely identified this issue earlier.

2.2.1.8. Ensure Requirements Are Verifiable

Verification that a system will meet requirements is performed using testing, analysis, demonstration, and inspection (TADI) activities. The methods used to verify each requirement shall be described, with reference to the specific TADI activity used.

When reviewing verifiability of requirements, reviewers need to ensure there is a method that definitively shows a requirement is satisfied. Reviewers should be able to clearly state the verification criteria. Requirements that depend on subjective or vague words (such as small, portable, fast, user-friendly) are not verifiable. An unverifiable requirement is an unnecessary requirement.

Verification engineers are sometimes referred to as test engineers. The T&E team has the responsibility of designing the tests necessary to empirically show key performance requirements have been met. A requirement may have a single or multiple verification methods. Some test results require additional analysis to quantify performance metrics called out in requirements. An example of this is the simple analysis of intruder detections (referred to as a hit) and missed intruder detections (referred to as a miss) to quantify the binomial probability of sense at 90% with a 95% lower confidence level (Table 5-1). In this case the analysis of test results is needed to show a requirement has been satisfied.

When testing for inter-system compatibility, a demonstration may be necessary to show subsystem one can communicate with subsystem two. In this case the T&E team must design a test to demonstrate a requirement has been satisfied.

Many national and international standards exist for product quality and safety. These standards ensure devices, components, and systems have been tested by independent laboratories to ensure compliance with prescribed safety and quality standards. The T&E team should ensure components and systems have been tested and approved by applicable accredited domestic or international organizations.

Conducting tests on a component or system can be expensive, but it is likely to cost the project more if effective component testing is not conducted. Execution of a thoughtful and deliberate test plan (or verification plan) will identify component deficiencies and any deficiencies in the requirements. The earlier these deficiencies are identified, the more likely you are to reduce risks to the project that can result in higher costs and longer schedules.

While a thorough test plan based on a good set of requirements is needed, it is also prudent to examine the verification methods to see if there are less expensive ways to verify a requirement. Consider the number of personnel needed to conduct the tests, where the tests can be conducted, what special equipment or facilities are needed to conduct a test, and how long testing will take. All these factors will contribute to cost and schedule of the test. An example of a way to reduce the cost of verification is provided below.

2.2.1.8.1. Example of Verification Method Cost Reduction

Requirement:

The electronic system shall function in cold temperatures, down to -46˚C (-50˚F) for a period of 24 hours.

Initial Verification Method:

Place the system in an environmental chamber, reduce the temperature to -46˚C (-50˚F) and run the system for 24 hours.

Cost Considerations:

An environmental chamber did not exist at the test site where other T&E activities were being conducted. One option is to ship the system to an offsite location for testing. A test team would also need to travel to the environmental chamber location to test the system and record the results. This option increases both test costs and schedule.

Verification Option Accepted by DT:

The system had been installed at a commercial location in a cold weather area for five years and successfully performed its function. Temperatures at this location could reach -51˚C (-60˚F) annually. Working through the system vendor, the security manager at the cold weather site was willing to provide a letter indicating the system had performed in cold weather conditions for the last five years at their location. The DT accepted this verification method, negating the cost and additional time to send the technology under test to the offsite location.

2.2.2. Requirements Verification and Traceability Matrix

When organizing and presenting the aggregated list of requirements, it is important to document them in a structured manner, showing what each requirement is, its origin, if it is necessary or simply desired, and how it will be verified. The structured documentation of requirements can be captured in a Requirements Verification and Traceability Matrix (RVTM). An example of a RVTM is shown in Table 2-1. The T&E team will encounter high level requirements that must be decomposed into

lower level requirements. The RTVM is a useful tool to show that lower level requirements trace back to the higher-level requirements and provide verification techniques appropriate for showing that high level requirements have been met.

Table 2-1. Notional Example of PPS Requirements RVTM

Policy Requirement Identifier	Source of Requirement	Functional Grouping	Policy Requirement Description	Threshold vs. Objective		Method of Verification			
				Threshold	Objective	Test	Analysis	Inspection	Demonstration
314	4733 Attachment 3 Section A Chapter IX PI.b	Intrusion Detection System	The system should initiate and transmit alarms, including: a) System failure b) Tamper c) Communication faults		X				X
313	4733 Attachment 3 Section A Chapter IX PI.b	Intrusion Detection System	The system shall detect intruders, including: a) Walkers b) Crawlers c) Runners with a probability of detection of 90% and a 95% lower confidence interval	X		X	X		

A hard requirement is identified as a threshold requirement, which implies the product "shall" meet. A soft requirement is identified as an objective requirement, which implies the product "should" meet. The "shall" requirements are a higher priority than the "should" requirements. This approach of defining and prioritizing requirements is a useful strategy to resolve conflicting requirements, simplify a design, and manage escalating project costs.

Once the RVTM is completed, the T&E team can begin the process of writing the test plan, ensuring all requirements that must be met by test or demonstration are included.

2.3. Resolution of Requirements Issues

During the review and analysis process, the T&E team will identify requirements that need clarification or correction. It is critical to the success of the project to engage the DT to resolve requirements issues, and the earlier the better. Site security management may not always understand their own needs or may not communicate them effectively to the DT. They will appreciate

identifying requirements issues early in the T&E process, which will save them money and ensure a better product. It is much better to identify requirements issues early in the T&E process, as opposed to identifying a missing or incomplete description of a requirement during acceptance testing or even worse, during operations. While the T&E team may assume nothing can be done about inadequate requirements, this is not necessarily the case. The T&E team can and must help site security management or the DT understand and correct, if necessary, bad requirements. When a product does not pass acceptance testing or performs poorly in the field, the customer is not likely to be understanding if the reason the T&E team cites for this poor performance is that the requirements were not well written.

This page left blank

3. MARKET SURVEY

3.1. Introduction

The term "market survey"98 is a subset of larger topic referred to as "market research." Efforts in market research generically include the investigation of the state of a market for a particular product or service, and analysis of consumers' needs. The previous section on requirements addressed a methodology to identify and document the consumers' needs. Given this rationale, the purpose of the market survey is to investigate the state of a market for a particular security product that could meet consumers' needs.

There will be instances when site security management or other sponsor will ask the test team to evaluate a specific technology and the sponsor will identify the vendor and model. In this scenario, the test team would still execute the steps covered in Section 2, but the market survey may not be necessary because the sponsor has specified the technology to use.

It is common for a sponsor to request the team identify a cost-effective solution to a security problem. For example, a sponsor requests a recommendation for a counter unmanned aerial system (CUAS) to be deployed at their site. In this case it will be up to the team to assess numerous commercial vendors for CUAS products and the respective product characteristics, including:

- Performance characteristics/metrics
- Acquisition costs
- Regulatory constraints
- Maturity of the product

These characteristics represent a subset of the parameters the team must consider before deciding which product(s) to acquire for T&E. A more complete list of characteristics/parameters will be covered in Section 3.6.

From the T&E perspective, the market survey provides a method to assess the costs and state of a technology and provides a tool to down-select potential products that are candidates for T&E. In the CUAS example, acquiring systems may be cost prohibitive. In this case a rigorous down select process will be warranted. A systematic down-select process will likely be needed to articulate to decision makers who control the budget the reason(s) why such an expensive system was chosen.

There are various methods to conduct a market survey to help identify security technologies that represent viable candidates for evaluation, including:

- Conducting a literature search
- Attending security conventions and trade shows
- Attending security demonstrations
- Conducting interviews with sites that have deployed a technology of interest
- Conducting a structured market survey and analysis

The first four methods will be briefly covered, while the emphasis of this section will be on the fifth technique, the structured market survey. The rational for this approach is that the audience for this

document can decide how much rigor is necessary for the market survey and scale the effort toward a more or less rigorous approach as appropriate.

3.2. Literature Search

A literature search is a quick method to locate qualified potential sources through the internet, databases, trade journals or professional journals, advertisements, telephone books, etc. It is an opportunity to find the current knowledge, thinking, etc., on a process or item of technology. It also could be used to determine who might be able to meet the desired needs. Further searching may result in discussions with vendor sales staff and engineers who possess a better grasp of the intricate workings of the technology and its performance limitations.

3.3. Attending Security Conventions and Trade Shows

Attending security conventions such as the Consumer Electronics Show (CES), the International Security Conference (ISC), and ASIS International is a useful start for newcomers to the security industry. It is common for trade shows like these to provide showrooms with over 1,000 vendors that are set up to demonstrate their technologies and services and answer questions. This is a useful forum to have face-to-face discussion with sales staff and engineers. Vendors are more than happy to provide contact information, business cards, and brochures on their products. Well-organized conferences, such as those identified, will publish a magazine that provides an overview of the showroom (useful when there are 1,000+ vendors), but more importantly will post articles and awards for the "best new security technology" at this show, or the "most innovative break through" in security technologies. This type of information can help attendees down-select which vendors to visit, as it is not normally possible to cover all the vendors present. Attending trade shows is a good starting point, but it is not recommended as the only source of information used in making a final decision on the best security technologies to evaluate.

3.4. Attending Security Demonstrations

First-hand observation of a security technology demonstration is a good way to see how a system performs in a more "operationally relevant" environment. Attending demonstrations can be time-consuming and costly, depending on the travel to the test site required. However, a demonstration in an operationally relevant environment is much more realistic than demonstrations on a showroom floor, and there will be more knowledgeable staff present to answer technology questions.

Attendees should pay attention to how closely demonstrations are choreographed or scripted. Highly choreographed demonstrations typically imply lower levels of maturity of the technology being demonstrated. An additional indication of lower technology maturity is if the system being demonstrated is only operated by vendor engineers. Demonstrations of more mature technologies can be conducted using security staff from sites, after a short training period. The less mature systems may require vendor engineers if they are complicated to operate or if there are enough "bugs" in the system to require an engineer to make corrections during the demonstration. Attendees can request a deviation from the scripted test/demonstrations to see how a technology might perform when subjected to non-scripted conditions. Data and performance observed during demonstrations can be insightful, but observers should be cautious in totally believing results from demonstrations. The real performance of the system will be revealed by results from the T&E team executing a well-written test plan.

3.5. Interviews

Interviews and discussions with individuals who have deployed a technology are a useful way to collect information. Normally technology users do not have the same profit motive to sell you a given product that the vendors do. They can provide positive and negative characteristics of the technology. This can include the quality and availability of vendor technical support when something goes wrong, whether the technology will not work well in certain site conditions (for example, underground pipes and wires may cause excessive nuisance alarms in a given sensor), or how long it takes to obtain replacement parts when the technology is experiencing issues (electrical failure in the field, for example). This first-hand user information is instructive and will be useful to help identify questions the respective vendors should be asked.

3.6. Structured Market Survey and Analysis

The four techniques cited above are useful exercises that will enhance the understanding of the current state of an available technology, but they may not provide the necessary rigor for high dollar acquisitions critical to security. This section will provide a more systematic approach to collecting information on security technologies, which will lead to a decision on which technology(s) to acquire for testing.

Although this approach provides a wider breadth of information from multiple vendors, it does take longer and costs more to implement. For example, one facility conducted a market survey on CUAS technologies in 2018. The process took approximately three months and their survey received over 300 responses. The responses were evaluated and prioritized, resulting in a down-selection to 25 candidate vendors/products. These were compared against key functional and performance requirements to arrive at a set of five candidate systems recommended for testing.

A more rigorous market survey approach is especially useful when considering a T&E program for new or emerging technologies, very expensive technologies, or technologies that are very expensive to test. For example, if testing a CUAS system that includes detection, assessment, and neutralization, purchase costs can be extremely costly. Testing of a CUAS system that includes RF neutralization will require special facilities that may also be very expensive to use and approvals to conduct the desired RF neutralization may take months. When comparing these costs to a three-month investment to conduct a market survey, the market survey appears to be a good investment.

It should be noted that the steps presented are not intended to be prescriptive or followed without deviation in all cases. The T&E team can decide where more rigor is needed and can pick and choose steps they think are appropriate for their application, risk, costs, and justification to the sponsor regarding technologies selected for T&E. The justification will be important if the technology does not perform as well as advertised. The T&E team may be expected to explain to the sponsor why a given technology was selected for T&E. The market survey and down select process will also include information on possible alternate candidates to be considered/discussed with the sponsor if a follow-on effort is planned.

Within the context of this document, the purpose of a market survey is to investigate the state of a market for a particular security product that could meet customer needs. The high-level processes proposed for a systematic market survey are:

1. Define the problem
2. Develop strategy and schedule
3. Implement strategy and schedule

1. Define the problem

What is the purpose of the survey, and what information will be collected?

The purpose of the market survey is to collect sufficient information to allow the team to identify the candidate technologies to be tested. What information will be needed to make this decision? It is assumed the requirements for the desired technology have already been defined, following the process described in Section 2. A subset of the previously defined requirements, referred to as "key requirements," will be incorporated into the market survey process. It is important to decide what information should be provided to the vendors in the Request for Information (RFI) package and what information the vendors are expected to provide. An example of key requirements is provided in Appendix A. These were the key requirements used in the CAUS market survey example mentioned in Section 3.6.

When defining the problem, the team must already understand the sponsor's budget for this T&E activity, including budget for acquisition of a technology and budget for testing. Budget limitations may dictate how many systems can be purchased for the T&E effort. There may be other options besides purchasing the technologies, which will be discussed in Section 4.

2. Develop Strategy and Schedule

After the team understands what information is needed, they should identify the strategy and schedule that will be used to down-select to a manageable number of technologies that will be selected for T&E. The strategy should include how the information will be collected from the vendors and organized. If there are 300+ respondents, as in the CUAS market survey example, data organization will be especially important. Once the vendor data has been collected and organized, the team must establish how the information will be analyzed and how vendors and their technologies will be scored and prioritized, ultimately identifying the top candidate technologies selected for T&E. An example is provided below showing steps and a proposed schedule.

How Information will be Presented to Vendors

Week 1: Develop a structured information format to be included in the announcement for the RFI

Based on the key requirements identified in the previous step, create a table to organize vendor input and instructions telling the vendor how to fill out the table (an example of this table is provided in Appendix B)

Determine how the request for the information will be distributed, i.e. sending the RFI to specific vendors the team is aware of; the announcement should include a point of contact (POC) to answer questions regarding the information requested, how to submit a response, when submissions are due, when vendors will be contacted if their system is selected for a more detailed data package, when vendors will be contacted if their system is selected for T&E, etc.

How the Information will be Analyzed

Week 2: Develop process to assess the strength of the information provided by the vendors

Determine the importance of each information category, which is reflected in how each information category is scored or weighted (an example of the scoring of key requirements is shown in Appendix C)

How the RFI will be Distributed

Week 3: Submit the RFI through channels required by the policy or contact specific vendors directly, allowing for a three-week period to respond

Week 6: Deadline for vendor responses

RFI Responses are Analyzed and First Down select Completed

Week 8: Complete the assessment of vendor responses, and down-select top 10[1] vendors that will be sent requests for more detailed information

Contact vendors advancing through the first down select process, letting them know they have been selected to provide a more detailed data package on their technology and should submit the detailed package in two weeks

A teleconference (telecon) may be necessary to discuss information provided by the vendor and resolve any questions the team may have; the detailed data package should address questions raised during the telecon and allow the vendor to provide any additional information that might be useful in the final selection of candidate technologies selected for T&E

Week 10: Receipt of the more detailed data packages from vendors

Detailed Data Packages are Analyzed and Top Three Technologies Selected

Week 12: Complete the assessment of detailed data packages, and select top three technologies to be evaluated, per sponsor approval

Week 13: Notify top three[2] candidates that their technologies have been selected for further evaluation

Document Market Survey Process and Results

Week 15: Complete a report that summarizes the strategy used for the market survey, examples of the RFI, summary of vendor responses (in an appendix), and justification for the selection of technologies to be evaluated; even if the sponsor does not request a formal report, an informal report documenting the strategy and result of the market survey is highly recommended, and should also include a brief section on lessons learned and how the process for the next market survey might be improved

3. Implement Strategy and Schedule

The information in this section includes the recommended steps and a notional schedule to conduct a systematic market survey. This level of rigor would not be appropriate for the majority of security technologies tested but would be appropriate when an item is very expensive to acquire (a million dollars, for example) or the test is very expensive to conduct, such as jamming a UAS, where approvals to conduct the test may take 6-12 months and the on-site testing cost per day can be extremely expensive.

The notional schedule provided shows the down selection of the top candidates at week 13 and documentation of the selection process and results by week 15. If this level of rigor is appropriate for the T&E of a security technology, it will be important to include this 15-week duration in the T&E schedule and account for the costs in the cost estimate for the T&E activity.

[1] the number 10 is used in this example, but it can be any number the team chooses
[2] The number three is used in the example, but it can be any number the team chooses

When the CA or the appropriate decision-maker approves this plan, the next step is to implement to it.

4. PROCUREMENT OVERVIEW

Procurement is defined as the act or process of procuring or obtaining an item or service. In the context of this document, procurement is not limited to the out-right purchase of an item. Since this document is intended to address T&E of security technologies, which includes component evaluation and implementation as shown in Figure 1-1, the purchase of a technology may not be necessary to evaluate it. A creative T&E team has other, less expensive options that may allow sufficient time to conduct an evaluation.

Of course, the team must comply with governmental laws and regulations and must comply with institutional procedures. When considering procurement options, it is prudent for the T&E team to work with their purchasing professional or department, if they have one.

While staying within the legal and institutional constraints, procurement of a security technology for T&E can be accomplished in several different ways, including:

- Purchasing the product
- Leasing the product
- Leasing the vendor and the product
- Obtaining vendor samples

4.1. Purchase the Product

Outright purchase of a security technology is the likely option if the technology is to be deployed and integrated into a site security system. In this case, there are some decision points to consider.

During purchase negotiations for a technology, it is important to consider the ability of the vendor to provide technical support onsite if the technology is not working as needed. For example, a common problem with installation of sensor technologies is excessive false positive alarms, also called nuisance alarms. The site may have locations with specific forms of RF interference, underground power or communications, or overhead pipes that can induce seemingly random flurries of nuisance alarms. In this kind of circumstance, it may be wise to include a maintenance contract with the vendor, with an agreement that they will be onsite within 48 hours (maybe 24 hours) to correct any problems.

If a system has components with a limited design life, it may be appropriate to also purchase a small inventory of replacement parts or even extra systems to maintain a 24/7 mission. For example, a site purchased and deployed several expensive thermal imagers needed for a critical function, which were thermally cooled. The cooling systems had a design life of 2,000 hours and took 45 days to replace when failures occurred. The coolers could not be replaced onsite; instead, the site had to send the whole imager to the manufacturer for maintenance. In order to maintain a 24/7 capability, the site purchased several extra imagers that could be immediately installed when a cooling system failed. The extra inventory was incorporated in the purchase of the technologies.

When testing technologies that are inexpensive and readily available, such as a passive infrared (PIR) sensor or a low-cost security camera, the most expedient choice may be to purchase the device and test it. If the technology is very expensive or takes an unacceptable amount of time for the vendor to build and deliver, it may be prudent to consider other options, such as leasing.

4.2. Lease the Product

When there is not sufficient budget to purchase an expensive system for component T&E, the vendor may be open to leasing the technology for a sufficient period to allow the team to evaluate their product. If the test results show the product meets requirements, the technology can be purchased. This arrangement allows the vendor to collect some compensation for their technology without the T&E team paying the whole purchase price to see if the technology can meet requirements. Many vendors will be open to this kind of arrangement if they see it leading to a new business area or future sales. For example, recently a T&E team was tasked with evaluating an imaging system. The cost estimate to conduct the evaluation of the system was significant, not including equipment costs. The sponsor did not want to pay that amount of money just to see if this technology would meet requirements. After some negotiations, the vendor was willing to lease the technology for several months at a much lower cost. This reduced the cost of the evaluation roughly by roughly half of the original purchase and evaluation cost. The cost of the lease contract also included vendor providing training to the T&E team on how to use the technology, as well as repair costs if the system experiences component failure. This reduced the financial risk to the sponsor during the process of determining if the technology could meet requirements.

At the time this document was being written, a new business model was introduced by a vendor for procuring and deploying expensive technologies. Rather than have the site purchase the expensive equipment and pay for maintaining the system and covering any associated costs, the vendor proposed leasing the system to the site at a much reduced cost per year, which included the vendor repairing components that fail in the field. This reduced the site's maintenance and deployment costs, allowing rapid acquisition of a new technology. For lower security applications, this new approach could be an advantageous arrangement for acquiring cutting edge technologies. For high security sites with stringent security procedures, this type of lease program may not be acceptable.

4.3. Lease the Product and the Vendor

During the evaluation of several expensive CUAS systems (the example discussed earlier), it was not practical to purchase million-dollar systems for T&E. Additionally, the systems were complex to set up, and it was vital for the team to know the systems were set up properly before testing began to ensure the T&E results were not invalid because of faulty installation.

To address these issues (once the market survey and down select of technologies was completed) the T&E team worked to establish a contract with each vendor to:

- Schedule a technical exchange meeting, allowing the vendor to provide an in-depth description of their technology
- Travel to the test site and set up their system
- Train the T&E team on the proper operation of the system and run any automated data collection features of the system

It is important to emphasize that the T&E team operated the system with vendor representatives present, which allowed the T&E team to identify bugs in the system, work arounds created by the vendor to make their technology work, and allowed the T&E team to evaluate the system using a structured test matrix they designed (rather than the vendor). This is preferred over watching a vendor-choreographed demonstration. Allowing the T&E team members to operate the system also provided additional insight into the limitations and maturity of the system. If the system failed to detect or neutralize a UAS, the vendor was present to verify the system was correctly installed and

operated. After testing was completed, the vendor was able to discuss why the system did not perform as expected during the structured test plan. This approach was advantageous to the T&E team because the million dollar purchase was avoided, the T&E team gained hands-on experience with the system nuances, the vendor made sure the system was set up correctly, the vendor was on site to replace component failures, and the vendor was present to explain why a system performed or did not perform as expected. For time-critical acquisitions and very expensive acquisition costs of a technology, this is the recommended acquisition strategy because it provides the most information in a short period of time.

4.4. Vendor Samples

When a vendor is trying to break into a new market they may be willing to lend a system to the T&E team for an evaluation. Many times, vendor representatives at security conferences or trade shows are open to this type of arrangement because they are trying to give their technology exposure to the security community. Assuming this approach is not counter to legal or institutional restrictions, this is a way for the T&E team to conduct quick evaluations to see if a new, inexpensive technology is capable of meeting security requirements. Normally, however, this type of arrangement does not allow for an in-depth evaluation, which requires possession of a technology for several months.

If the T&E team understands the fundamental physics of the technology, worst case threats can be identified to challenge the performance of a technology. For example, many new low-cost radar systems are being marketed for security applications. This new generation of low-cost radars is the result of automotive industry investments in collision avoidance and autonomous navigation. In this example, a worst-case test would include a slow-moving intruder attempting to crawl across a perimeter. Typical perimeter sectors are 100 meters in length. So, a worst-case test would be constructed to see if the radar can sense the slow-moving crawler at a range of 100 meters. If the radar has a horizontal field of view of 180 degrees, the worst-case test would be detecting the slow-moving crawler at 50 meters. This assumes the radar is located in the middle of the sector. In this example, after determining the radar can detect the worst-case threat, it is important to collect nuisance alarm data (false positive alarms). Collection of nuisance alarm data requires monitoring the radar's alarm output when subjected to the test bed environment for several days, during typical weather conditions. This provides a quick assessment of the radar's ability to meet nuisance alarm requirements. The test data is usually shared with the vendor, assuming the site does not have security practices that would prevent sharing test information. Arrangements to share test results should be discussed and agreed to prior to accepting a sample technology

This page left blank

5. PHYSICAL SECURITY PERFORMANCE TEST AND EVALUATION PROCESS

This section will present the primary elements of creating a sensor test plan and provide sample test matrices and results for an interior PIR sensor and an exterior bistatic microwave sensor. The emphasis will be on test strategy, test set up, and test procedures, with a focus on pre-deployment testing of security components. The rationale for this approach is that a thorough test and evaluation of a security technology during the component performance T&E (see Figure 1-1) will form the basis for test procedures employed in subsequent phases of the T&E lifecycle. After testing fundamentals are established, they are applied to subsequent testing from design through retirement.

The information below describing the test strategy, test setup, and test procedures addresses the core of performance testing. The previous sections of this document were intended to provide a foundation for the information needed to perform testing. In Section 2 the importance of creating good requirements and how to verify requirements was presented. Testing is an effective and powerful way to verify a technology can meet a requirement. In Section 3 information from the requirements was structured and formatted to present to vendors in the market survey to see if they had technologies that could meet requirements. Appendix C shows an example of how vendor information collected from the market survey will be weighted, specifically showing the mandatory requirement (number 9) that asks the vendor to provide raw data, signal data, NAR data, detection performance, etc. Test data provided by the vendor shows their technology has been tested and may be capable of meeting the requirements in your environment. Vendor data can decrease the project and technical risk of selecting non-viable technologies for component T&E. However, vendors may not be willing or able to provide the requested test data, and unfortunately, the testing performed by your team may be the first time a technology is tested against the requirements your design must meet.

5.1. Introduction to Performance Testing for Sensors

Section 1.3 provides a discussion regarding employing an integrator in place of an inhouse capability. If the integrator option is employed, there are several ways they could be involved in the performance testing of the PPSs. They could provide desired data from testing they have conducted on the systems being proposed (this could include performance testing conducted at their own test bed). In this example, the integrator must prove the systems perform as required in an operationally relevant environment to validate that they comply with all prescribed regulatory performance requirements.

The term "performance testing" can have multiple meanings depending on the audience. In this context, we define the term as the process of conducting tests on hardware, software, people, procedures, or systems under known and documented conditions to determine performance in terms of performance metrics.

A few important aspects embedded in this definition include:

- Performance testing can be conducted on hardware, software, people, systems, or procedures
- If testing is to be performed on a system, the elements included in the system must be identified
- The test conditions must be identified and documented

- Performance metrics must be identified

A performance-based security design is constructed using performance metrics produced from testing. Performance metrics are included in the calculation of the probability of security system effectiveness (P_E) [1]. Further discussion on performance metrics is provided in Section 5.3.2.

Performance testing is not limited to a specific step in the T&E lifecycle illustrated in Figure 1-1. It can be applied to every step in the cycle from component T&E through retirement. Typically, the most thorough and rigorous testing is performed during the component T&E. The time allotted to conduct a component T&E can vary significantly depending on the complexity of the system/component being tested and the level of rigor necessary to acquire the desired information. This timeframe can be anywhere from weeks to months, although there is constant pressure to decrease time and cost of component T&E. Consequently, a component T&E test plan is likely to be the most comprehensive and difficult to write. When conducting tests supporting subsequent T&E lifecycle activities, much of the content from the component T&E test plan can be used.

5.2. Creating a Test Plan

In this section an outline of a simple test plan is presented. As an aid to the reader, a sample test plan, which follows the same structure, is also provided in Appendix D and includes instructions on how to fill out each section. The sample test plan is a resource to guide the test team in developing a plan that will address their specific needs, and the reader is encouraged to use all, or parts, of the sample test plan as needed.

This section focuses on steps that can be included in a test plan. The details for the sections in the first part of the outline, from the title page through the introduction, are left up to the writer. It is important to note that Section 1.4 in the Appendix D test plan template addresses technical performance requirements as well as non-technical requirements such as safety, regulatory constraints, OPSEC (Operational Security), and general site security constraints. The non-technical requirements are just as important to the T&E effort as the technical requirements.

As the reader uses the test plan template in Appendix D, the amount of detail included in the introduction will be site/organizationally dependent. This document also provides detailed information on the test strategy, test setup, test procedures, results and analysis, and conclusions in the appropriate sections that follow.

5.2.1. General Outline for a Test Plan and Report

Test Plan Template provided in Appendix D

Title Page

Abstract – if appropriate

Acknowledgements – if appropriate

Table of Contents

List of Figures

List of Tables

Executive Summary

Acronyms

1. Introduction
    1.1. Purpose
    1.2. Scope
    1.3. Background
    1.4. Requirements
    1.5. Selection Criteria
2. Test Strategy
    2.1. Performance Metrics
    2.2. Test Parameters
    2.3. Test Matrix
    2.4. Ideal Conditions, Degraded Conditions, Vulnerabilities, NAR
3. Test Setup
    3.1. Test Equipment
    3.2. Test Configuration
4. Test Procedures
    4.1. Testing Under Ideal Conditions
    4.2. Testing Under Degradation Tests
    4.3. Vulnerability Tests
    4.4. NAR Collection
5. Results and Analysis
    5.1. Results from Tests Under Ideal Conditions
    5.2. Results from Test Under Degraded Conditions
    5.3. Results from Nuisance Alarm Tests
6. Conclusions and Recommendations
    6.1. Conclusions
    6.2. Recommendations
    6.3. Closing Comments

References

Glossary of Terms

Performance Characteristics and Definitions of Sensor Tests

Example Summary Briefing for Tests Conducted

External Distribution

Internal Distribution

The outline provided and the resulting report can serve two functions: the test plan and the test report. Sections 1-4 represent the outline for the test plan, and after completing those first four sections, the test plan is complete. After conducting the tests in the test plan, the results are analyzed and recorded in Section 5. Conclusions that can be drawn from the test results and analyses are documented in Section 6. Completion of Sections 5-6 completes the test report.

5.3. Test Strategy

The fundamental technical reason for creating a test plan is to identify and document tests that will be conducted to show a technology or system can meet technical and/or performance requirements. The results from the tests will provide the technical information necessary to properly design the most effective implementation of that particular device/system based on actual performance characteristics rather than reliance on manufacturer's advertised data. The test plan will convey the rationale used to create the necessary tests, how the tests will be conducted, what data will be recorded, and how the data will be analyzed. A graded testing approach starting with testing under ideal conditions, then progressing to testing under degraded conditions and collection of nuisance alarm data, and finally conducting vulnerability tests is recommended. This approach will provide the most comprehensive evaluation of a system, can reduce cost and schedule to complete the system evaluation, and should be conducted early in the T&E lifecycle (Figure 1-1).

5.3.1. Ideal Test Conditions, Degraded Conditions, Vulnerabilities, NAR

5.3.1.1. Ideal Testing

The philosophy used to establish the number and types of tests to be conducted in a T&E activity is driven by the need to identify the performance characteristics and limitations of the security elements being tested. For this reason, it is recommended that every PPS technology tested begin with a structured set of tests under ideal conditions, which are meant to establish baseline performance. The ideal tests are created to determine if a security technology is capable of meeting requirements under ideal conditions. Ideal testing is followed by testing under degraded conditions and vulnerability testing.

The tests created to determine if the system can meet requirements under ideal conditions can be captured in a test matrix. Creation of a test matrix and an example are given in Sections 5.7.2 and 5.8.2. If the test results show a system cannot meet requirements under ideal test conditions, it is not going to meet requirements under degraded conditions (like harsh weather) or during vulnerability testing. Unless the sponsor requests otherwise, no further testing is required, which saves time and money for the sponsor and the test team. The process of evaluating a system under ideal conditions can be viewed as a control gate or decision point to determine if further investment in testing a system is warranted.

The sponsor may request the test team work with the vendor to correct performance issues identified during ideal testing. This will likely result in schedule slips and additional costs, which the sponsor should be made aware of before the test team pursues this path. The additional effort to help the vendor correct problems may be appropriate, depending on the objectives and scope specified.

5.3.1.2. Degradation Testing

During ideal testing it is common for the team to notice unusual performance characteristics of a technology, even though it successfully met requirements. These insights and observations should be noted, as they may point to conditions that can degrade performance or result in vulnerabilities.

Degradation testing is conducted to determine how a technology performs when subjected to less than ideal conditions, such as rain, fog, dust, or high winds. The test matrix constructed for ideal testing may include hundreds of tests, but it may be difficult to execute hundreds of tests during harsh weather conditions. To address this challenge, a subset of the ideal test conditions should be conducted under degraded conditions. This allows the ideal test results to be compared with degradation test results, giving the test team a "like-to-like" comparison of the technology's performance.

5.3.1.3. Vulnerability Testing

In general, all sensors can be defeated and therefore have vulnerabilities. One of the unfortunate characteristics of vulnerabilities of a system or component is that their absence cannot be proven, but their presence can. Another way of saying this is that a test team (or vendor) cannot prove there are no vulnerabilities in a system. However, the presence of a vulnerability *can* be proven through testing. Existence of a serious vulnerability in a system is often classified to prevent adversaries from using this knowledge to attack and defeat a security system.

Vulnerability testing is different from the ideal and degradation testing in a couple of different ways. The first difference is there is typically no requirement specified regarding vulnerabilities, so there is no explicitly written criterion to determine if the technology under test passes or fails. Often the presence of a vulnerability is an unwritten requirement. If a vulnerability is identified in a system or component, it will be up to the sponsor to decide if the vulnerability represents an acceptable security risk. Identification of a vulnerability early in the PPS T&E lifecycle (Figure 1-1) allows designers to modify the design of a security system in such a way that it mitigates the risk of the identified vulnerability. Another strategy to mitigate sensor vulnerabilities is to design a sensor system using complementary sensor phenomenologies, such that the strengths of one sensor augments the weaknesses (or vulnerabilities) of another.

The second difference regarding vulnerability testing compared to ideal and degradation testing is that the testers are intentionally structuring tests that attempt to exploit possible weaknesses in the technology with the intent of circumventing the intended security. Different types of sensors and sensor models have different vulnerabilities. Identification of vulnerabilities can be accomplished by exploiting the sensor physics, signal processing, installation, degradation factors, CONOPS, or site conditions. Ideal testing and degradation testing will often indicate the possible existence of vulnerabilities or suggest additional testing to better characterize specific vulnerabilities. Vulnerabilities or defeat methods can be described in terms of two categories: (1) **bypassing** defeats a sensor by avoiding the sensor's detection envelope, and (2) **spoofing** allows an intruder to pass through the sensor's expected detection zone without generating an alarm.

For high security applications, it is recommended that approximately 10% of the test budget be allocated to vulnerability testing during the component T&E activity shown in the T&E lifecycle (Figure 1-1). The rationale for this recommendation is that the identification of vulnerabilities early in the T&E lifecycle allows decision makers and designers the opportunity to make informed decisions regarding a component or system early in the lifecycle. The identification of a vulnerability may result in rejection of a technology despite impressive performance under normal conditions.

Sensor bypass characterization is typically easier and less expensive to determine. For example, tests to determine a sensor's detection envelope that reveal how far an intruder must stay away from the sensor to keep from being detected are easy to conduct. Spoofing attacks that could allow an intruder to move through a sensor's detection envelope can be much more difficult to identify. Spoofing attacks require more knowledge of the sensor and can be expensive and time-consuming. Because of the uncertainty associated with the identification of spoofing attacks the recommendation is made to allocate 10% of the test budget to vulnerability testing. This places a limit on how much time and money will be allocated to this effort.

Because of the security sensitivities of techniques and methodologies used to identify defeat methods, this topic will not be addressed in detail in this document.

If results from tests conducted in ideal conditions do not compare well with the CA's performance requirements, vulnerability tests will likely not be required in an evaluation.

5.3.1.4. Nuisance Alarm Testing for Sensors (Interior or Exterior)

When considering the purchase of sensors, the most overlooked performance metrics are nuisance alarm rates (NAR) and false alarm rates (FAR). Definition of and further discussion on NAR/FAR is provided in Section 5.3.2. Collection of nuisance alarm data should be conducted after completing ideal testing. Ideal testing of a sensor can be completed in a few days, whereas NAR/FAR collection may range from a few weeks to several months, depending on the schedule agreed to with the sponsor. Assuming the sensor passed ideal test requirements, the sensor settings should be recorded and fixed prior to initiating NAR/FAR data collection. This ensures the NAR/FAR data collection is based on a set of sensor parameters that also passed ideal testing requirements.

There are numerous case studies where unwitting consumers make large investments in purchasing the latest technology with flashy displays and colorful boxes that are automatically placed around an image of an intruder, showing how well a technology can detect an intruder. The consumer purchases and installs the technology around their site only to encounter an overwhelming number of nuisance alarms or false alarms. At some point, as the NAR/FAR increases to a critical level, the detection goes to zero. It is up to the DT to determine what levels of NAR/FAR are acceptable. Vendors are only too happy to show a consumer how well a technology can detect an intruder, but are less enthusiastic about telling the consumer the NAR/FAR. Unfortunately, this scenario continues to persist at the cost of the consumer. As a result, it is good practice for a consumer to ask for NAR/FAR data from the vendor and at a minimum install the sensor technology in their environment (or similar) and monitor NAR/FAR for 10-to-30 days before purchasing the technology.

Typical maximum NAR/FAR requirements are:

Exterior Sensor

- Three nuisance alarms per 24-hour period per sensor averaged over a 30-day period
- One false alarm per 24-hour period per sensor averaged over a 30-day period

Interior Sensor

- Three nuisance alarms per 2,400-hour period per sensor averaged over a 100-day period
- One false positive alarm per 2,400-hour period per sensor averaged over a 100-day period

When conducting a thorough evaluation of a sensor technology, the process of collecting NAR/FAR data will be the most time-consuming element and can be an expensive task if the infrastructure to collect and assess NAR/FAR has not been automated.

5.3.2. Sensor Performance Metrics

Per the definition of performance testing provided in Section 5.1, performance metrics must be identified and collected from the test results. For sensors, the key performance metrics are:

- NAR/FAR Nuisance Alarm Rate/False Alarm Rate
- P_S Probability of Sensing an Intruder

These key performance metrics will likely be specified in requirements for an intrusion detection system. There will be other requirements for a detection system such as temperature, humidity, and weather conditions a technology must be capable of withstanding while providing reliable performance. For example, a sensor may be required to function within a temperature range from -46˚C to +66˚C (-50˚F to +150˚F). Although very important to the ultimate performance and reliability of the deployed security technology, these types of requirements are not specifically addressed in this manual.

5.3.2.1. NAR/FAR

NAR and FAR are an integral part of a sensor's performance. Nuisance alarms are caused by a stimulus other than an actual adversary. Nuisance alarms can sometimes be attributed to sub-optimal settings of operating parameters but are most commonly encountered in technologies that cannot perform in the desired environment. The number of nuisance alarms generated in a given environment is often directly influenced by the detection sensitivity of a sensor. For example, when a sensor is adjusted to a more sensitive setting, thus improving its ability to detect an adversary, it will be more prone to alarm on stimuli other than an adversary, such as gusts of wind, rainfall, or changes in temperature.

False alarms are alarms for which an external stimulus cannot be identified. They are sometimes caused by faulty electronics within the sensor, such as intermittent shorting of electrical contacts. Generally, the cause of false alarms is not known immediately, and they are not diagnosed until the frequency increases to the point where maintenance or repair of the sensor is required. False alarms are also referred to as unknown alarms because it is possible they are being caused by an intruder attempting to spoof or bypass a sensor. Unknown alarms should be kept to an absolute minimum by using proper assessment and good maintenance practices.

NARs and FARs are performance metrics that reflect how well a sensor can be expected to perform under operational conditions. Ideally, nuisance alarm collection periods should span all conditions a sensor is expected to see in an operational environment. During performance testing of interior and exterior sensors, automated systems can be used to monitor a sensor constantly (24/7) for nuisance alarms over an extended period. Even though interior sensors do not directly experience the weather conditions from the four seasons (as do exterior sensors), they do experience differences in heating, air conditioning, hot or cold surfaces, and warm or cold air currents resulting from personnel entry or exit. An example of a table (Table 5-18) showing NAR collection is provided in Section 5.8.5. Both NAR and FAR are quantified in terms of "alarms/24-hour period."

5.3.2.2. P_D – Probability of Detecting an Intruder

P_D is the product of P_S, P_A, and P_T[3,4]. Because the formal definition of probability of detection requires metrics for P_A and P_T, they are not normally known during component sensor testing. For convenience in this discussion, both P_A and P_T are assumed to equal to a value of "1." The actual P_D of the intrusion detection system (IDS) can be determined after the design of the IDS is known and tested.

The expression for P_D, showing the dependency on P_S, P_A and P_T is provided below:

$$P_D = P_S * P_A * P_T$$ [5]

Probability of detection is a metric that characterizes the IDS (as opposed to a component) and will be quantified after the installation is complete. P_S can be quantified during the component test and evaluation step of the T&E lifecycle.

5.3.2.3. P_S – Probability of Sensing an Intruder

P_S is the probability that an intrusion detection sensor will sense an unauthorized intruder within the sensor's detection envelope. Sufficient data must be acquired in order to determine the probability of sense for a given sensor with a given statistical certainty. The requirement for P_S with the associated statistical certainty will likely vary relative to the nature of what is being protected. For high-security applications, the sensor and assessment system might be required to achieve a minimum of a 90% probability of sensing with a 95% confidence level. Based on binomial reliability values extracted from Table 5-1. Binomial Reliability Table in Section 5.6, this metric would require a sensor to detect 30 out of 30 attempts in order to achieve this level of performance. Each series of tests (such as walk tests, slow walk tests, or crawl tests) should be conducted independently for statistical accuracy. In this example, 30 walk tests, 30 slow walk tests, and 30 crawl tests would be conducted.

5.3.2.4. P_T – Probability that an Alarm Indicator will be Transmitted

P_T is the probability that an alarm indication will be transmitted or communicated effectively and in a timely manner to an evaluation or assessment point. This metric will be established after the sensor and the communications infrastructure is installed at the site.

5.3.2.5. P_A – Probability of Assessing the Cause of an Alarm

Assessment refers to the process to determine the cause of an alarm. More specifically, a decision must be made to determine whether an alarm was caused by an intruder or not. Assessment can be accomplished by presenting an image of the alarm stimulus to an alarm monitor or by direct visual observation. The methodology and metrics to quantify the effectiveness of alarm assessment, such as resolution and timeliness, will not be addressed in this document but will be included in subsequent revisions.

---

[3] Garcia, M.L., *Design and evaluation of physical protection systems*, Butterworth-Heinemann, 2007.

[4] Probability of Detection = Probability of Sense (P_S) * Probability of Communication (P_T) * Probability of Assessment (P_A). For detection of an intruder to occur, three things must happen: the sensor must work properly (Ps), the intrusion must be communicated to the CAS (P_T), and the response force must assess the alarm (P_A). If any of those conditions fail to be met (i.e., the guard ignores the alarm), detection does not occur.

[5] Garcia, M.L., *Design and evaluation of physical protection systems*, Butterworth-Heinemann, 2007.

5.3.3. Test Parameters

Per the definition of performance testing cited in Section 5.1, the test conditions must be identified and documented. The description of the test conditions is captured by identifying the test parameters associated with the execution of the test. Test parameters include the controlled parameters and the uncontrolled parameters. The term "controlled" implies these parameters are controlled during the experiment. Examples of controlled parameters are cited in the outline below. The term "uncontrolled" implies these parameters are not controlled in the experiment but are important to record. For example, it might be very important to determine how a sensor performs in rain, but scheduling rainfall for an experiment cannot be done. Notional examples of the test parameters are given in the following outline and specific examples for an interior sensor and exterior sensor are given in sections 5.7.1and 5.8.1.

I. Controlled Parameters

Sensor Settings

- Range setting
- Sensitivity settings
- Timing settings

Test Parameters of the Intruder

- Direction of intruder approach
- Speed of the intruder approach
- Intruder posture
- Intruder size

Installation Information

- Number of units tested (same make and model)
- Mounting height
- Description of the test environment
- Other installation configuration details

II. Uncontrolled Parameters

- Weather conditions (for exterior sensor testing)
- Air conditioning turning on/off (for interior sensors)
- Authorized/unauthorized nearby traffic

5.3.4. Test Matrix

The test matrix generated and recorded in the test plan is essential. A test plan without a test matrix is incomplete. The test matrix represents a structured approach that identifies what tests will be conducted and what data will be recorded under what test conditions. The test matrix will be provided to the test team and will directly influence the cost and duration required to conduct the necessary tests to characterize the security technology. As tests are conducted, the test team will record results of the tests, filling out the test results in the test matrix.

Test parameters must be identified and well-defined to bound the scope and expectations of the testing. Well-defined parameters will also provide the T&E team with a path to consistent testing

and results and enable any follow-on testing to maintain that consistency. Examples of possible parameters to be used for testing an interior and exterior sensor are found in the following sections.

Sample test matrices will be provided for interior and exterior sensors in sections 5.7.2 and 5.8.2

5.4. Test Setup

Specific information must be included in the test setup:

- Description of test equipment used
- Description of the sensor to be tested, including:
    - Make/model of the sensor (including a picture is recommended)
    - Any spec sheets or user manuals that were used (consider placing these in an appendix of the test plan)
- Test configuration, including:
    - Mounting conditions, height, orientation, drawings
    - Sensitivity settings/parameter settings
    - Power supplies required by the technology
    - Connections to communications (and communications protocols if appropriate)
    - Description of the test bed
        - Dimensions of the test bed
        - Environmental conditions
        - Ambient RF environment, if there is a possibility of interference

NOTE: It is recommended that a data acquisition system be employed to collect alarm data, specifically supporting 24/7 NAR and FAR data collection. To determine the cause of an alarm, a video system will be needed that can record (recommended) 5 seconds before and 5 seconds after an alarm is generated by the sensor being tested, allowing a reviewer to determine the cause of the alarm. One or more video cameras will be needed and are selected for the application, including field of view, ability to create an image under environmental/test conditions, range to the area of interest, and imager resolution. The cost of this equipment can vary widely depending on the type and number of sensors, cameras, and video management systems used.

The information included in the test setup are largely controlled parameters and are important to document because they will:

- Allow others to duplicate your tests to verify test results, if desired
- Allow others to test the technology in their site-specific environment, using the same setup, meaning any changes to performance may be attributed to environmental conditions (uncontrolled parameters)

- Provide security designers the models and installation details that will be pertinent to how the technology might be used in the security design and implementation

5.5. Test Procedures

After creating the test matrix and documenting the test setup, the test procedures can be created. The test procedures provide a step-by-step set of instructions for the test team to conduct the test and record data. It is recommended that a draft set of test procedures be provided to the test team to get their input before going to the field. The review of the test procedures may also have safety and/or security implications, so including safety and security personnel during the review of the procedures may prevent dangerous test scenarios or security infractions. It is recommended that the test plan authors document the test procedures, rather than conducting tests based on verbal agreements. The importance of recording the test procedures increases as:

- Members of the test team leave the organization, preventing resolution to questions or concerns about the test results or how the tests were conducted
- Members of the test team cannot remember what was done on a previous test series
- Other organizations planning to duplicate test procedures so they can replicate the tests and compare results

Examples of test procedures are provided for exterior and interior sensors in Sections 5.7.4 and 5.8.4.

5.6. Results and Analysis

The analysis of recorded data is the next step in the experimental process. This step enables the test team to determine if the technology or system under test will meet requirements by comparing the performance metrics produced by the analysis to the requirements specified. For most test series, the analysis of the test data is conducted after the data is collected. It is strongly recommended that a limited analysis effort be conducted on the initial data collected to make sure the data can be analyzed as expected and to determine if there are specific conditions not recorded that will influence the analysis.

Depending on time limitations and access to the test site, there may be limited options to collect additional data or record specific conditions after the team has completed the test series and left the test site. When the team analyzes the first data sets shortly after collecting the data, errors in the recorded data or critical omissions of data are detected and can be communicated to the test team quickly. The detected errors or omissions often result in a change in the test procedures and/or parameters. The test effort will likely be improved by conducting analysis of the initial data collected during the beginning stages of the test period.

For extended duration test efforts (weeks to months) it is recommended that the analysis of the data be conducted daily, and a member(s) of the team be assigned this task. For extended duration efforts, the analysis lead should report back to the test team daily to communicate any errors or data omissions detected, allowing the test procedures to be updated as needed.

5.6.1. Analysis of P_S Data

The typical requirement for describing how well a sensor is expected to sense the presence of an intruder is to specify the probability of sensing an intruder (P_S) and a lower confidence level (C_L).

Estimation of these metrics is based on the binomial tables[6]. For example, if the requirement is a P_S of 90/95 (a probability of 90% with a lower confidence level of 95%), it would require 30 detections out of 30 attempts. An excerpt from the binomial tables is shown in Table 5-1.

Table 5-1. Binomial Reliability Table

		Confidence Level (γ)					
n	r	0.800	0.900	0.950	0.975	0.990	0.995
30	30	0.94777	0.92612	0.90497	0.88430	0.85770	0.83811
30	29	0.90365	0.87643	0.85140	0.82783	0.79841	0.77725
30	28	0.86271	0.83219	0.80467	0.77926	0.76810	0.72600
30	27	0.82380	0.79010	0.76140	0.73471	0.70238	0.67969
30	26	0.78609	0.75101	0.72039	0.69278	0.65967	0.63663
30	25	0.74925	0.71264	0.68103	0.65279	0.61920	0.59598
30	24	0.71311	0.67531	0.64299	0.61433	0.58049	0.55725
30	23	0.67756	0.63886	0.60605	0.57716	0.54327	0.52013
30	22	0.64250	0.60316	0.57007	0.54111	0.50734	0.48440
30	21	0.60740	0.56813	0.53497	0.50604	0.47256	0.44993
30	20	0.57370	0.53372	0.50056	0.47188	0.43882	0.41650
30	19	0.53988	0.49987	0.46691	0.43856	0.40603	0.38430
30	18	0.50642	0.46657	0.43395	0.40604	0.37421	0.35302
30	17	0.47330	0.43378	0.40163	0.37427	0.34325	0.32279
30	16	0.44052	0.40149	0.36995	0.34320	0.31315	0.29331
30	15	0.40807	0.36970	0.33889	0.31297	0.28390	0.26485

The terms in the table are defined as:

- n the number of attempts
- r the number of hits or sensor detections
- γ confidence level

The values in the highlighted box show a probability of 0.90497 (rounded to 0.90) at a confidence level of 0.95 for 30 detections out of 30 attempts. Moving one row below the red box shows a probability of 0.85 with a confidence level of 0.95 for 29 hits out of 30 attempts. A common shorthand notation for a probability of 0.90 at a lower confidence level of 0.95 is "P_S=90/95."

[6] Binomial Reliability Table (Lower Confidence Limits for the Binomial Distribution), by James Cook, et. al., NAVWEPS Report 8090, January 1964.

Examples of P_S estimates based on collected data are provided for an exterior sensor in Section 5.8.5.

5.6.2. Analysis of NAR/FAR Data

The analysis of NAR/FAR data is relatively simple. The NAR/FAR requirements are usually specified in number of alarms per 24-hour period for exterior sensors. Assuming a 30-day NAR collection period, the analysis of the data could include:

- Total number of nuisance alarms recorded during the collection period, with the units of alarms/day
- Nuisance alarm break down, showing the causes of the alarms:
    - Nuisance alarms caused by wildlife, the total number attributed to wildlife, and alarms/day over the 30-day period
    - Nuisance alarms cause by weather, the total number attributed to weather, and alarms/day over the 30-day period (further breakdown of weather conditions might be warranted, such as alarms caused by rain, snow, wind, low sun angle, etc.)

NOTE: This data will be useful to the designers if a sensor is tested in an environment that might be different than the deployment location. For example, if a sensor had low NAR for all conditions except snow, and the deployment location is in the desert and doesn't experience snow, the sensor could be a strong candidate for the intended site location if it met all the other requirements.

- Total number of false alarms during the collection period
    - Number of false alarms that could not be determined using video, for example RF interference could cause an alarm but the video would add not value to assess the cause of the alarm
    - Number of false alarms caused by equipment malfunction, determined after troubleshooting and possibly repair of a sensor, for example:
        - Program or logic faults caused by voltage spikes in the power supply or voltage spikes that come through the electrical ground caused by nearby lightning strikes
        - Wind blowing the sensors out of alignment
        - Water that permeates through gaskets or seals and shorts electronics
        - Faulty solder joints encountered during cold conditions
        - Vendor software monitoring sensor outputs locks up and requires a re-boot

NAR/FAR results are very telling when testing and comparing performance of several different sensor technologies installed side-by-side in a testbed, which guarantees they see the same environmental conditions. NAR/FAR data is typically the most time-consuming part of sensor evaluation. It is recommended that the P_S testing is completed first, identifying the least sensitive setting at which the sensor can detect the required threats. Then the team can use those settings to determine the sensor's NAR/FAR performance.

Examples of NAR analysis are provided for exterior and interior sensors in Sections 5.7.5 and 5.8.5.

5.7. Interior Sensor Examples

This section will apply the concepts described in Sections 5.1 through 5.6 to an interior sensor to provide an example of how to apply those concepts. In this section, we will work all the way through an example, provide sample data from a hypothetical sensor, and complete results and analysis.

The interior sensor that will be used in this example is a wall mounted PIR sensor with 90 degrees of coverage. More specific information on the sensor is included in Section 5.7.3.

5.7.1. Test Parameters (Interior Sensor)

After acquiring the sensor, the test team will familiarize themselves with the technology, including a review of vendor documentation on recommended installation procedures, how to provide power and communications, any network requirements, any computer requirements to run their user interface, etc. After the team is familiar with the sensor and has reviewed the user manual, they are ready to identify a list of the parameters that will be used for this particular evaluation.

I. Controlled Parameters (examples)

Sensor Settings

- Range setting
  - 3 meters to 9.1 meters (fixed at 9 meters during testing) (10 feet to 30 feet [fixed at 30 feet during testing])
- PIR sensitivity
  - High (fixed at high)
  - Low

Test Parameters of the Intruder

- Intruder path
  - Radial
  - Tangential
- Speed of the intruder approach
  - 0.15 m/sec (0.5 ft/sec)
  - 0.3 m/sec (1.0 ft/sec) (fixed at 0.3 mps, needed to meet requirements)
- Intruder posture
  - Walking upright
  - Belly crawling
- Target size (two test subjects were used for testing, large and small)
  - Small: 150 cm and 45 kg (4 feet, 11 inches and 100 pounds)
  - Medium: 168 cm and 68 kg (5 feet, 6 inches and 150 pounds) – not included in testing or test matrix
  - Large: 183 cm and 91 kg (6 feet and 200 pounds)

NOTE: The heights and weights of the test targets used to "bin" the three target sizes are approximate. The actual testing for the interior sensor used a person who was 178 cm tall and weighed 86 kg (5 feet, 10 inches and weighed 190 pounds). The test team thought the height and weight of this test subject was closer to the large target (vs. the

medium target). The second test subject was 150 cm tall and weighed 68 kg (4 feet, 11 inches and weighed 150 pounds). This test subject was a small target size. The target size "bins" are used just as an example. For testing, the actual size and weight of the test subjects should be recorded.

- Test grid configuration
  - The 90-degree field of view was divided into nine, 10-degree increments
  - The 9-meter (30-foot) range was divided into six tangential arcs, spaced 1.5 meters (5 feet) apart

Installation Information

- Number of units tested (same make and model)
  - Unit #1 (only one unit was tested)
  - Unit #2
- Mounting height
  - Mounting between 2.4 and 7.6 meters (8 and 25 feet) – mounted at 2.4 meters (8 feet)

II. Uncontrolled Parameters

- Room temperature
- Air conditioners/heaters turning on/off by facilities
- Power spikes
- Power outages and power resets

5.7.2. Test Matrix (Interior Sensor)

Five test matrices are presented in this section, based on the selected test variables. The first test matrix, labeled "Detect/No Detect-Tangential, Small" is used to establish the performance metric P_S/C_L for a small intruder moving across the PIR's field of view. The remaining four matrices are used to create detection envelopes for large and small intruders moving across the PIR's field of view, referred to as tangential motion, and large and small intruders moving directly toward the sensor, referred to as radial motion.

Describing the test matrices:

- The variable "intruder path" has two levels (radial and tangential)
  - The radial path has 10 test angles or sublevels
  - The tangential path has eleven ranges or sublevels (seven are marked on Figure 5-2, and the other paths are located in between the marked paths to correspond with the indicated paths in Table 5-2)

NOTE: A description of the test procedures to conduct both a radial test and a tangential test are provided in Section 5.7.4

- The variable "posture" has two levels, walk and crawl (belly crawl)
- The variable "speed" has one level, 0.3 m/sec (1 ft/sec)

- The variable "target size" has two levels, small and large

NOTE: It is desirable to have the same two subjects conduct all the tests to provide consistency of results and allow analysts to observe changes in performance that could be caused by the other variables

- The variable "sensitivity" has one level, high

5.7.2.1. Test Matrix to Establish P_S

In order to obtain a P_S/C_L of 90/95, 30 successful detections are required for 30 attempts. In this example the range from the PIR sensor to each tangential arc location was discretized into 11 ranges, starting at zero meters from the sensor and incrementing every 0.75 meters to a maximum range of 9 meters. In order to create 30 tests per condition, three tests or three repetitions were conducted at each of 11 ranges, producing 33 tests. The three repetitions per test condition are signified by the notation "3X" shown in each cell of the matrix. The test matrix to establish P_S only includes tests for the small intruder, representing the more difficult intruder to detect compared to a medium or a large stature test subject.

Table 5-2. Detect/No Detect – Tangential, Small

Tangential Path (in meters)	0	0.75	1.5	2.25	3	3.75	4.5	5.25	6	7.5	9	Number of Attempts	Number of Detects	P_S/C_L
0.3 m/sec walk (dist. from 0-degree line)	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	33		
0.3 m/sec walk (dist. from 90-degree line)	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	33		
0.3 m/sec crawl (dist. from 0-degree line)	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	33		
0.3 m/sec crawl (dist. from 90-degree line)	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	3X	33		
	Tests conducted every 0.75 meter from the sensor to a range of 9 meters, resulting in 33 tests per test condition* * See Figure 5-2 showing "0-degree line" and "90-degree line"*													

A total of 132 tests will be necessary to conduct the full list cited in the test matrix shown in

Table 5-2. In general, the number of tests included in a test matrix are a consequence of how many variables and levels are included in the test plan, which are driven by the test requirements. Adding variables and levels will provide more insight to sensor performance characterization, but this comes at a cost because it will also increase the number of tests, increasing the cost and schedule of the test effort.

For example, adding another velocity of 0.15 m/sec (0.5 ft/sec) will double the number of tests, requiring 264 tests. It is left to the discretion of test team to determine the number of variables and levels needed to collect sufficient data to adequately characterize the sensor. It is assumed that CA approval of the test plan will be required, and the CA may request additional tests if the proposed test matrices will not produce sufficient data to meet requirements.

5.7.2.2. Test Matrix to Establish Detection Envelopes

Table 5-3. Detection Envelope Test Matrix for Radial Paths (Small Test Subject, High Sensitivity)

Description of person conducting test: Small Stature; Height____; Weight_____; (**GREEN**)[7]											Average	Number of Hits
Angle of Radial Path (degree)	0	10	20	30	40	50	60	70	80	90		
0.3 m/sec walk (dist. from sensor)												
0.3 m/sec crawl (dist. from sensor)												
**Radial tests conducted every 10 degrees*												

Table 5-4. Detection Envelope Test Matrix for Radial Paths (Large Test Subject, High Sensitivity)

Description of person conducting test: Large Stature; Height____; Weight_____; (**RED**)											Average	Number of Hits
Angle of Radial Path (degree)	0	10	20	30	40	50	60	70	80	90		
0.3 m/sec walk (dist. from sensor)												
0.3 m/sec crawl (dist. from sensor)												
**Radial tests conducted every 10 degrees*												

[7] Note that the red and green indicators in the tables correspond to the graphical representation of the results, which are shown in sections 5.7.5.2.1 and 5.7.5.2.2.

Table 5-5. Detection Envelope Test Matrix of Tangential Paths (Small Test Subject, High Sensitivity)

Description of person conducting test: Small Stature; Height____; Weight_____; (**GREEN**)								Number of Hits
Tangential Path (distance in meters)	0	1.5	3	4.5	6	7.5	9	
0.3 m/sec walk (dist. from 0-degree line)								
0.3 m/sec walk (dist. from 90-degree line)								
0.3 m/sec crawl (dist. from 0-degree line)								
0.3 m/sec crawl (dist. from 90-degree line)								
**Tangential tests conducted every 1.5 meters from device to 9 meters*								

Table 5-6. Detection Envelope Test Matrix of Tangential Paths (Large Test Subject, High Sensitivity)

Description of person conducting test: Large Stature; Height____; Weight_____; (**RED**)								Number of Hits
Tangential Path (distance in meters)	0	1.5	3	4.5	6	7.5	9	
0.3 m/sec walk (dist. from 0-degree line)								
0.3 m/sec walk (dist. from 90-degree line)								
0.3 m/sec crawl (dist. from 0-degree line)								
0.3 m/sec crawl (dist. from 90-degree line)								
**Tangential tests conducted every 1.5 meters from device to 9 meters*								

5.7.3. Test Setup (Interior PIR Sensor)

5.7.3.1. Description of Test Equipment Used

The equipment used in the evaluation of the interior PIR sensor consisted of the following:

- PIR sensor unit (description of PIR sensor included in Section 5.7.3.2)
- A 90-degree test grid marked on the floor using masking tape (see Figure 5-3)
- Nuisance alarm monitoring system
- Digital video recorder (DVR)
- Power supply for sensor(s)
- Mechanic's creeper (to facilitate the belly crawl)

- Cameras as needed to record nuisance alarms
- Test sheet/test matrix

5.7.3.2. Description of the Sensor to be Tested

- The interior PIR sensor system is a microprocessor-based passive infrared sensor (the test team should include sensor make and model information and any additional sensor description as appropriate)
- The PIR sensor detects intruders by sensing the infrared energy emitted by a human intruder moving in its field of view
- The sensor employs two pyroelectric detectors, one for detecting motion in close proximity below the sensor and the other that covers the longer range of the sensor
- A photograph of the sensor, along with an illustration of the manufacturer's advertised detection area, is shown in Figure 5-1
- The PIR has two sensitivity selections, high and low; the manufacturer states the sensor tolerates environmental extremes better in the low sensitivity mode, while the high sensitivity setting is used when adequate detection is not achieved in the low sensitivity mode; during tests, the PIR was set to "high sensitivity" because adequate detection was not achieved using the low setting
- A copy of the spec sheet and the user manual is included in an appendix to the test report.

NOTE: A copy of the spec sheet should be included, if possible

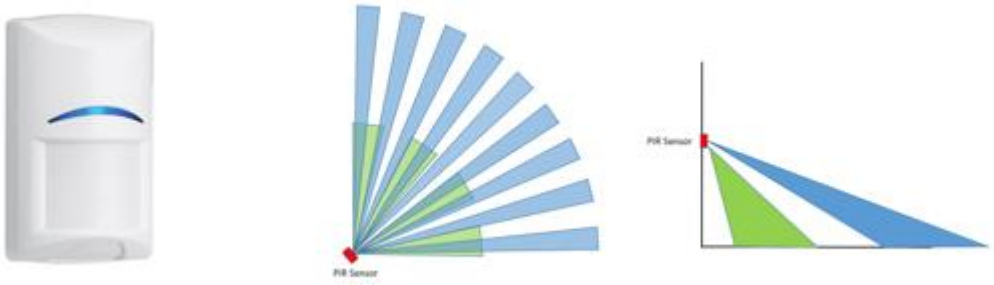


Figure 5-1. Interior PIR sensor

5.7.3.3. Test Configuration

- The test bed was a large conference room, inside an office building; the ambient environment was consistent with an office environment, and the room thermostat was set to 21℃ (70˚F)
- Test bed was a room measuring approximately 24.4 meters by 15.2 meters (80 feet by 50 feet)
- Figure 5-2 shows the dimensions of the test area and camera mounting locations, and a picture of a notional test area is shown in Figure 5-3; note the size of the test area required to evaluate

this sensor, which is larger than most rooms inside a building (when testing an interior sensor, it is desirable to find a room large enough to test the full range of the sensor)

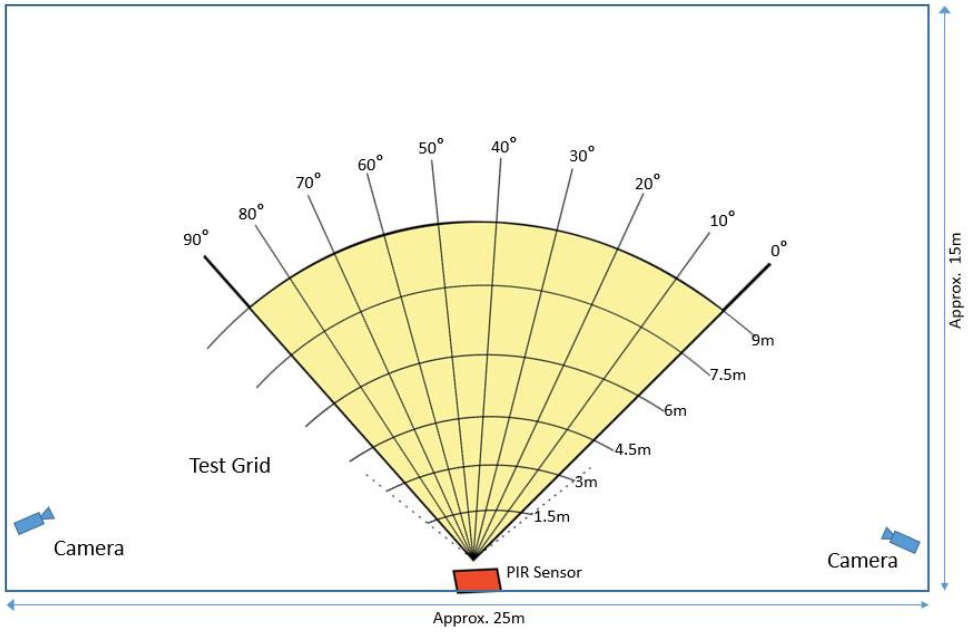


Figure 5-2. Diagram of Test Grid Layout

- The mounting height of the sensor was 2.4 meters or eight feet (the maximum range of the sensor should be 9.1 meters when mounted at 2.4 meters); the test area is large enough to allow at least a 0.75-meter no-detection zone around the sensor detection envelope to minimize NAR/FAR and facilitate accurate detection zone characterization. To facilitate testing, a test grid can be created on the floor of the test bed. Figure 5-3 shows an example of a test grid that was created on the floor of a test bed, using masking tape
- The sensor settings were configured for high sensitivity

Figure 5-3. Example of a Test Grid Layout Using Tape

5.7.4. Test Procedures (Interior Sensor)

The following sections provide the test procedures to establish the probability of sensing the intruder (P_S/C_L) and the detection envelopes of the PIR sensor.

5.7.4.1. Test Procedures to Establish P_S

The test procedures to conduct the tests required to establish P_S/C_L are the same as those to establish the detection envelope, except a Pass "P" or Fail "F" are noted in the test results instead of recording a distance travelled. An example of the test matrix with Pass/Fail notations are provided in Section 5.7.5

5.7.4.2. Test Procedures for Detection Envelopes

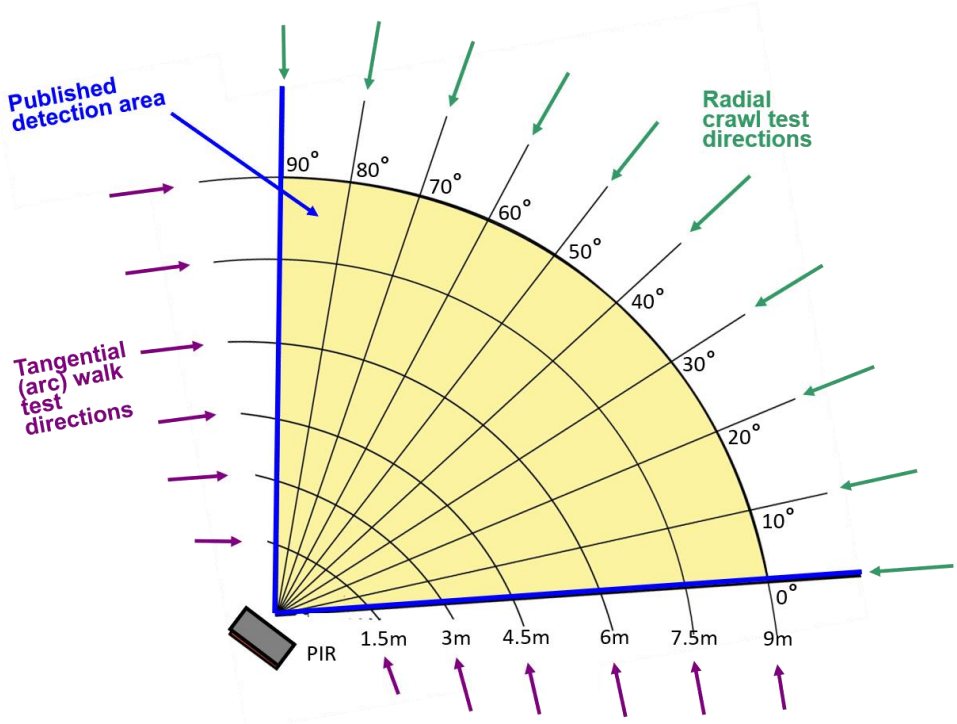


Figure 5-4. Test Grid with Radial and Tangential Paths

5.7.4.2.1. Tangential Tests to Identify Detection Envelope

Figure 5-4 illustrates the tangential paths to be tested, indicated by the purple arrows. Tangential tests are conducted to investigate the capabilities and limitations of the sensor to detect an intruder moving across the sensor's field of view or tangentially with respect to the sensor field of view. In most cases PIR sensors are more sensitive to detecting an intruder moving across the field of view as opposed to an intruder moving directly toward the sensor, referred to as a radial path. This information is important to security designers because it will influence their design, specifically helping them decide where to place the sensor and what dependable detection ranges can be expected. This is especially important when considering that interior PIR sensors are typically placed to detect movement along a path through a room or hallway, etc. Although most pathways can be considered relatively straight lines from point A to point B, to facilitate consistent results, the sensor characterization tests will include testing for detection along tangential arcs across its field of view.

To conduct the tangential test, the test subject will:

1. Start on the 0-degree radial line at the point where it meets the tangential arc 1.5 meters (5 feet) from the sensor
2. Step back from the test angle to ensure they are out of the detection field and wait for 30 seconds (allowing the sensor to reset)
3. When the test coordinator indicates the test start, the test subject will advance at the designated speed, following the arc across the field of detection
4. When the sensor detects the intruder, mark and record the location and advance to the next arc (3 m or 10 ft) and repeat the test as described in the previous steps

The same test should be conducted for each of the tangential arcs from 1.5 m to 9 m (5 ft to 30 ft), starting from the 0-degree radial line. The same procedures should then be followed from the other side of the sensor grid, or the 90-degree radial line. The same test technique should also be conducted with the test subject walking right underneath the sensor, corresponding to a radial distance of zero feet shown in the test matrix

These results will help the designers understand if this path is covered by the sensor, or if it will need to be covered by another sensor. If the sensor does not detect the motion and allows the subject to pass across the entire arc without an alarm, the test should be repeated. If it fails to detect the second time, the result should be noted, and the test subject will move on to the next tangential arc.

5.7.4.2.2. Radial Tests to Create Detection Envelope

Figure 5-4 also illustrates the radial paths to be tested, indicated by the green arrows. A radial test will consist of a simulated radial intrusion at each of the 10 radial locations shown in Figure 5-4. To accomplish one radial test, the test subject will begin outside the detection envelope (for example at 0-degrees and a range of 10.75 meters [35 feet]) and advance toward the sensor until detected.

Once the test subject is detected, the radial distance from the sensor is recorded in the test matrix. The test subject moves to the next starting point (ex. 10-degrees at a range of 10.75 meters [35 feet]), waits for the sensor to stabilize (at least 30 seconds), and conducts the next radial test. Note that a radial test normally results in detection because the test subject continues to advance toward the sensor until detected. If the test subject advances all the way to the sensor (a range equal to zero), a radial distance of "0" is recorded.

NOTE: To accomplish these tests, it is helpful to construct the test grid as noted in Section 5.7.3, Test Setup (see example shown in Figure 5-3). It is important to wait 30 seconds between tests, to make sure the sensor has returned to an undisturbed state

5.7.4.3. Nuisance Alarm Collection

After installing camera(s) in the test bed as-necessary to cover the entire field of detection of the sensor, the sensor and camera(s) should be connected to a system capable of both recording when an alarm is declared by the sensor and recording video of the entire detection field. Ideally, the video recording system will be configured to capture five seconds before and five seconds after the sensor alarm. NAR/FAR collection normally begins when the intrusion test period has concluded. It will operate over night or after the test team has completed activities for that day (i.e. no simulated intruders present). The test team will frequently review the alarms recorded by the system, noting

the number of alarms recorded and the time of the alarms. Using the video management system, the video will be reviewed to determine the cause of each alarm. The test team will record the following results:

- Number of alarms
- Time of Alarm
- Cause of an Alarm

Any other extenuating circumstances that might add value to the NAR/FAR performance should also be noted; for example, if there was a lightning storm overnight or a facility power outage occurred at 3 A.M. and power was restored at 5 A.M..

It may take only a few days to collect intrusion data for this type of sensor, but collection of NAR/FAR data can take much longer for there to be enough useful information. For interior sensors in a relatively sterile indoor environment, it can be expected that there will be few nuisance and/or false alarms.

5.7.5. Results and Analysis (Interior Sensor)

Following the test procedures cited in the previous section, the results from the P_S/C_L tests and the detection envelope tests are presented and discussed.

5.7.5.1. Test Results Establishing P_S

The results from the tangential tests collected to establish P_S/C_L are summarized in

Table 5-7. The notation "3P" indicates three tests were conducted at each test condition and the sensor successfully detected all three attempts. Given 33 detections were recorded for 33 attempts, a P_S/C_L of 91/95 can be estimated using the binomial tables discussed in Section 5.6. The value of 91/95 is shown in the table, which is a consequence of conducting 33 of 33 tests as opposed to 30 of 30 tests. The important result from these tests is that a value of P_S/C_L greater than 90/95 was established.

Table 5-7. Detect/No Detect – Tangential, Small

Tangential Path (distance in meters)	0	0.75	1.5	2.25	3	3.75	4.5	5.25	6	7.5	9	Number of Attempts	Number of Detects	Ps/C_L
0.3 m/sec walk (dist. from 0-degree line)	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	33	33	91/95
0.3 m/sec walk (dist. from 90-degree line)	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	33	33	91/95
0.3 m/sec crawl (dist. from 0-degree line)	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	33	33	91/95

Tangential Path (distance in meters)	0	0.75	1.5	2.25	3	3.75	4.5	5.25	6	7.5	9	Number of Attempts	Number of Detects	Ps/C_L
0.3 m/sec crawl (dist. from 90-degree line)	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	3P	33	33	91/95
**Tests conducted every 0.75 meter from the sensor to a range of 9 meters, resulting in 33 tests per test condition*														

Performance metrics like P_S should be conducted and verified both during component T&E and after being installed with application-specific requirements. For example, if the need is to detect a person walking or crawling from point A to point B in a specific field installation, the sensor should be installed at the site so the intruder path lies across its field of view, maximizing the probability of detection. The sensor should then be tested in this deployed configuration. The process of certification testing is described in Section 8.

5.7.5.2. Test Results to Establish Detection Envelopes

5.7.5.2.1. Radial Tests

The data collected to establish the detection envelopes for the radial and tangential intruder paths are shown below.

Table 5-8. Radial Intruder Path Detection Envelope Data (Large Test Subject)

Description of person conducting test: Large Stature; Height: 178 cm; Weight: 86 kg (**RED**)											Average	Number of Hits
Angle of Radial Path (degree)	0	10	20	30	40	50	60	70	80	90		
0.3 m/sec walk (dist. from sensor)	7.6	5.2	7.9	6.4	8.2	6.7	7.6	6.7	8.5	7	7.2	10
0.3 m/sec crawl (dist. from sensor)	5.4	4.6	5.4	4.3	5.2	5.5	7.3	3.7	5.2	4.6	5.1	10
**Radial tests conducted every 10 degrees*												

Table 5-9. Radial Intruder Path Detection Envelop Data (Small Test Subject)

Description of person conducting test: Small Stature; Height: 150 cm; Weight: 68 kg (**GREEN**)											Average	Number of Hits
Angle of Radial Path (degree)	0	10	20	30	40	50	60	70	80	90		
0.3 m/sec walk (dist. from sensor)	6.4	4	7.3	6.1	7	4.6	7.3	5.2	7.6	6.1	6.2	10

Description of person conducting test: Small Stature; Height: 150 cm; Weight: 68 kg (**GREEN**)											Average	Number of Hits
0.3 m/sec crawl (dist. from sensor)	4.6	2.4	5.2	3.7	4.3	2.1	7	4.6	4.6	3.7	4.3	10
**Radial tests conducted every 10 degrees*												

When collecting data to establish the detection envelope, the test procedure will almost always yield a detection rate of 100%, unless the detection range is zero. Examining the results from Table 5-8 and Table 5-9 show the average detection range for the large radial crawler is 5.1 meters and is 7.2 meters for the large walker. In both cases the average detection range is less than that advertised by the vendor (30 feet). It is expected that the sensor detection for the walker is better than for the crawler. However, it may be somewhat troubling that the sensor had a few very short detection ranges for the small radial walker; for example, 10 degrees and 50 degrees at 5.1 meters and 6.7 meters , respectively. This erratic detection performance is illustrated in Figures Figure 5-5 and Figure 5-6.

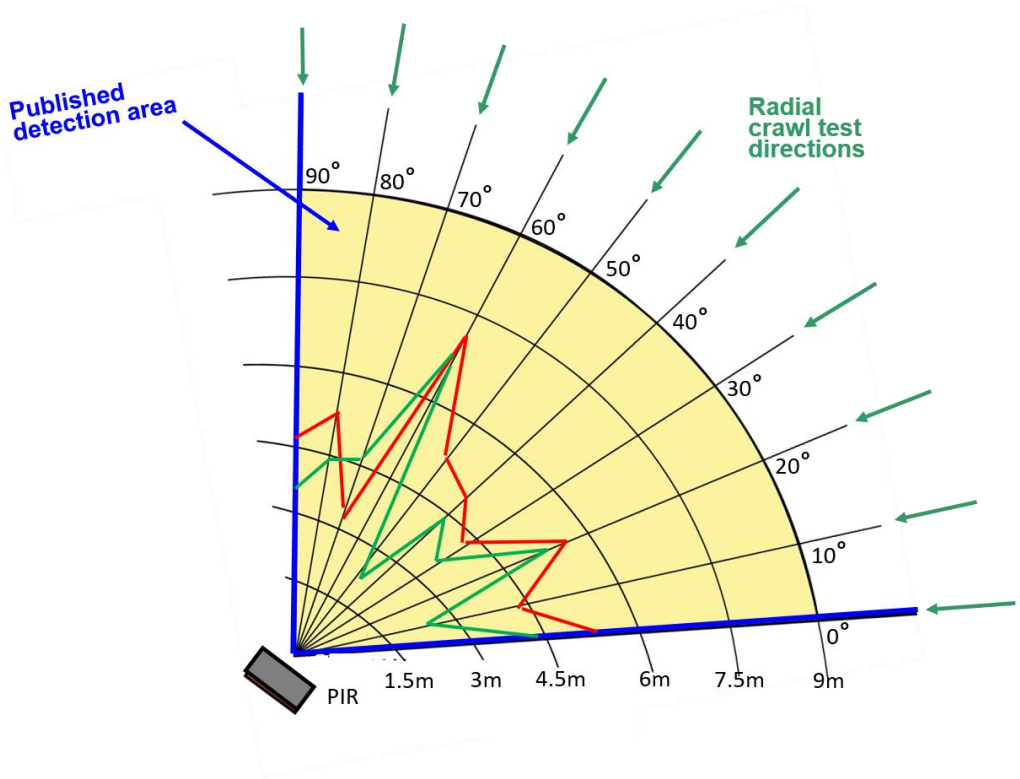


Figure 5-5. Radial Crawler

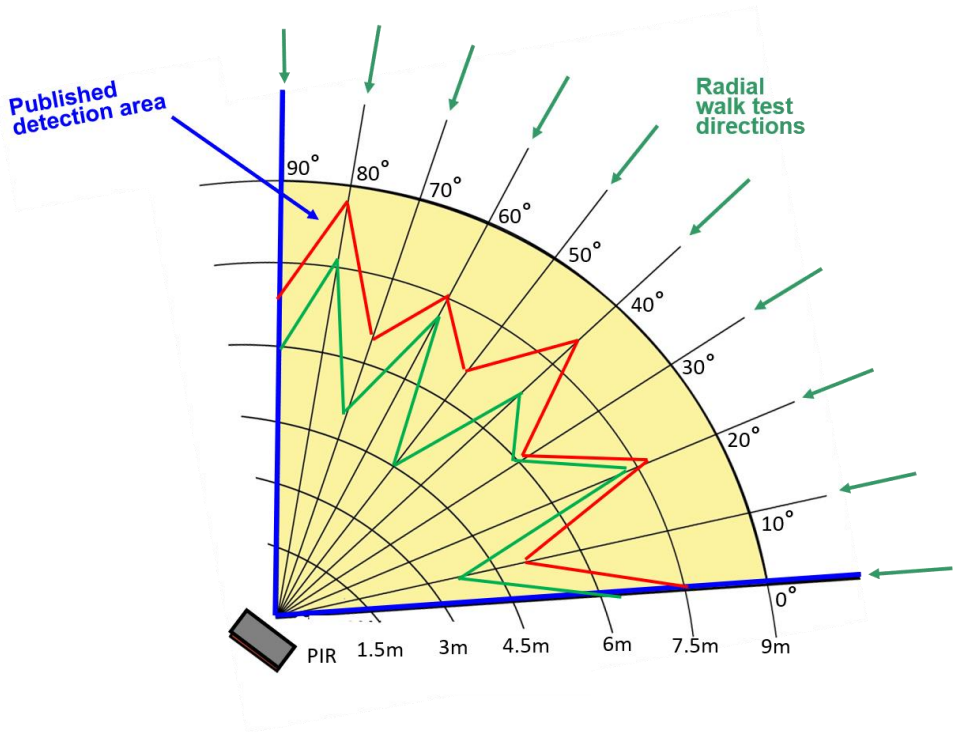


Figure 5-6. Radial Walker

It may be troubling that the radial walker and radial crawler (FiguresFigure 5-5 andFigure 5-6) had large fluctuations in detection ranges. However, one explanation for this could that this PIR sensor uses two pyroelectric detectors, each with its own lens focusing the thermal energy in segments on to the detector with spaces of no detection between the segments. (see the image on the far right in Figure 5-1 in Section 5.7.3).

This phenomenon illustrates that this type of sensor is not meant to be installed primarily to detect movement radially toward the sensor. The IDS design should take this into account when considering placement of the sensor.

5.7.5.2.2. Tangential Tests

The results from the test bed tangential test are shown in Table 5-10 and Table 5-11. The data in the table indicates the average detection envelope of the walking intruder is generally larger than that of the crawler and the detection envelop of the smaller subject is smaller than that of the larger subject. This is consistent with PIRs, as the walker has a larger area for the PIR to detect. Figures Figure 5-7 and Figure 5-8 illustrate the results of the actual detection envelope for tangential movement across the field of view of the sensor, both for the large and for the small test subjects. This information will be useful in designing the placement for this sensor to provide the most effective detection, which is detecting movement along a path across the field of view of the sensor.

Table 5-10. Tangential Intruder Path Detection Envelope Data (Large Test Subject)

Description of person conducting test: Large Stature; Height: 178 cm; Weight: 86 kg. (**RED**)								Average
Tangential Path (distance in meters)	0	1.5	3	4.5	6	7.5	9	
0.3 m/sec walk (dist. from 0-degree line)	0.3	0.3	1.2	1.2	0.6	1.5	1.2	0.9
0.3 m/sec walk (dist. from 90-degree line)	0.3	0.3	0.6	1.2	0.6	2.1	1.8	1.0
0.3 m/sec crawl (dist. from 0-degree line)	0.3	0.9	0.6	0.9	2.1	1.8	2.4	1.3
0.3 m/sec crawl (dist. from 90-degree line)	0.3	0.6	0.9	1.5	1.2	1.5	2.1	1.2
**Tangential tests conducted every 1.5 meters from device to 9 meters*								

Table 5-11. Tangential Intruder Path Detection Envelope Data (Small Test Subject)

Description of person conducting test: Large Stature; Height: 150 cm; Weight: 68 kg. (**GREEN**)								Average
Tangential Path (distance in meters)	0	1.5	3	4.5	6	7.5	9	
0.3 m/sec walk (dist. from 0-degree line)	0.3	0.9	0.9	1.5	1.5	1.88	2.4	1.3
0.3 m/sec walk (dist. from 90-degree line)	0.3	0.6	1.2	1.2	0.9	2.4	3	1.4
0.3 m/sec crawl (dist. from 0-degree line)	0.3	0.9	1.5	1.5	2.4	2.1	2.7	1.6
0.3 m/sec crawl (dist. from 90-degree line)	0.3	0.6	1.2	1.2	1.5	2.1	3.4	1.5
**Tangential tests conducted every 1.5 meters from device to 9 meters*								

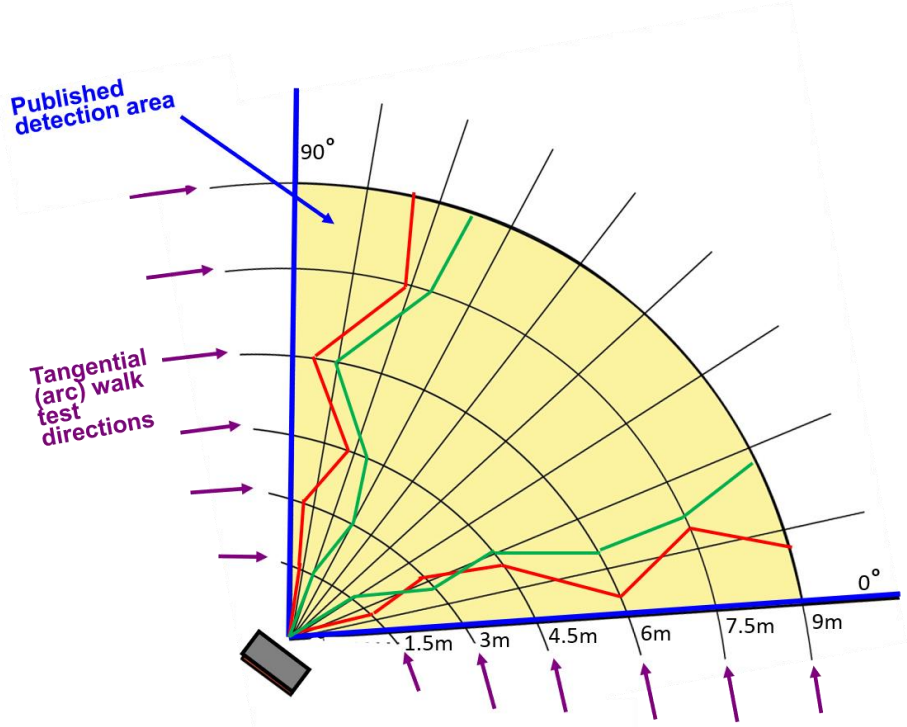


Figure 5-7. Detection Envelope-Tangential Walker

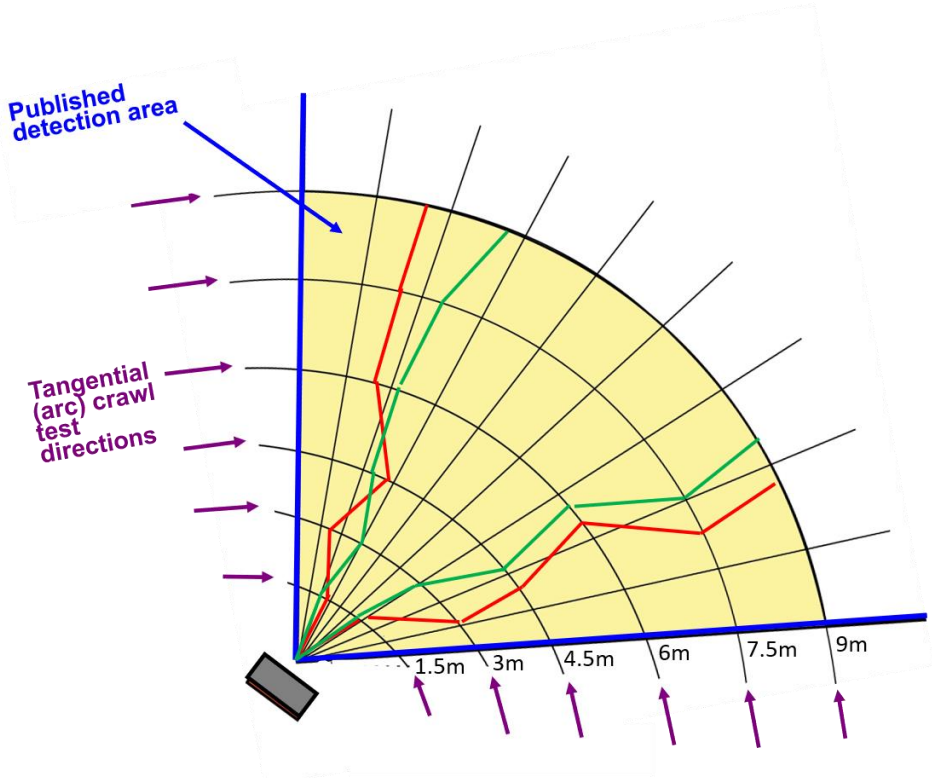


Figure 5-8. Detection Envelope-Tangential Crawler

As mentioned in the discussion on radial tests, an important result of these tests is the realization that this PIR does not perform as-advertised (90-degree detection zone) when the sensor is subjected to the test environment described in this document. But this should not disqualify the sensor from being used, as long as the designers place the device to maximize its detection capabilities based on test results.

Because the results from this test example yield less-than-advertised detection ranges, it may be necessary to install multiple sensors to provide complete coverage of all potential pathways and ensure there are no viable pathways an adversary could exploit. These characterization tests will provide the designers with information to enable an effective implementation.

5.7.5.3. Results from NAR Collection

Nuisance alarm data from this sensor was collected over a one-month period, monitoring the sensor 24-hours-a-day, every day during that one-month period. No nuisance alarms were recorded. This is not unusual for results obtained in a carefully controlled test environment. It will be essential to again monitor for NAR/FAR after the sensor has been installed in the location for its ultimate deployment. Only then can it be determined if there are sources that can/will cause unacceptable NAR/FAR results.

5.8. Exterior Sensor Examples

This section will apply the concepts described in Sections 5.1 through 5.6 to a bistatic microwave exterior sensor. The COTS sensor will consist of a "double stack" sensor, meaning two sensor heads are mounted on a solid base, see Figure 5-11. The lower sensor head will operate at 24 GHz and the upper sensor head will operate at 10 GHz. More details on the sensor, mounting, and test bed will be provided in Section 5.8.3, Test Setup. The test matrices shown will serve two purposes, 1) Determine the sensor's ability to sense the presence of an intruder (P_S/C_L), and 2) Allow the estimation of the detection envelope, i.e., the region where the detection occurs. This information will be of value to the design efforts for the system.

NOTE: For lower security applications, it is also common to use a single microwave sensor on the post. The advantage to using a stacked configuration is the 24 GHz sensor mounted close to the ground reduces the dead zone immediately next to the sensor head and the 10 GHz sensor produces a larger detection envelope.

5.8.1. Test Parameters (Exterior Sensor)

I. Controlled Parameters

Sensor Settings

- Sensitivity setting
  - 24 GHz (fixed sensitivity for all tests – per vendor recommendations)
  - 10 GHz (fixed sensitivity for all tests – per vendor recommendations)

Test Parameters of the Intruder

- Intruder path
  - Perpendicular to transmit (Tx)/receive (Rx) beam path
- Speed of the intruder approach
  - 0.15 m/sec (0.5 ft/sec) (crawling, walking)

- 0.3 m/sec (1.0 ft/sec) (crawling, walking)
- 5 m/sec (16 ft/sec), or as fast as can safely move (running)

- Intruder posture
  - Standing upright
  - Hands and knees crawling
  - Belly crawl
  - Aluminum sphere (used to simulate belly crawl for convenience)
  - Rolling (not included in test matrix)
- Target stature
  - Small: 150 cm and 45 kg (4 feet, 11 inches and 100 pounds) (a small stature person was used for all tests)
  - Large: 183 cm and 91 kg (6 feet and 200 pounds) (not included in test matrix)

NOTE: It is important to recognize that more parameters can be added (such as the rolling intruder), but this will increase the size of the test matrix, the number of tests that will be conducted, and the cost and schedule to complete the testing activity. When adding test parameters, the test team must assess the value of additional information versus the cost to acquire the additional test data.

Installation Information

- Mounting height of sensors (per vendor recommendations)
- Alignment reading (per vendor recommendations)
- Distance between Tx and Rx heads (116 meters)
- Test distance from Tx to Rx (every 3 meters starting 3 meters from the Tx)
- Distance from fence line
  - Middle of the test bed (mid-line between two fences)

II. Uncontrolled Parameters

- Wind and resulting fence movement
- Rain (puddling or running water)
- Snow
- Wildlife
- Blowing debris

5.8.2. Test Matrix (Exterior Sensor)

Tables

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100
Small Stature																																				
Posture	Speed																																			
Runner	4.9 m/sec*																																			
Walker	0.3 m/sec																																			
Belly Crawl	0.15 m/sec																																			

Al Ball Drag	0.3 m/sec																																			

**or as fast as safely possible*

,Table 5-13, andTable 5-14 are examples of three different test matrices. The first matrix, labeled "Detect/No Detect Matrix – All Threats," identifies the test conditions to estimate P_S/C_L performance for multiple types of intruders attempting to pass through the detection envelope of the microwave sensor. Test results will be indicated in the proper cell by inserting "P" for pass or "F" for fail, indicating if the sensor detects or doesn't detect the intruder. The test results from this matrix will be used to determine if the sensor can meet the security performance requirements. Note that the test locations start at three meters and continue through to 103 meters, even though the desired length of the detection is 100 meters, indicated by the grey background in the table. The additional three meters on either side of the 100-meter distance provides detection data within the recommended eight-meter stand-off that will be used when deployed. This ensures good detection at the microwave cross over points as shown in Figures Figure 5-9 and Figure 5-10.

The second and third test matrices identify the test conditions to estimate detection envelope for a small stature walker and the aluminum ball, simulating a small stature belly crawler. This information will be used by the security designers when laying out the sensor spacings and overlaps. Additional test conditions may be of interest and used to expand the test matrices to better understand the performance of the sensor, but the three examples provided in this section are limited for the sake of brevity.

Table 5-12. Detect/No Detect Matrix – All Threats

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103	Number Attempts	Number Detects	P_S/C_L
Small Stature																																									
Posture	Speed																																							
Runner	4.9 m/sec*																																							
Walker	0.3 m/sec																																							
Belly Crawl	0.15 m/sec																																							
Al Ball Drag	0.3 m/sec																																							

**or as fast as safely possible*

Table 5-13. Detection Envelop for Al Sphere

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103
Small Stature																																						
Al Ball Drag (unsecure to secure, see Fig 5-13)	0.3 m/sec																																				
Al Ball Drag (secure to unsecure)	0.3 m/sec																																				

Table 5-14. Detection Envelop for Walker

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103
Small Stature																																						
Walker (unsecure to secure, see Fig 5-13)	0.3 m/sec																																				
Walker (secure to unsecure)	0.3 m/sec																																				

5.8.3. Test Setup (Exterior Sensor)

The equipment required in the evaluation of the microwave sensor includes:

1. Two microwave heads, a transmitter and a receiver
2. A 100 m measuring tape
3. The 116 m test bed layout shown in Figure 5-9
4. Marking tape or stakes to mark the specified range points
5. Short (1.5-inch) PVC pipe with bright marking tape to be used for marking detection envelop (approx. 40 pieces)
6. Nuisance alarm monitoring system
7. DVR
8. One camera (or more) as needed to assess the cause of alarms
9. Test sheet/test matrix

Figure 5-9 provides dimensions of the spacing and location of the test bed for the microwave transmitter and receiver. The lighter red dashed lines represent the bounds of the test zone. The heavy red dashed line denotes +/-3 m beyond the desired test zone, allowing the team to determine how detection degrades beyond the desired detection zone. The 8 m standoff distance between the microwave heads and the beginning of the desired detection zone or test zone is incorporated into the test bed layout and is useful because it will allow for standoff when incorporating multiple microwave units in a basket weave configuration, as shown in Figure 5-10.

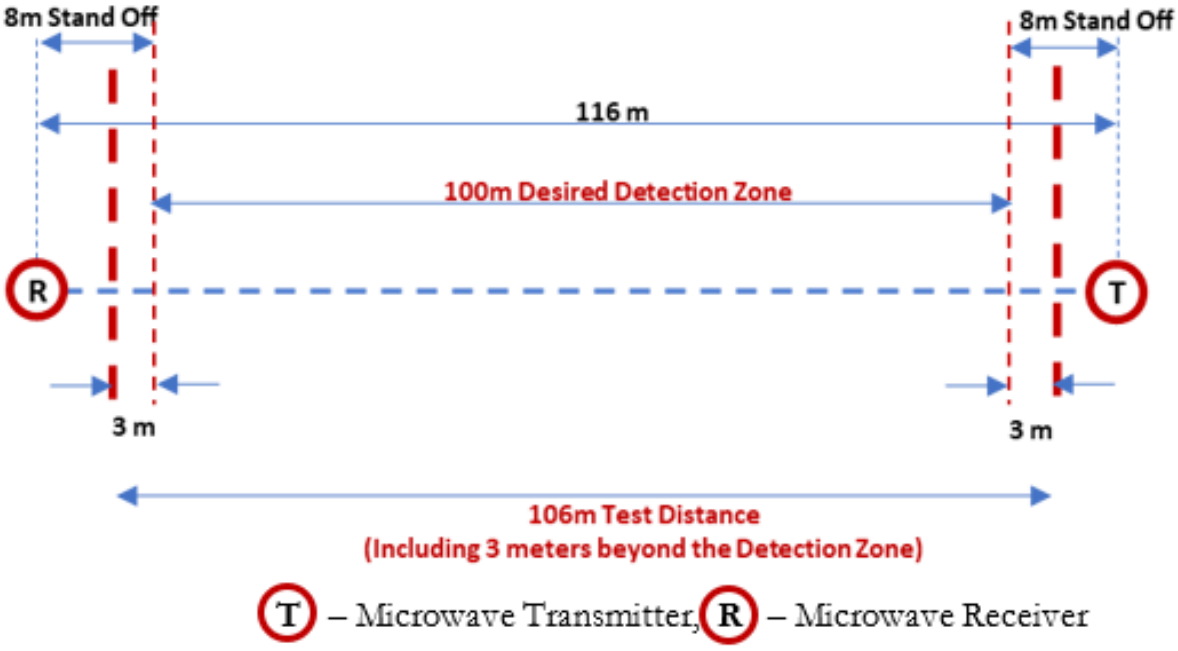


Figure 5-9. Dimensions of Layout for Microwave Test Bed

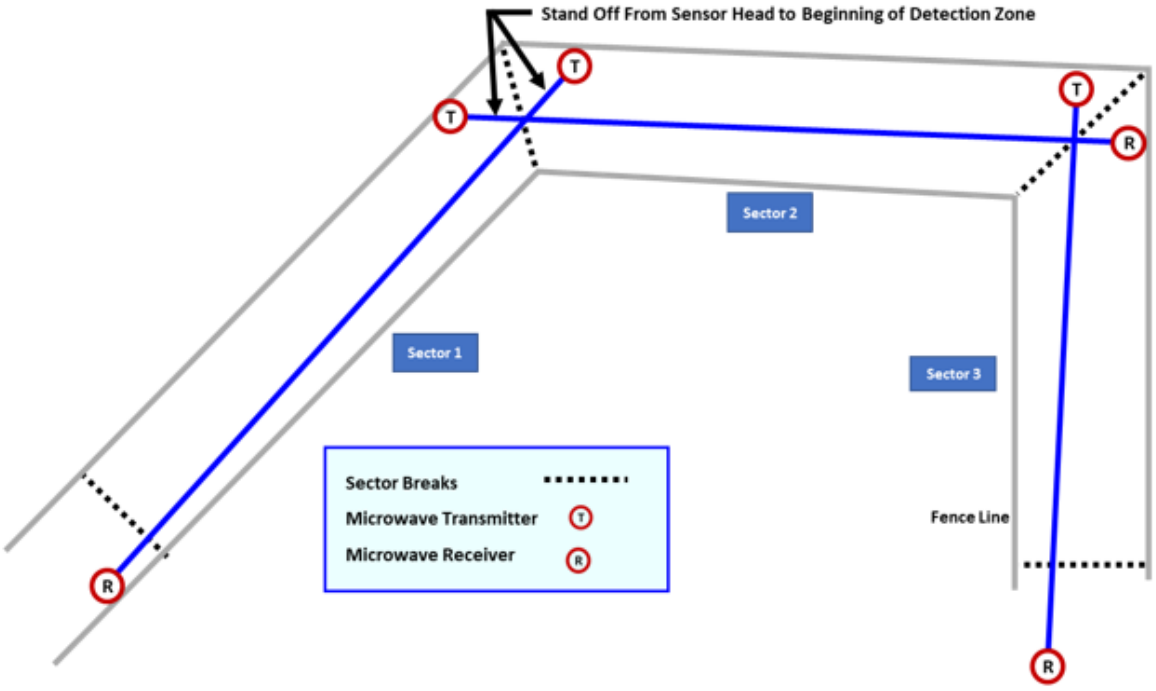


Figure 5-10. Notional Microwave Layout Showing Stand Offs from Sector Breaks

An example of mounting a double-stacked microwave sensor is shown in Figure 5-11. Although it is not within the scope of this document to provide installation directions for the microwave sensors, it is important to note that the distance from the bottom microwave head to the grade of the test bed will dictate the size of the resulting dead zone, which could allow a belly crawler to go under the bottom beam undetected. There will also be a dead zone in the spacing between the top and the bottom sensor heads (Figure 5-12). Understanding the existence and size of these dead zone spaces provides the needed information for the designers to ensure the stand-off distance (typically 8 m) is sufficient to cover these areas when overlapping the detection envelopes of adjacent zones, as illustrated in Figure 5-10. This will ensure a continuous line of detection, a fundamental principle of designing an IDS.

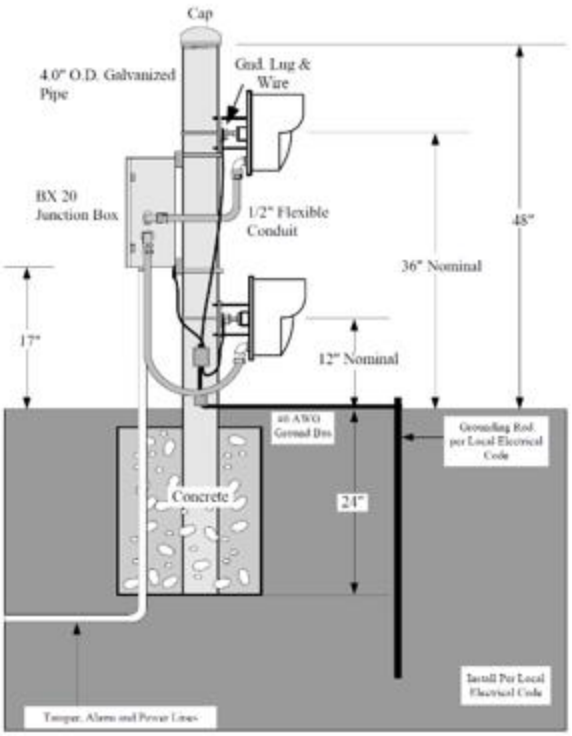


Figure 5-11. Dual Stack Microwave Installation Details

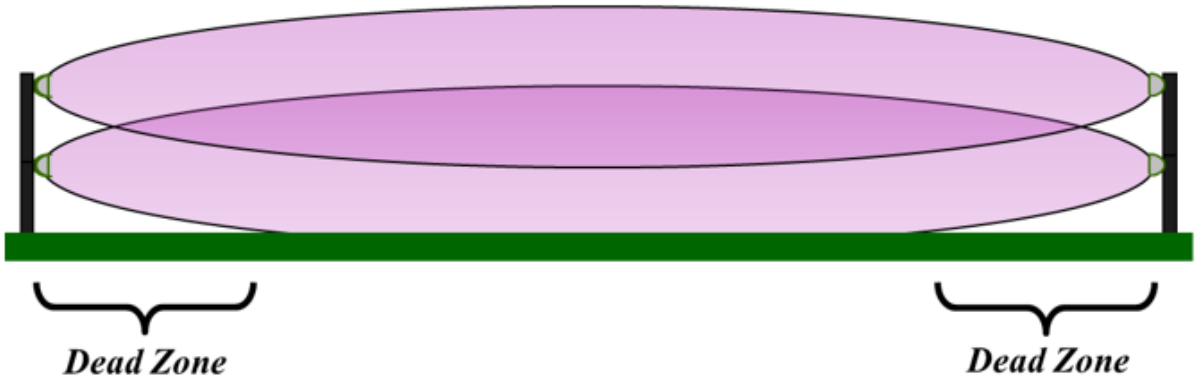


Figure 5-12. Microwave Dead Zones

5.8.4. Test Procedures (Exterior Sensor)

5.8.4.1. Detect/No Detect Tests Using Human Test Subject

The process for testing for the detect/no detect zone is as follows:

1. Layout test grid to facilitate testing every three meters between the Tx and Rx, consistent with the test matrices, Tables

Distance (in meters)	-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100

Small Stature																																			
Posture	Speed																																			
Runner	4.9 m/sec*																																		
Walker	0.3 m/sec																																		
Belly Crawl	0.15 m/sec																																		
Al Ball Drag	0.3 m/sec																																		
**or as fast as safely possible*																																			

2. , Table 5-13, and Table 5-14
3. Position the test subject outside the detection zone of the microwave at the desired range, and remain motionless for at least 30 seconds
4. When the test coordinator tells the test subject to begin, they will advance across the location of the detection zone specified in the test matrix, from one side of the detection zone to the other, as shown in Figure 5-13
5. The test subject continues to advance across the detection zone of the sensor, from the unsecure side to the secure side, until either a detection is declared by the sensor or the test subject advances all the way across the detection zone with no detection
6. Results from each test are recorded in the test sheet and the test subject moves to the next location; after an appropriate time for the sensor to re-set (estimated at 30 seconds), step 4 is repeated.
7. Repeat the same procedure using each of the crossing techniques at each three-meter location shown in the test matrix; additional instruction for using the aluminum ball in place of the belly crawler (oriented with body parallel to the center line) is found in the next section

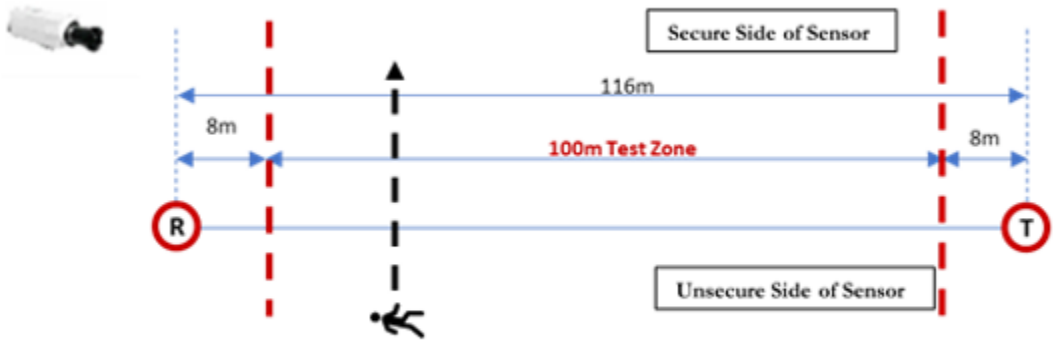


Figure 5-13. Test Subject Advancing Across Microwave Detection Zone

5.8.4.2. Detect/No Detect Tests Using Aluminum Ball/Radar Target

The test procedure using the aluminum ball (an aluminum sphere with a 30.5 cm [12-inch] diameter) is similar to the previous steps provided, with the exception that it takes two people to conduct a test.

1. Use the same three-meter layout test grid as in the previous exercise
2. Two people position themselves on either side of the sensor's detection envelope at the desired range, holding a rope or string attached to the aluminum ball, Figure 5-14
3. After waiting 30 seconds to allow the sensor to return to an undisturbed state, the test coordinator will initiate the test
4. Starting with the aluminum ball on the unsecure side (see Figure 5-13) of the detection envelope, the tester will drag the ball across the detection zone at the designated speed until the sensor declares an alarm or the ball moves all the way across the detection zone undetected; it is important that the test personnel are not in the detection zone, as the test should respond to the aluminum ball, not the people pulling the ball
5. Record the results, P or F on the test matrix, and move to the next location to repeat the test

Figure 5-14. Aluminum Target Used for Microwave Testing

5.8.4.3. Detection Envelope Tests

The procedures for estimating the dimensions to determine the detection envelop are similar to the previous steps, with two exceptions. Tests are conducted from both sides of the same three-meter marks along the length of the zone and the distances from the beam center line are recorded in the test matrix. The steps are:

1. Layout test grid
2. Position the test subject outside the detection zone of the microwave at the desired range, and remain motionless for at least 30 seconds
3. When the test coordinator tells the test subject to begin, they will advance across the detection zone per the test condition cited in the test matrix (walk, crawl, run, etc.) from the unsecure side to the secure side, as shown in Figure 5-13

4. The test subject continues to advance across the detection zone of the sensor until either a detection is declared by the sensor or the test subject advances all the way across the detection zone with no detection
5. When an alarm is generated, the subject will place one of the PVC markers on the ground at the detection point to indicate where the alarm occurred
6. The test is repeated at the same range, starting from the secure side and advancing to the unsecure side, and the location is marked where the alarm occurs
7. The distance from each detection point to the beam center line is measured and recorded in the test matrix, and the detection points are marked using colored pieces of PVC pipe (see Figure 5-15) or small, brightly colored stakes; this has the advantage of leaving an image of the sensor's detection envelope on the ground, and observing the pattern on the ground can sometimes indicate variations in the detection envelope, which can be correlated with cables, fences, posts, or other metal conductors that can influence the detection envelope
8. Results from each test are recorded in the test sheet and the test subject moves to the next location

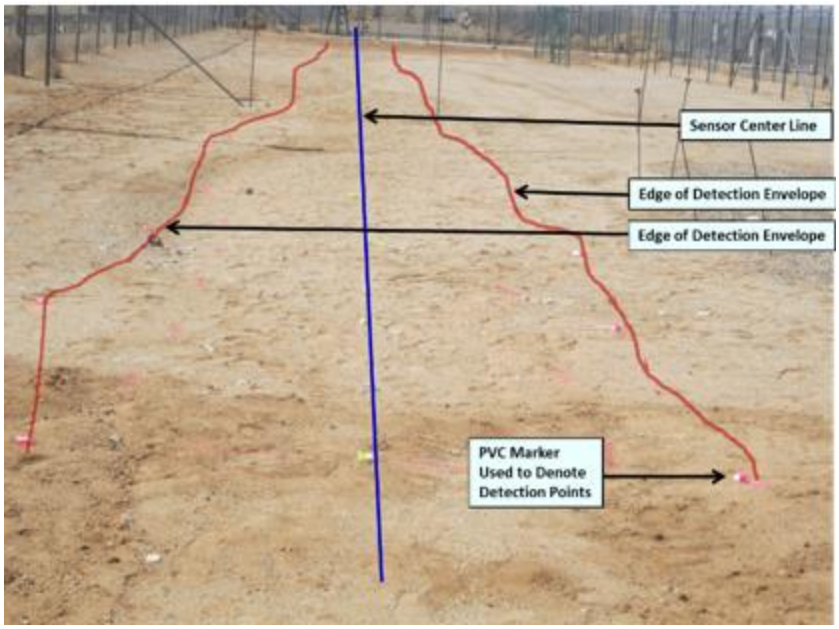


Figure 5-15. Detection Envelop Marked Using PVC Markers

5.8.5. Results and Analysis (Exterior Sensor)

5.8.5.1. Results from Detect/No Detect Tests

Results from the tests are shown in the Table 5-15 test matrix, with the results filled in. The results show the sensor will adequately detect the small runner, walker (0.3 m/sec), belly crawler (0.15 m/sec), and aluminum ball drag (0.3 m/sec). From the binomial tables, the P_S/C_L values are 92/95, which satisfies the requirement of 90/95 for this sensor. Looking at the results for the aluminum ball drag tests, the tests show that three meters beyond the required detection zone (-3 and 103 m), the sensor still detects the simulated intruder. This is expected if the lower microwave (24 GHz sensor) is mounted as shown in Figure 5-11. This gives the design engineer the needed information

to ensure reliable detection can be provided when the microwave heads are spaced the 116 meters apart that will be required to accommodate the 8 m standoff and basket weave layout in the deployment.

Although the test results from a belly crawler are not shown in this example, the slow-moving belly crawler and the aluminum ball drag yield very similar results.

Table 5-15. Detect/No Detect Matrix – All Threats

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103	Number Attempts	Number Detects	P_S/C_L
Small Stature																																									
Posture	Speed																																							
Runner	Approx. 4.9 m/sec **	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	34	34	92/95
Walker	0.3 m/sec	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	34	34	92/95
Belly Crawl	Est. 0.15 m ft/sec	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	34	34	92/95
Al Ball Drag	0.3 m/sec	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	34	34	92/95
***or as fast as safely possible*																																								

5.8.5.2. Results from Detection Envelope Tests

The results from the tests to estimate the detection envelopes provide more information regarding the lateral dimensions of the detection envelope, shown in the tabulated results in Table 5-16 and Table 5-17 and Figures Figure 5-16 and Figure 5-17. In comparing the detection envelopes for the walker and the aluminum ball, it is observed that the detection envelope for the walker is larger than the detection envelope of the aluminum ball. This is expected, because the walker's cross section is several times larger than that of the aluminum ball.

Table 5-16. Detection Envelop for Walker

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103
Small Stature																																					
Walker (Outer)	0.3 m/sec	0.8	1.0	1.5	1.2	1.6	1.3	1.5	1.6	2.0	1.8	1.9	2.0	1.9	2.0	1.9	2.5	2.3	2.5	2.6	2.9	2.5	2.4	2.5	2.6	2.2	2.4	2.6	2.1	2.3	1.9	1.5	1.4	1.1	1.1	1.1	0.8
Walker (Inner)	0.3 m/sec	-1	-1.1	-1.3	-1.6	-1.5	-1.3	-1.4	-1.7	-1.6	-1.7	-1.8	-1.9	-1.7	-2.1	-2.8	-2.3	-2.5	-2.6	-2.9	-2.6	-2.9	-2.5	-2.4	-2.5	-2.6	-2.5	-2.4	-2.6	-2.1	-2.0	-1.4	-1.5	-1.4	-1.3	-1.2	-1.0

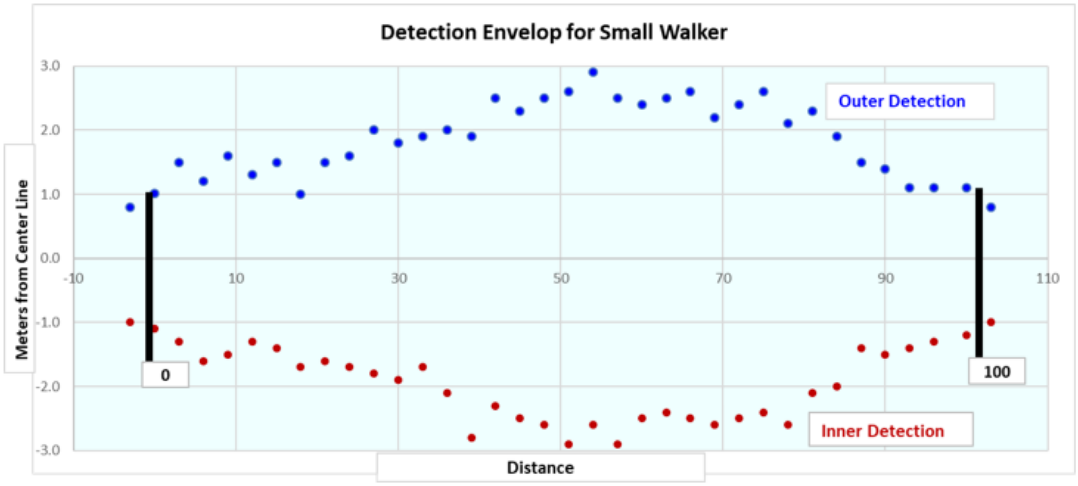


Figure 5-16. Microwave Detection Envelope for Small Walker

Table 5-17. Detection Envelop for Al Sphere

Distance		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103
Small Stature																																					
Al Ball Drag (outer)	0.3 m/sec	0.3	0.6	0.6	1.0	0.5	0.8	0.4	0.7	0.6	0.7	0.5	1.0	0.7	1.1	0.9	1.0	1.1	1.2	1.3	1.5	1.2	1.3	1.4	1.6	1.5	1.4	1.3	1.3	1.2	1.1	1.0	0.9	0.8	0.7	0.7	0.3
Al Ball Drag (inner)	0.3 m/sec	-0.4	-0.8	-0.8	-0.4	-0.7	-0.6	-0.5	-0.5	-0.6	-0.7	-0.8	-0.9	-1.0	-1.1	-1.2	-1.3	-1.5	-1.2	-1.3	-1.4	-1.6	-1.5	-1.2	-1.3	-1.4	-1.6	-1.5	-1.4	-1.3	-1.3	-1.2	-1.1	-1.0	-0.9	-0.9	-0.4

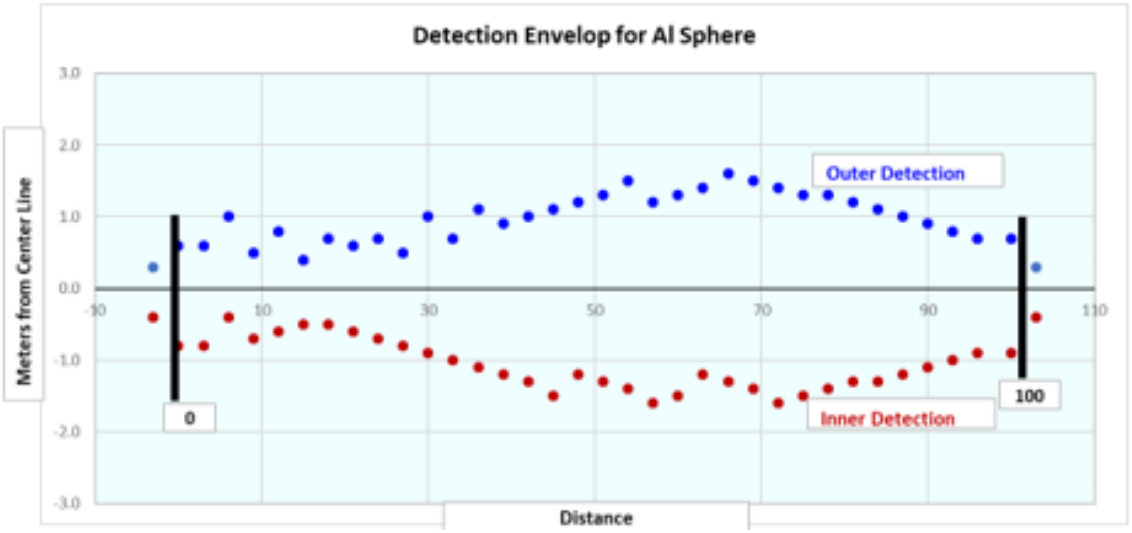


Figure 5-17. Microwave Detection Envelope for Aluminum Sphere

The plots shown in Figures Figure 5-16 and Figure 5-17 are fairly symmetrical around the sensor's center line, but this is not always the case. Asymmetry in the detection envelope could be caused by changes in the microwave field from nearby conductors such as fences, barriers, or other sensors like e-field or taut wire sensors. A quick study of the asymmetry of the detection envelope can provide more insight into how the sensor responds to its environment and possible nuisance alarm sources, providing an enhanced understanding of how to deploy the sensor in the field.

5.8.5.3. Results from NAR/FAR Collection

Several interesting observations can be made from the results of the NAR/FAR data collection (Table 5-18). In this example, a snowstorm occurred during the 30-day NAR collection period and the majority of the nuisance alarms from weather were recorded during the snowstorm, with 38 snow-related alarms out of a total of 40 weather-related nuisance alarms. Based on these results, the average NAR, including those from snow, is estimated at 1.6 per day. This would exceed the requirement of 1.0 per day. These results could make using this technology problematic if installed in a location with frequent snowstorms. If installation of the sensor is planned for an area that does not receive snow, the average NAR would be 0.3 per day and would meet the requirements in a snowless environment. The NAR data and analysis of the causes of nuisance alarms is valuable in determining if this system should be installed in a particular environment.

Table 5-18. NAR/FAR Data Collected Over a 30-Day Period

	False Alarms	Nuisance Alarms	NAR Weather	NAR Wildlife	Average FAR Alarms/Day	Average NAR Alarms/Day
Microwave	4	48	40	8	0.1	1.6
	Minus snow-related NAR/FAR from snowstorm					
	4	10	2	8	0.1	0.3
38 of the 48 nuisance alarms occurred during heavy snowfall experienced during snowstorm						
Per discussion w/vendor, treating the microwave dome w/Rain-X will prevent snow from building up on the dome and sliding across the surface						
6 wildlife alarms caused by coyotes; 2 caused by a badger						
1 nuisance alarm from wind that knocked an orange cone over and into the microwave's detection envelop						

Per discussions with the microwave vendor, application of a water repellent will reduce the amount of snow that builds up on the microwave dome and will prevent the majority of the snow-related (and some rain-related) nuisance alarms. This would have been important information for the vendor to provide prior to testing, but unfortunately this kind of situation occurs routinely when testing sensors. Ideally, the NAR collection would be repeated using the water repellant and another 30-day NAR collection would be conducted during the snow season. This would impact both test schedule and cost, and there is no guarantee snowy weather will occur during the next 30-day NAR collection period, which would not provide the desired information regarding the effectiveness of the water repellent reducing nuisance alarms from snow.

Looking at the NAR/FAR tabulated results, the false alarm rate (0.1) is under the typical requirement of one per day. When a high FAR is produced by a sensor, it typically means the technology is not mature. Issues that can cause high FAR include, water seeping into the sensor housing, electronics that are susceptible to cold or hot weather conditions, power spikes from unstable power or lightning, or voltage spikes on the sensor's electrical ground. A high FAR is also a good indicator of high maintenance costs if deployed, often requiring manual resets or replacement of electrical boards inside the sensor.

This page left blank

6. DESIGN PROCESS

6.1. Introduction

Although systems engineering has many forms, at a high-level, design of any complex system requires developing clear objectives of the system, designing a system to meet the objectives, and then analyzing the design to determine if it sufficiently meets those objectives. If the system does not meet the objectives, it can be redesigned in an iterative process until the objectives are met. In some cases, if a design does not meet the defined objectives, the objectives can be revisited to ensure they are accurate and realistic.

In security, the objective is to protect people, assets, facilities, and the environment from an individual or group attempting to cause harm. In contrast, the objective of safety is to protect facilities, assets, people, or the environment from natural disasters, equipment failures, or human errors. A systems engineering-based physical protection framework known as the Design and Evaluation Process Outline (DEPO) was developed by Sandia National Laboratories to guide the design and evaluation of physical protection systems, illustrated in **Error! Reference source not found.**.

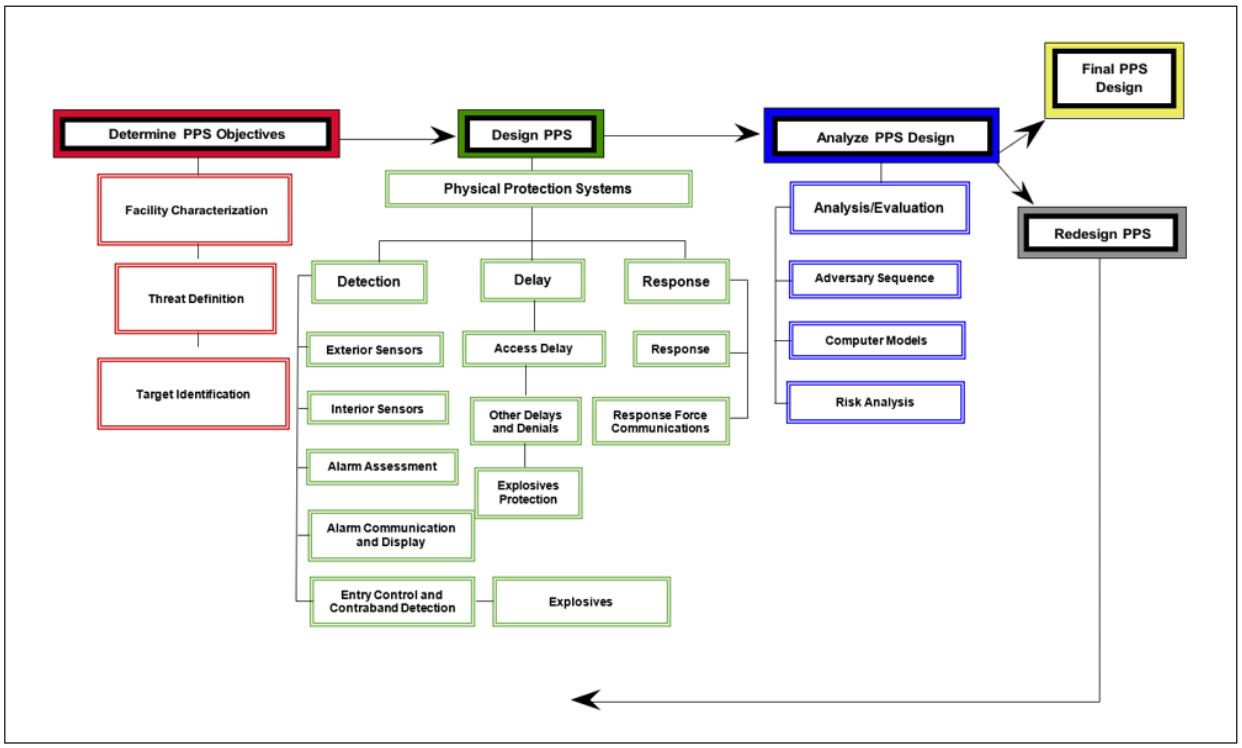


Figure 6-1. Design and Evaluation Process Outline (DEPO)

6.2. Design and Evaluation Process Outline

The security design process follows the DEPO methodology defined in the previous section (**Error! Reference source not found.**), which encompasses the first several elements of the lifecycle wheel. The steps in the design and evaluation process outline include:

- Define PPS requirements as outlined in activity one of the lifecycle; all relevant requirements applicable to the project should be identified, defined, and understood

    - The CA will review the PPS design to identify any requirements that are not being addressed
    - This is typically accomplished during design reviews, which are normally required by the CA
        - Multiple design reviews may occur at different stages of the design maturity, specifically for conceptual design and 30%, 60%, and 90% reviews; the number of reviews will be dictated by the scope and complexity of the project
        - At each review, the CA, design team, implementation team, and the T&E team will review the design to make sure it can both meet requirements and be built

- Begin the design of the PPS by identifying qualified PPS systems that may meet the requirements set up by the CA. This step will also include activities two through four of the lifecycle, described in Section 2.1.1
- Evaluate the PPS design to ensure all performance and other prescriptive requirements are satisfied
    - This evaluation considers the effectiveness of all PPS systems to protect the NM assets or facilities to a defined level of performance and is accomplished by analyzing the effectiveness of the entire PPS system, which includes intrusion detection, access control and contraband detection, delay features, and response
    - If the analysis of the system is shown to be acceptable, the design advances to the installation or implementation step, shown in the lifecycle wheel.
    - If deficiencies are found, a process to re-evaluate the requirements, possible PPS upgrades/modifications, and analysis will be repeated until all requirements are proven to be met
- There may be times when the design team requires additional test data before they can complete a design phase
    - In this case, the T&E team could conduct limited elements of the T&E effort, rather than completing the entire effort all over again
    - Retesting could be necessary as the result of faulty data, improper test procedures, excessively noisy data, missing data, etc.

Depending on the scope of the PPS upgrades and/or requirements, it may be advantageous to conduct a PITCO. This involves providing a test bed to verify software configurations, connectivity for power, communications protocols, data rates, and latency requirements can be met as designed and built.

- PITCO test beds are not traditionally used for a single security component as it can be time consuming and expensive; the PITCO can be useful for inter-system compatibility and can be the first PPS system check to verify inter-system interface requirements are correct and complete
- It is the responsibility of the T&E team to test and verify subsystems have the appropriate interface definitions and requirements and report back to the design team and the sponsor

- This activity is meant to identify inter-system compatibility issues prior to installation at the site
    - Compatibility issues can be caused by insufficient detail or mistakes in requirements or specifications
    - It is the responsibility of the design team to specify inter-system compatibility requirements during the design phase of a PPS, but iterations on interface requirements and component specifications may occur between the design phase and implementation
- Any information and data acquired through the PITCO process will provide the design team with additional information to incorporate into the design of the systems to be implemented

6.3. Design Guidelines

Certain guidelines should be observed during the PPS design. Design of the PPS begins with a review and thorough understanding of the protection objectives the system must meet. This review can be done simply by addressing the required features of a PPS, such as intrusion detection, entry control, access delay, response communications, and a protective force. However, a PPS design based on required features cannot be expected to lead to a high-performance system unless those features, when used together, are enough to ensure adequate levels of protection. Feature-based designs only check for the presence of a number or type of component, with no consideration for how effectively the component will perform during an adversary attack. A good PPS will be designed using components that have validated performance measures established for operation. Component performance measures are combined into system performance measures by the application of system modeling techniques. This process is the fundamental foundation for a performance-based design.

A PPS is generally better if reliable detection with low NAR/FAR is far from the target, and delays are near the target. In addition, there is close association between detection (exterior or interior) and assessment.

The designer should be aware that detection without assessment is not detection, since without assessment the operator does not know the cause of an alarm. If the alarm is the result of some trash blowing across an exterior area or lights being turned off in an interior area, there is no need for a response, since there is no valid intrusion (i.e., by an adversary).

Another close association is the relationship between response and response force communications. A response force cannot respond unless it receives a communication call for a response.

These and other features of PPS components help ensure designers take advantage of the strengths of each piece of equipment and use equipment in combinations that complement each other and protect any weaknesses.

Additional features of an effective PPS that should be considered when designing physical security systems include:

- **Continuous lines of detection –** Provides for detection of all viable pathways for an adversary to enter the space, if IDSs are required to detect unauthorized entry to a space. For example, when protecting a building or room, this would include ensuring all credible pathways into the room, i.e., doors, windows, vents, walls, ceilings, and floors would be

considered in the evaluation of credible pathways an adversary might take to gain entrance into the room and be included in the design for detection.

- **Defense in Depth –** Provides for multiple layers of detection, delay, or access control capability, reducing the probability of a single point of failure. It is better and more efficient to provide the first opportunity for detection as far away from the target as possible and delay features as close to the target as possible. Multiple opportunities to detect an adversary and delay their progress along all credible paths will help ensure response forces will be able to interrupt and neutralize the threat before adversaries accomplish their task.
- **Balanced Protection –** Provides relatively equal protection along all credible paths. This affects delay and detection features and ensures all credible pathways have the same, or nearly the same, effectiveness in detecting and delaying a threat.

7. IMPLEMENTATION

After the design of the security system has been completed and approved, sensor, camera, lights, etc., locations, orientations, settings, and necessary power and comms infrastructure are identified and documented in the design package[8]. The next step in the T&E lifecycle is to install and implement the design.

Testing associated with installation can be considered in three stages:

Stage 1: After initial sensor installation, alignment, and settings are completed, conduct a representative subset of the full test matrix (e.g., 5-10 tests), monitoring sensor output locally as shown in Figure 7-1

Stage 2: After the sensor is connected to the site monitoring system, conduct a representative subset of the full test matrix (e.g., 5-10 tests), monitoring and recording alarm outputs at the alarm monitoring station, Figure 7-2; at this stage initial nuisance alarm data should be collected and monitored by the alarm monitoring system

Stage 3: After all the sensors are installed and connected to the site's monitoring system, complete all the tests in the test matrix and observe nuisance alarm data, monitoring all sensors simultaneously, Figure 7-3; this test should be a "dry run" for the certification testing

7.1. Recommendations on Documentation and Payment for Installation

It is recommended the DT specify a checklist the installer or integrator should complete and present, showing test results for all three stages of installation acceptance and certification. To ensure the installation, testing, and documentation is completed, the DT or funding source should not make final payment for the installation until certification is completed when using commercial security contractors. This checklist will become a part of the final documentation for the installation of the sensors and will serve as supporting information in the certification phase of the sensor system.

Contractually speaking, payment to the installer can be structured to provide partial payment after the completion of each installation stage and the final certification phase. If the installation is the responsibility of an integrator, the integrator will specify the payment and performance schedule with the installer, and the integrator would be responsible for providing the required test documentation. It is recommended that the installation contract with the installer specify partial payment after each stage of the installation testing is completed, with final payment provided after certification testing is completed.

In the example provided in this section, a 25% payment could be made after reports are approved by the funding source for stage 1, stage 2, stage 3, and certification testing. It is also important to retain all documentation accepted by the funding source, as part of the construction documentation for the security system. The ability to review the stage 1 reports will be invaluable when trouble shooting the sensor system, and during stage 2, stage 3, and certification testing.

Further description of each stage is provided the following sections.

[8] Because this manual is focused on the T&E lifecycle of sensors, the following T&E stages during implementation specifically discuss sensors, but the authors recognize there are multiple security elements that will need to be tested during implementation.

7.1.1. Stage 1

Sensor installation cannot be completed until the necessary power and communications installations have been completed. Once the sensor is initially installed, it will be aligned, and sensor settings should be configured to cover the detection envelope specified in the design drawings. If the design documents do not specify the detection envelope, the installer should consult the DT to ensure the bounds of the detection envelope are understood. Completion of the checklist or installation test data form that is given to the installer should specify the sensor settings and data collection needed to show the sensor has been installed correctly. The data collected and documented should highlight any anomalies or conditions that could cause nuisance alarms and provide verification that tamper switches function properly.

Data collection to show the sensor is functioning correctly can be accomplished using the sensor interface provided by the vendor or basic tools like a voltmeter or an ohm meter, as shown in Figure 7-1.

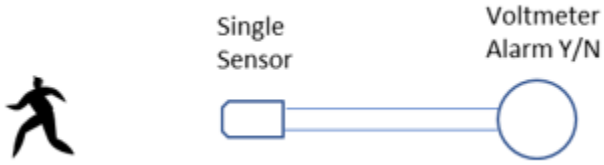


Figure 7-1. Notional Configuration for Stage 1 Testing

It is prudent to document any onsite directions or deviations provided to the installers by the designers or others.

During this stage of the installation testing, a limited set of performance tests selected from the test matrix used in the component T&E should be executed and results recorded. To accommodate actual site installation dimensions and conditions, the test matrix will need to be modified (i.e. changes in ranges, sector lengths, overlap, etc.). Using the example of the microwave sensor presented in Section 5.8, the following test matrix (Table 7-1) is offered as an example of the subset of tests to be conducted during Stage 1 of the installation. The recommended tests are identified using the letters "1LT," denoting a Stage 1 limited performance test. In the test matrix example provided in Table 7-1, the limited tests are conducted at the ends of the desired detection zone and in the middle. The aluminum ball drag is the most difficult simulated intrusion to detect. If the sensor detects the aluminum ball, it will likely detect the other intruders. The walk test is also cited as a limited test because it is easy and quick. If the sensor does not detect the walker, there is no need to test with the aluminum ball.

Table 7-1. Detect/No Detect Matrix – All Threats

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103
Statute: Large, Medium, or Small																																					
Runner	Approx. 4.9 m/sec*																																				
Walker	0.3 m/sec		1LT																1LT																	1LT	
Belly Crawl	est. 0.15 m/sec																																				
Al Ball Drag	0.3 m/sec		1LT																1LT																	1LT	
**or as fast as safely possible*																																					

During installation, there may be interference from other elements of the PPS design, such as delay barriers, fence lines, other sensors, or pedestrian portals that could degrade sensor performance. It is possible that the interfering objects are installed as designed and the sensors are installed as designed, but interference still exists. This issue should have been accounted for in the design phase, but mistakes or oversights do occur. These issues should be brought to the attention of the designers and corrected before proceeding.

Regarding nuisance alarm monitoring during this stage, it is not convenient to monitor nuisance alarms continuously using a volt/ohm meter or the vendor interface. It is possible to set up a recording device, monitoring the sensor outputs if desired, but not necessary at this time. During the execution of the limited performance tests, note if any alarms occurred that were not caused by the test subject. If such problems are identified, the sensor alignment and/or sensor settings should be adjusted to mitigate the cause of the nuisance alarm. If changes to alignment or sensor settings are made, the limited set of performance tests should be repeated. The DT should review the stage 1 testing documentation and sign off on it before proceeding to stage 2.

7.1.2. Stage 2

After successfully completing and documenting the stage 1 testing, the sensor can be connected to the site's monitoring system, as shown in Figure 7-2.

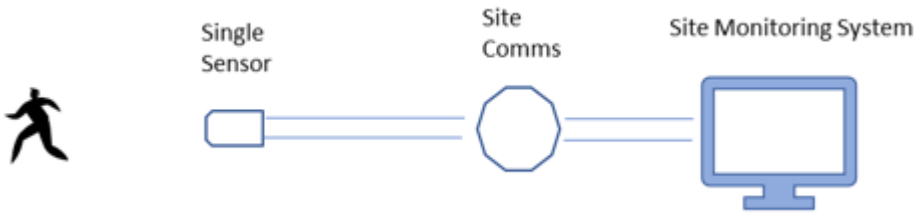


Figure 7-2. Notional Configuration for Stage 2 Testing

After connecting the sensor to the monitoring system, a few walk tests from the test matrix should be conducted to make sure the sensor is still functioning as it was during the stage 1 tests (the same walk tests conducted in stage 1 could be repeated, for example).

After completing the walk tests to verify the sensor is working like it was during the stage 1 testing, the next step is to determine if the sensor has any unacceptable nuisance alarm sources by using the site's alarm monitoring capability. Collecting valid nuisance alarm data during construction will require some coordination with the construction workers, equipment operators, and other personnel on site. Because of the difficulty in collecting valid nuisance alarm data, the test team will need to coordinate with the necessary parties to determine when NAR data can be collected and for how long. A reasonable NAR collection time for stage 2 is two-to-three days and nights. The DT should expect verification of the sensors' NAR performance, as required, before accepting the stage 2 installation testing. It is important that the installer not be allowed to approve their own installation. The installers will likely lack the objectivity needed to represent the DT's interests. If there are problems, the installer should be required to fix any issues. If changes to the sensor alignment or settings are modified, the changes should be documented in the stage 2 report/checklist, and the installer should repeat the limited set of performance tests conducted in stage 1.

7.1.3. Stage 3

After completing stage 2 testing, stage 3 testing can begin. Stage 3 testing is conducted while using the site's monitoring system to monitor all the sensors simultaneously. Verification of alarm conditions should be accomplished by monitoring the sensor outputs from the alarm monitoring system, as shown in Figure 7-3.

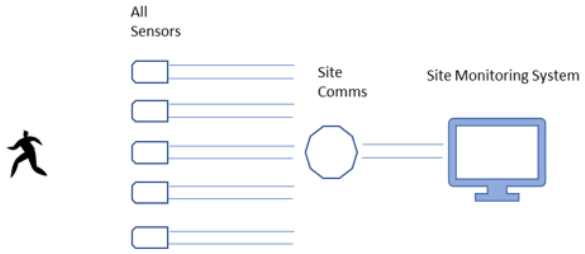


Figure 7-3. Notional Configuration for Stage 3 Testing

This stage of testing will identify interference from undesired sources including interference from adjacent sensors or faulty electrical grounding. If problems do occur, these issues should be brought to the construction management and design teams to determine the appropriate resolution. After the problem(s) are fixed, performance of the sensor should be verified by testing using the complete test matrix, shown in Table 7-2. Executing the complete test matrix does take more time and could be considered excessive, but it reduces risk going into the certification testing. Ideally, the stage 3 testing should be a dry run for the certification testing. If there is resistance to executing the complete test matrix, at a minimum the aluminum ball drag tests should be conducted.

Table 7-2. Detect/No Detect Matrix – All Threats

Distance (in meters)		-3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	100	103
Statute: Large, Medium, or Small																																					
Runner	Approx.. 4.9 m/sec*																																				
Walker	0.3 m/sec																																				
Belly Crawl	est. 0.15 m/sec																																				
Al Ball Drag	0.3 m/sec																																				
**or as fast as safely possible*																																					

Nuisance alarm collection should also be conducted for a limited period during stage 3. This will include monitoring nuisance alarms from the whole sensor system (i.e., all sensors that are running and all personnel and vehicle portals that are functioning). The NAR collection period will be specified by the DT. A continuous 10-day period is recommended for monitoring the sensor system. The 10-day period will enable observation of performance during shift changes and other site operational conditions. The third phase of the installation testing will be completed when the installer provides the DT documentation showing proper performance and the DT signs off on the stage 3 test report.

8. CERTIFICATION

Certification of the sensor system can begin after completing installation of all components of the security system, which will allow the sensor system to be certified in its deployed location and configuration. The three-stage testing strategy described in Section 7 is structured to identify any design oversights or installation issues associated with the sensors used to create the intrusion detection system. Ideally, if stage 1, 2, and 3 testing activities are designed and executed correctly, there will be no performance issues uncovered during the certification testing of the sensors.

Prior to conducting certification of the sensor system, the test team should provide the DT a copy of the certification test plan. Because the certification test plan should follow the test procedures used in the stage 3 implementation testing, it should be relatively easy to generate.

Certification testing of the ability of the sensor system to detect the simulated intruders will be a repeat of completing the test matrix shown in stage 3 testing. Results from the tests specified in the test matrix, showing the sensors can detect the simulated intruders specified in the requirements, will be documented in a certification package produced by the installer.

Tests that verify tamper switch function, which prevents an intruder from opening secure enclosures such as field panels or sensor housings, will also be conducted. These tests should be included in stage 1, 2, and 3 test reports.

It is the prerogative of the DT to specify additional tests, such as using a very small person (for example a 45-kilgram [100-pound] test subject) belly crawling across the detection envelope to further challenge the sensors' detection limit. Ideally, the DT will specify these additional tests in the requirements, allowing the installer to conduct stage 1, 2, and 3 tests prior to certification.

The DT may also request data be collected on each sensor to show the detection envelope of each. The decision to include detection envelope data increases the cost and schedule for conducting tests.

After confirming reliable detection of the intruders defined in the requirements, nuisance alarm monitoring for the whole sensor system can be conducted. The DT will specify the length of the NAR collection period. A typical duration is 30 days. During this period, no changes to sensor settings, sensitivity, or alignment will be made. After the NAR collection period is completed and the data is documented, the DT and delegated reviewers will review all documented data to determine whether the sensor system meets requirements.

It is likely that the certification test will identify issues with equipment, security procedures, or operations, and it will be up to the DT to ensure all issues have been resolved to an acceptable level.

Although this document is focused on the performance of the sensors, certification testing assesses how the sensor system functions and integrates into the complete security system, including how personnel responding to alarms perform, how well the monitoring system handles the incoming alarms and logs them, how well the procedures provided to personnel are written, and how well the alarm monitoring officers are trained.

A final documentation package for the certification is compiled, which includes the baseline sensor performance data necessary for certification. The baseline performance will be periodically checked in the subsequent sustainment and maintenance testing. The final documentation for certification testing should highlight that the sensor system met all requirements. If issues are identified during certification testing, they will be presented to the DT, who will determine if issues need to be resolved before approving the certification of the sensor system or if the risks are acceptable.

The elements of a certification test move beyond simply testing the sensor performance and can include:

- The sensor's ability to detect intrusions, P_S
- Nuisance alarm performance of the sensor
- Tamper switch performance
- Sensor self-test (most sensors do not have this capability)
- Line supervision
- Performance during and after power loss, including backup power
- Annunciation
    - At the CAS
    - At the SAS
- Assessment
    - Cameras
    - Video recorders
    - Encryption
    - Artificial lighting
- Network security and performance

9. SUSTAINMENT AND MAINTENANCE

The process of sustainability involves maintaining the required functionality and performance of PPSs after they are certified for operation. This includes all elements of detection, delay, and response. Systems are maintained through a program of scheduled testing and preventive maintenance of all PPS systems and procedures. There should also be a program for efficiently conducting corrective maintenance when required. Procedures for ongoing testing and evaluation are managed to identify and rectify any failures within the systems in a timely manner. Systems are also evaluated to ensure continued compliance, as prescribed requirements may evolve over time.

Maintenance includes all actions necessary for retaining an item or restoring it to a serviceable condition. An ongoing maintenance program prevents failures, minimizes loss from failures, and increases reliability of system operations through upkeep and repair. A comprehensive maintenance program will minimize system disruptions and maximize the useful life of equipment.

An effective sustainability program should incorporate the following six elements:

- Management organization
- Training, qualifications, and quality assurance
- Plans and procedures
- Maintenance management
- System evaluations/performance testing
- Configuration management

The following sections detail these elements further.

9.1. Management Organization

Management structures should satisfy the functions of planning, coordinating, implementing, testing, and evaluating the effectiveness of the sustainability program. Staff performance in the execution of maintaining a security system is influenced by the quality of management and the provision of expectations, requirements, sufficient budget, and standards for the conduct of work, training, documented procedures, etc. Therefore, a well-developed management organization is an essential feature of effective and sustainable nuclear security.

9.2. Training, Qualifications, and Quality Assurance

An effective maintenance program will include a qualification or certification process for maintenance personnel. Training personnel to certify they possess the requisite knowledge, skills, and abilities to conduct critical operations required by their job function is extremely important. Ensuring testing and maintenance personnel are trained and qualified to perform maintenance on site-specific systems includes professional training by qualified vendors and on-the-job training for site-specific configurations/systems.

A quality assurance policy and quality assurance program should be established and implemented, with a goal of providing confidence that specified requirements for all activities important to physical protection are satisfied (this will include their associated level of performance as well).

9.3. Plans and Procedures

Plans and procedures are key for the sustainment of the security system. The DT is responsible for verifying the implementation of prescribed requirements by a site's security management team. As

such, the security management team must develop plans and procedures to document and direct how they achieve the protection objectives.

Plans and procedures serve as the basis for day-to-day operations. Plans outline the overall structure of the security maintenance program for the protection of nuclear material, e.g. the physical protection plan and individual plans and procedures guiding the testing, evaluation, and maintenance of the PPS. These plans document how regulatory requirements are being satisfied. Procedures support the physical protection plans, provide a clear definition of the roles and responsibilities of facility personnel, and outline how tasks and operational activities are to be performed. When consistently applied, plans and procedures help achieve and maintain a desired level of performance.

These plans include test plans, which provide procedures to conduct the various types of performance tests/evaluations (see Section 9.5, Systems Evaluations/Performance Testing), maintenance work orders and reports, and operating procedures. A sample template for a test plan is provided in Appendix D.

9.4. Maintenance Management

There are two general approaches to maintenance activities: preventive and corrective. Corrective maintenance (CM) is conducted after a problem or failure occurs to a device or system. Preventive maintenance (PM) is planned and scheduled to stop a failure from occurring.

9.4.1. Preventative Maintenance

Preventive maintenance occurs according to a predetermined schedule and can also be planned if a higher component failure rate is occurring than expected. The maintenance can be scheduled during operational hours or during times when operations will be least affected. PM consists of activities such as adjustments, replacements, inspections, calibrations, lubrications, and/or repair of systems and components and is conducted regardless of the component's condition at the time. Scheduled inspections are performed to assess the condition of a component, which is a key aspect of PM to minimize downtime of essential equipment. PM also serves to extend the useful life of the equipment.

PM activities can be divided into two categories: invasive and non-invasive. Invasive maintenance involves the temporary removal or inactivation of equipment/components in order to conduct maintenance activities. During invasive activities, the equipment is unavailable. Non-invasive activities include measures such as inspections, monitoring, or testing. During this time, equipment/components remain operational and are still capable of performing intended functions (e.g., detection, delay, or response).

- **Advantages –** The ability to choose the time of the maintenance so it will have the least impact on operations, increased equipment/component life, decreased failures, increased reliability and efficiency, and overall cost savings
- **Disadvantages** – Servicing components/equipment can be time-consuming and may not be absolutely necessary to maintain operations; depending on the time intervals, PM can result in a significant increase in inspections and routine maintenance

While PM is not the optimal maintenance approach in some respects, it can be more effective than a purely reactive program. By performing PM as the equipment designer specifies, the life of the equipment can be extended. This translates into cost savings. PM will generally result in the equipment running more efficiently, which also means cost savings. While it will not prevent

catastrophic equipment failures, PM will decrease the number of failures. Minimizing failures results in maintenance and capital cost savings. By expending the necessary resources to conduct PM activities, equipment life is extended, and its reliability is increased. In addition to an increase in reliability, money is saved over time, especially in comparison to a reactive-based maintenance approach.

9.4.2. Corrective Maintenance

The purpose of corrective maintenance is to identify, isolate, and rectify a fault so the failed (or near failing) equipment or components can be restored to an operational condition within the tolerances or limits established for in-service operations.

- **Advantages** – The CM approach is acceptable for systems that utilize noncritical equipment; further, costs for CM are lower in the short term, and CM also requires less staff, since less routine work is being performed
- **Disadvantages** – Increased long-term costs due to unplanned equipment unavailability/downtime, possible secondary equipment damage, and possible neglect of equipment; these failures often occur at the most inopportune times, affecting operations and increasing costs to bring in technicians after hours; unexpected failures can also compromise the security and/or safety of the materials or facilities they are protecting

Sometimes a hybrid of the PM and CM approaches should be considered. This involves a process of critical component determination, which includes an effort to determine which systems are critical systems. A critical component has been evaluated and classified as critical due to its overall potential impact, should it fail. This includes impact to security, safety, operations, or the environment. Critical security systems are those that contribute significantly to the evaluation of system effectiveness.

9.5. System Evaluations/Performance Testing

The philosophy used to establish the number and types of tests to be conducted in T&E for maintenance is driven by the need to show the technology under test continues to provide the performance documented during the certification of the technology. The DT may require execution of the complete test matrix used during the certification testing (Table 7-2) or may accept a subset of the test matrix, such as the matrix followed during implementation testing (Table 7-1). Executing the complete test matrix takes more time, resources, and funding but has the advantage of verifying the technology still works like it did when certified. Executing a subset of the complete test matrix will save time and money but does not provide a complete set of test data showing the technology continues to meet performance requirements. The conservative approach is to conduct the complete test matrix. The decision regarding how many tests to execute, and how often, will be determined by the DT and will depend on how much risk is acceptable, balanced with the budget and manpower allocated to the maintenance organization.

The recommended strategy is to execute the full test matrix annually or semi-annually (see Section 9.5.2, Periodic Performance testing) and subsets of the complete test matrix more often. Functional testing, described in Section 9.5.1, represents a quick set of tests typically conducted on a daily or weekly basis. Periodic performance tests are typically conducted annually or semi-annually.

9.5.1. Functional Testing

Functional testing is conducted on a frequent basis to confirm the system is functioning. For example, on a weekly basis, a technician or guard while on patrol will walk into the detection envelop of a sensor to ensure it reports an alarm to the monitoring station. If the test is successful, verifying the system is functional, no further testing is warranted. It does not indicate how well the system is working, only that it is functional. This testing is important to verify no general failures in the system have occurred without the knowledge of the monitoring station. If the device/system fails this test, the appropriate personnel can be notified to investigate further to resolve the problem.

9.5.2. Periodic Performance Testing

Periodic performance testing is essentially the same as certification testing but is conducted on a scheduled, periodic basis (usually semi-annually or annually) to verify that the device/system is still performing at the level it did when certification testing was conducted. The intent of this testing is to verify that no degradation to performance has occurred over time. This level of testing should also be conducted whenever significant maintenance or modification to the system is done that may alter the performance. Examples of modifications/maintenance include if a power supply is replaced, or sensitivity settings are changed due to an unacceptable number of nuisance alarms.

9.5.3. Pass/Fail Criteria

For each test procedure, basic test results will be documented as either pass or fail. It is critical that the criteria that is used to determine whether the test resulted in a pass or fail be carefully defined. Some tests are straight forward, such as a person walking completely through the detection field of a microwave sensor without generating an alarm. This would definitely be considered a fail.

Other tests need additional clarification for the test team to determine a pass or fail. For example, what constitutes a pass/fail for climbing a fence with a fence disturbance sensor installed? Is it a fail if the sensor fails to detect the person after the first foot and hand is placed on the fence in an attempt to climb it? Or is the criteria set at "the sensor failed if the person can climb the fence and place one foot on the top without an alarm"? The second scenario is a more reasonable result, as it allows the sensor sensitivity to be set to a credible setting to detect a person climbing the fence and facilitate compliance with NAR/FAR requirements.

A fail does not necessarily preclude a passing result if corrective action is taken to address the failure (e.g., change the test conditions) and a re-test is performed. Again, if any substantial modifications are made to the installation or sensitivity/parameter settings, the testing must start again from the beginning to maintain the integrity of the results.

It is left to the discretion of the DT to determine when re-testing should occur and the conditions of the re-testing process. If the DT decides it is appropriate to perform a re-test of the failed test, the issue(s) and any corrective action(s) should be noted on the testing log sheet and documented in the test report.

9.6. Configuration Management

Configuration management is the process of identifying and documenting the characteristics of a facility's PPS—including computer systems and software—and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into facility documentation.

Configuration management establishes consistency among documentation that reflects design requirements, physical configuration, sensor alignments, sensor sensitivity settings, and operational activities. It includes analysis, drawings, and procedures for the facility. The goal of configuration management is to maintain a reliable understanding of known states of security elements throughout the life of the PPS, particularly as changes are being made.

An effective configuration management program also supports and benefits maintenance activities. It will provide necessary data to engineers and maintenance personnel when modifications or corrective actions are needed.

Configuration management activities can be accomplished manually through a paper-based system but typically require the use of computerized maintenance management systems (CMMS). These software-based systems aide in reporting (e.g., calculation of cost of machine breakdown) and scheduling (e.g., PM for each component). A CMMS is also useful for assessment and document control (e.g., management of latest document revisions, changes, etc.) and the management of a master equipment list of all deployed PPSs. This master equipment list assists in the prioritization of spare parts that the facility needs to support the maintenance and repair of critical PPS elements.

Effective configuration management includes five main elements

- **Design Control –** Document and maintain design requirements for structures, systems, and components to ensure they are, and remain, accurate and consistent with the as-built facility. Design requirements to be documented should include, at a minimum, those that affect operations, installation, function, performance, and maintenance.
- **Work Control –** Maintain documented processes and procedures for identifying and mitigating risks when planning, authorizing, and performing work. This ensures changes to the system are documented to confirm consistency is maintained between facility design requirements, documents, and physical configuration.
- **Change Controls –** Use to ensure changes are properly reviewed and coordinated across various organizations and personnel responsible for activities and programs at the facility. It is essential that changes are not made if they will negatively impact the facility mission. Change controls should also include firmware/software upgrades issued by vendors and implemented at the site.
- **Document Controls –** Ensure only the most recently approved versions of documents are used in the process of operating, maintaining, and modifying PPSs. Revisions to documents must be controlled, tracked, and completed in a timely manner. It is also important that revised documents get distributed to the appropriate users to ensure the latest version is applied, when necessary.
- **Assessment of the Maintenance Program –** Properly performed assessments identify inconsistencies, evaluate the root causes for problems, and prescribe improvements to avoid future inconsistencies in the maintenance program. The assessment process will be approved by the site security management and includes an ongoing analysis to determine if trends exist or are developing, indicating possible failure or compromise of a system, device, and/or procedure. Tracking these trends will influence the decision to retire a technology, discussed in the next section. Assessments also assist with increasing or decreasing the frequency of maintenance testing and show how effectively the relationships between design requirements, physical configuration, and facility configuration information are established and maintained.

This page left blank

10. RETIREMENT

Retirement is the last phase of the T&E lifecycle shown in Figure 1-1, but has strong ties to the first step in the lifecycle, assessment of requirements and regulations. Product retirement and disposal is an important part of system life management. At some point, any deployed system will become one or more of the following: un-economical to maintain, obsolete, or un-reparable. A comprehensive systems management process includes an anticipated equipment phase-out period and takes disposal and replacement into account in the design and lifecycle cost assessment.

Knowing when to repair, replace, or retire a PPS involves decisions that are easier to make when every detail with respect to each security element is known and documented. These details include date of manufacture, date of installation, software or firmware upgrades, expiration date (if any), maintenance schedules and costs, performance requirements, number of times it was repaired, and so on.

Another important aspect to consider when making decisions about system retirement options is performing an evaluation of current applicable requirements. An assessment of current requirements, regulations, laws, and types and quantities of assets being protected should be conducted to ensure any changes that have been made since the original deployment are considered when determining what PPS requirements are applicable. Perhaps changes in requirements and regulations or a change in the threat analysis since the initial deployment of the system have eliminated the need for the PPS and replacement may not be necessary.

The following sections will provide information on PPS lifecycle management, factors that affect the life expectancy of a PPS, and a discussion on the importance of conducting a comparative analysis of repair versus replacement costs when making decisions on a path forward.

10.1. Lifecycle Management

Equipment lifecycle management parallels the T&E lifecycle illustrated in Figure 1-1, and is the process to manage the end-to-end operational life of a device or system. This includes acquisition, through operational usage, and final failure, replacement, and/or retirement.

The graph shown in Figure 10-1 demonstrates the typical life of equipment in terms of failure rates of a component in the field. In the beginning of the operational life of a PPS or device, there will be several early failures because of manufacture defects, installation problems, and operational errors. During the lifetime of a security system, there will be a smaller number of occasional random failures. Then toward the end of life there will be an increasing number of age-related failures until reaching an unacceptable failure rate. Planning for, and managing, this lifecycle from beginning to the end of life is the objective of a maintenance program. The length of the effective operational time will vary depending on many factors, such as quality of components, operational environment, and comprehensiveness of the maintenance program throughout the lifetime of the system. Further, planning is necessary in order to ensure adequate funding is set aside each year to carry out necessary maintenance functions and activities.

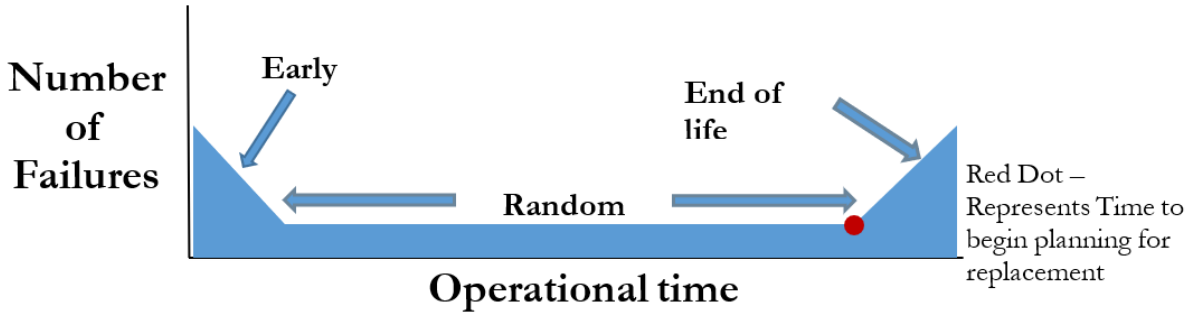


Figure 10-1. Life Expectancy of a Physical Protection System

10.2. Life Expectancy

System life expectancy depends on several factors. Most manufacturers will be able to provide an estimated timeframe for the effective life of service of a system during normal operations. Often those expectations are reflected in a warranty or in a published expected mean time between failure (MTBF) or mean time to failure (MTTF). The term MTBF is used for repairable systems, while MTTF denotes the expected time to failure for a non-repairable system. Failures are those conditions that place the system out of service and into a state for repair. As a technology ages and age-related failures occur, there will be instances when replacement parts are no longer produced by the manufacturer. This condition will prematurely reduce the life expectancy of a technology and force its retirement sooner than planned. Unfortunately, manufacturers may not communicate plans to discontinue parts or technologies to customers.

Other factors that can affect the reliability and length of MTBF or MTTF include:

- The operational environment in which the system is installed, including humidity, temperature, location (exterior, interior), radiation, etc., which will play a significant role in the expected life of the system
- A comprehensive sustainment and maintenance program should also extend the operational life of a system

Another factor that will influence the decision to retire a technology is the mean time to repair (MTTR). As a technology ages, the original manufacturer of the replacement parts may change and the time to acquire replacements or replacement parts may be unacceptable (ex., several months).

These factors are important to consider, as they will dictate the expected reliability of consistent performance. They can also be included in the calculation of the risk of failure, which can affect the probability of system effectiveness.

10.3. Repair Cost vs. Replacement Cost

Managing the lifecycle of assets involves keeping track of the lifetime costs of a PPS, which include costs for activities like the preventive and corrective maintenance required throughout the life of the system. Incurred costs include man-hours to support the maintenance and repair activities as well as materials/parts used. Tracking the costs for maintenance and repair over the lifetime of the system will provide important information including an understanding of the baseline costs of maintaining the system when first installed. Additionally, if carefully monitored, it will reveal any trends that develop for increasing frequency in needed repairs over time.

If the cost of repairs becomes higher than the cost of replacing an asset, then in most cases replacement is the best option. This is especially true when replacing the failing device/system with an identical or compatible system.

If replacing with a different model or manufacturer, or maybe even a different technology due to obsolescence or a manufacturer stopping support for a particular system, there are several things that need to be considered. The direct costs associated with replacing one system with a different system might include additional costs for engineering/design services, special training for technicians, additional or different infrastructure, spare parts, special tools (hardware or software) needed for testing and/or calibration, etc. In addition, the cost or impact on site operations must be included.

The process for determining the most efficient, cost-effective path to take when considering repair or replacement can be complicated and should be started many months, if not years, before the life of the system is expected to end. The red dot shown in Figure 10-1 indicates the time (at the latest) to begin the process of identifying a replacement technology. The sooner security management can begin the replacement process the better. Waiting too long will likely result in excessive maintenance costs, as discussed earlier in this section. If the technology experiences total failure and a replacement is not available, the site may be forced to provide a security guard to oversee the area previously protected by the failed technology. Another option is to deploy a temporary fix using technologies that were not originally designed into the system. Posting a guard and temporary deployments are referred to as compensatory measures and are typically expensive mitigation measures.

REFERENCES

[1] Garcia, M.L., *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann, 2007.

[2] Binomial Reliability Table (Lower Confidence Limits for the Binomial Distribution), by James Cook, et. al., NAVWEPS Report 8090, January 1964.

APPENDIX A. EXAMPLE OF KEY REQUIREMENTS INCORPORATED INTO THE MARKET SURVEY

The following are key requirements incorporated into a market survey for CUAS technologies. These are provided to give the reader an example of key requirements that would be developed during the "define the problem" step in the proposed process to conduct a market survey.

1. Must provide a system capable of detection and mitigation of UAS less than 24.9 kg (55 lbs.), speed up to 50 knots, at elevations from 0.3 to 1,036.3 m (1-3,500 feet) above ground level (AGL)

   This was a key requirement defined by the sponsor

2. Neutralization cannot be kinetic (guns) or laser methods

   This was a key requirement defined by the sponsor and US government (USG) regulatory restrictions

3. Must be capable of operating 24/7, 365 days per year

   This was a key requirement defined by the sponsor

4. Detection method must meet Federal Communications Commission (FCC), Federal Aviation Administration (FAA), National Telecommunications and Information Administration (NTIA), National Environmental Policy Act (NEPA), Underwriters Laboratories (UL), industrial hygiene (IH), and Environmental Safety & Health (ES&H) requirements for safe operation in the US

   This was a key requirement base on USG regulatory restrictions

5. Mean time to failure no less than 10,000 hours

   This was a key requirement defined by the site/user of the system

6. Mean time to repair is no less than three consecutive days

   This was a key requirement defined by the site/user of the system

7. CUAS is capable of being operated by one or less full-time operators

   This was a key requirement defined by the sponsor and the site/user of the system

8. Vendor must be willing to provide a technical briefing within one week of placement of contract

   This was a key requirement defined by the T&E team

9. Must be able to deliver a CUAS to a test site within two weeks of placement of contract

   This was a key requirement defined by the T&E team

10. The system must provide continuous sensing ability out to a range of 5.8 km (3.6 miles) or more for UASs

    This was a key requirement defined by the T&E team

11. Ability to provide assessment (classification)[9] ability out to a range of 3 miles or more for Group 1 and 2—in day and night

[9] Classification means the system can determine if the alarm stimulus is caused by a threat or a non-threat (bird, weather, etc.)

This was a key requirement defined by the T&E team

12. Must be a mature COTS product, not a in development; a low maturity product will require more funding to mature it to a reliable and fieldable state

    This was a key requirement defined by the T&E team

13. Vendor must be stable; there have been instances where the vendor that sold the best product went out of business shortly after purchase and completion of the test and evaluation

    This was a key requirement defined by the T&E team

APPENDIX B. EXAMPLE OF KEY REQUIREMENTS MATRIX TO BE SENT TO VENDORS IN RFI

Mandatory Requirements		Vendor Response	Vendor Comments
1	Must provide a system capable of detection and mitigation of UAS less than 24.9 kg., speed up to 250 knots, at elevations from 0.3 to 1,036.3 meters AGL	**Y/N**	
2	Mitigation cannot be kinetic or laser methods	**Y/N**	
3	Must be capable of operating 24/7, 365 days per year	**Y/N**	
4	Detection method must meet FCC, FAA, NTIA, NEPA, UL, and ES&H requirements for safe operation in the US	**Y/N**	
5	Mean time to failure no less than 10,000 hours	**Y/N**	
6	Mean time to repair is no less than 3 consecutive days	**Y/N**	
7	CUAS is capable of being operated by 1 or less full-time operators	**Y/N**	
8	Must be willing to provide a technical briefing within 1 week of placement of contract	**Y/N**	
9	Must be able to deliver a CUAS to a test site within 2 weeks of placement of contract	**Y/N**	
10	Must be willing to instruct the test team on how to record raw data, including signal to threshold, noise, and alarm data	**Y/N**	

Technical Performance		Vendor Response	Vendor Comments
1	**Ability to mitigate UAS threat by taking control of the UAS and flying the UAS to a set of predefined coordinates** –most UASs		

	Technical Performance	Vendor Response	Vendor Comments
	–some UASs –No, cannot do this—just uses energy on target		
2	**Can mitigate up to 4 UASs simultaneously** – 4 or more – 2-4 – No—don't know or cannot do more than one		
3	**Possesses a NAR/FAR of 2 per day or less averaged over a 30-day period** – 2 or less per day – 2-6 per day – don't know		
4	**Ability to provide continuous sensing ability out to a range of 5.8 km or more** **For Sense Range** – can detect UASs at greater than (GT) 5.8 km – can detect UASs out to 3.2 to 5.8 km – don't know or can detect UASs at less than (LT) 3.2 miles **For Size of Dead Spot** – dead zone from sensor head is less than 30.5 m – dead zone from sensor head is GT 30.5 m and LT 91.4 m – dead zone is GT 91.4 m		
5	**Ability to provide assessment (classification**) ability out to a range of 3 miles or more for UASs—in day and night** – can assess UASs at GT 3 miles – Mod—can assess UASs out to 2-3 miles – Low—don't know or can assess UASs out to LT 2 miles ***Classification means the system can determine if the alarm stimulus is caused by a threat or a non-threat (bird, weather, etc.)*		

	Technical Performance	Vendor Response	Vendor Comments
6	**Ability to provide continuous tracking ability out to a range of 5.8 km or more for UASs** – can track UASs at GT 5.8 km – can track UASs out to 3.2 to 5.8 – don't know or can track UASs out to LT 3.2 km		

	Non-Technical Criteria	Vendor Response	Vendor Comments
1	**Technical Maturity –** – Successfully deployed by a US agency, with references – Tested by a US agency, with test data available – COTS—does it exist—do they have logistical support?		
2	**Vendor maturity –** are they stable, how long have they been in business? – 10 years or more – 3 to 9 years – 1 to 3 years – LT 1 year		
3	**Example CUAS Acquisition Costs per System Spec –** – Less than $1M to protect a 1.6 by 1.6 square km site – $1-2M to protect a 1.6 by 1.6 square km site – GT $ 2M to protect a 1.6 by 1.6 square km site		

APPENDIX C. MATRIX SHOWING SCORING OF KEY REQUIREMENTS

Table C-1. Scoring of Mandatory Requirements

Number	Mandatory Requirements	Vendor A	Vendor B	Vendor C
1	CUAS is an integrated system, including detection, assessment, and neutralization	Y	Y	N
2	Neutralization depends on kinetic or laser neutralization	Y	Y	N
3	Capable of continuous 24/7 operation in all weather	Y	Y	Y
4	Meets FCC, FAA, IH, ES&H, NTIA, NEPA, and UL requirements	Y	Y	Y
5	MTTF of 10,000 hrs.	Y	Y	Y
6	MTTR of 3 days or less	Y	Y	N
7	System can be operated by 1 person	Y	Y	?
8	Vendor will provide training to set up and operate the system	Y	Y	Y
9	Vendor will provide access to raw data (e.g., signal, noise, etc.)	Y	Y	Y
10	Vendor will provide technical briefing within 1 week of placement of contract	Y	Y	Y
11	Vendor will deliver CUAS technology to the test site within 2 weeks of placement of contract	Y	Y	Y

	Legend
Y	Yes – meets criteria
N	No – does not meet criteria
?	Could not tell if vendor meets criteria—need more info

In this example, only vendors A and B meet the mandatory requirements. Based on this selection criteria, vendor C will not be considered for selection.

If no vendors meet the mandatory requirements, the team may want to make modifications as needed.

Table C-2. Scoring of Technical Performance Requirements

Number	Technical Performance	Vendor A	Vendor B	Vendor C
1	**Ability to mitigate UAS threat by taking control of the UAS and flying the UAS to a set of predefined coordinates** 10 – High—most UASs 5 – Mod—some UASs 1 – No—cannot do this—just uses energy on target	10	5	10
2	**Can mitigate up to 4 UASs simultaneously** 10 – High—4 or more 5 – Mod—2-4 1 – No—don't know or cannot do more than one	5	1	5
3	**Possesses a NAR/FAR of 2 per day or less averaged over a 30-day period** 10 – High—2 or less per day 5 – Mod—2-6 per day 1 – Low—don't know	5	1	10
4	**Ability to provide continuous sensing ability out to a range of 3.6 miles or more for UASs (2 scores)** **Score 1 – for detection range** 10 – High—can detect UASs at GT 5.8 km 5 – Mod—can detect UASs out to 3.2 to 5.8 1 – Low—don't know or can UASs out to LT 3.2 km **Score 2 – for size of dead spot** 10 – High—dead zone from sensor head is LT 30.5 m 5 – Mod—dead zone from sensor head is GT 30.5 m and LT 91.4 m 1 – Low—dead zone is GT 91.4 m	10 5	5 5	1 10
5	**Ability to provide assessment (classification**) ability out to a range of 3 miles or more for UASs—in day and night** 10 – High—can assess UASs GT 4.8 km 5 – Mod—can assess UASs out to 3.2 to 4.8 km 1 – Low—don't know or can assess UASs out to LT 3.2 km ***Classification means the system can show that the alarm stimulus is caused by a threat or a non-threat (bird, weather, etc.)*	1	10	5

Number	Technical Performance	Vendor A	Vendor B	Vendor C
6	**Ability to provide continuous tracking ability out to a range of 5.8 km or more for UASs** 10 – High—can track UASs at GT 5.8 km 5 – Mod—can track UASs out to 3.2 to 5.8 1 – Low—don't know or can track UASs out to LT 3.2 km	5	1	1

In this example, because vendor C did not meet the mandatory requirements, vendor A would be the top candidate based on the scoring criteria.

This page left blank

APPENDIX D. EXAMPLE TEST REPORT TEMPLATE

Provided below is a detailed example of a test plan and report template. The level of detail included in actual test plans and reports will vary based on specific testing needs, site requirements, etc.

ORGANIZATION TITLE REPORT

Document Control Number
Classification
Printed Month Year

Note to Author – blue text is used to describe the report writing process. Remove blue text before submitting any draft for review

Test Report Template

Type a short, concise, descriptive title to clearly convey the topic of the report

Enter author(s) name in the following format: John Q. Public (separate multiple authors with a comma)

Document Control Number
Classification
Printed Month Year

Title

Author(s)
Department Name, Org #

Abstract

<<highlight this line and start typing here>>

The abstract is typically required for all reports. It should be a brief informative paragraph (no more than 200 words) summarizing what is documented in the body of the report; the abstract should not include any proprietary information. The reader should be able to determine from the abstract if the information in the report is of interest to them; it should not be an introduction or a teaser to entice the reader to read further. Write the abstract after the main body of the report is complete.

Acknowledgments

<<Highlight this line and start typing here>>

This is an optional section. If included, in one or two paragraphs, acknowledge contributions from the following:

- *Sponsor and source of funding*
- *Vendor and any assistance provided by the vendor*
- *If a joint effort, all the entity departments and/or other government contractor organizations*
- *Any other individuals providing direct assistance with the work*

Contents

Placeholder for the table of contents; author or technical writer should auto-generate after report is written

Figures

Placeholder for a list of figures; author or technical writer should auto generate after report is written.

Tables

Placeholder for a list of tables; author or technical writer should auto generate after report is written

Executive Summary

<<Highlight this line and start typing here>>

The executive summary should be a high-level overview of the report. It should include:

- *Reason for the activities discussed in the report*
- *Activities performed*
- *Major conclusions and findings*

Remember:

- *Write the executive summary last*
- *Structure the executive summary as a simple, informative essay*
- *Do not include information not addressed in the report*

Acronyms

Only keep the acronyms that are actually in the report

24/7 ..... 24 hours a day, 7 days a week
CCTV ..... closed circuit television
CONOPS ..... concept of operations

DVR ..... digital video recorder
FAR ..... false alarm rate
I/O ..... input/output
MTBF ..... mean time between failure
MTBR ..... mean time between repair
NAR ..... nuisance alarm rate
P_A ..... probability of assessment
P_D ..... probability of detection
P_S ..... probability of sense
PIR ..... passive infrared

1. Introduction

Note: Sections 1 through 42 in this template represent the test plan. See Appendix A of this template for the steps that should be followed to gather necessary information and prepare a test plan for sensor evaluations.

1.1 Purpose

<<Highlight this line and start typing here>>

The purpose of the report should be 2 to 3 paragraphs and should include the following:

- *Why you are doing the evaluation*
- *The significance of the technology with respect to the customer*

1.2 Scope

<<Highlight this line and start typing here>>

The scope of the report should be 1 paragraph and should include the following:

- *Boundaries of the report*
- *What the report does and does not include*

1.3 Background

<<Highlight this line and start typing here>>

The background should be 2 to 3 paragraphs and should include:

- *Information about previous evaluations of the system/sensor (reference or cite if available)*
- *Details on the events leading up to the need for this evaluation*

1.4 Requirements

<<Highlight this line and start typing here>>

This section should be an introductory sentence and a bulleted list of references. The list should include:

- *Requirements that drive the tests*
- *References to major documents produced during project development*
- *Guidance used during test development*
- *Specific requirements from the site*

Use this section to specify test guidelines. The following boiler-plate text and common test references are provided as an example. Remove any references that are not appropriate.

SAMPLE:

The following documentation was used to determine and define test criteria used in this evaluation:

- IAEA Nuclear Security Series No. 13, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC225/Revision 5)

1.5 Selection Criteria (Optional Section)

<<Highlight this line and start typing here>>

If your project entails selecting components to be tested, include a discussion here about the selection process (criteria, methodology) and final selection. If the information is more than one page, provide the details in an appendix.

Information to be provided should include:

- *How was the initial group of components created (e.g., online search? SMEs? customer-directed?)*
- *What selection criteria were used to rank components in the group?*
- *What were the component rankings (include rationale behind weight rankings, if needed)?*
- *What was your final recommendation?*

2. Test Strategy

This section should be about 5 pages and should tell HOW you crafted the tests. Together with Section 1, this section represents the test plan. Detailed and specific test procedures are included as appendices.

2.1 Performance Metrics

<<Highlight this line and start typing here>>

- *Provide actual performance metrics*
- *If more than one type of test is being conducted (e.g., performance, nuisance alarms, degradation, defeat method, etc.), the description of criteria for each type of test is required.*

The following sample text is provided as an example

SAMPLE:

The following performance metrics are used to quantify performance of <name> technology.

- Probability of sensing (P_S)
- Probability of assessment (P_A)
- Probability of transmission (P_T)
- Nuisance alarm rate (NAR)
- Distance from the sensor that results in acceptable P_S values for a given threat (P_S range)

- Probability of detection (P_D)

The tests described in the following sections were designed to generate empirical values for the desired performance metrics.

2.2 Test Parameters

<<Highlight this line and start typing here>>

- *Identify the variables that can be controlled in these tests*
- *Identify the variables that cannot be controlled in these tests*

The following sample table is provided as an example

SAMPLE:

Table X. Sample Table of Variables (Controlled, Not Controlled)

Variable – Controlled	
Threat Vector	Test grid included walking paths across the detection zone every 3 meters Note: Only walks were tested and included in this example.
Sensor Settings	Threshold settings, gain, (and others)
Variable – Not Controlled	
Weather Conditions	Clear, rain, wind, hail (varied over time)
Terrain	Flat terrain located within a perimeter isolation zone

2.3 Test Matrix

<<Highlight this line and start typing here>>

- *Describe the tests conducted (based on the test criteria and variables)*
- *Link each test back to the specific test objective it fulfills; if you have objectives with no tests, or tests without objectives, rethink your test objectives and strategies*
- *Provide a test matrix that indicates the tests conducted*
- *Examples of test matrices are shown in the appendices*

2.4 Ideal Conditions, Degraded Conditions, Vulnerabilities, NAR

<<Highlight this line and start typing here>>

- *Describe ….*

3. Test Setup

- *Describe…*
- *This section should be about 3 pages long (if longer than 3 pages, place in an appendix)*

3.1 Test Equipment

<<Highlight this line and start typing here>>

- *Describe device (system/sensor components), including drawings and photos*
- *Use spec sheets information from the vendor or developer (if detailed, place in an appendix)*
- *Note: Check with technical writer (or relevant organization representative) to determine if copyright issues are involved and/or if permission is needed from the vendor to use their pictures*
- *Define any other equipment used in conjunction with the test*

3.2 Test Configuration

<<Highlight this line and start typing here>>

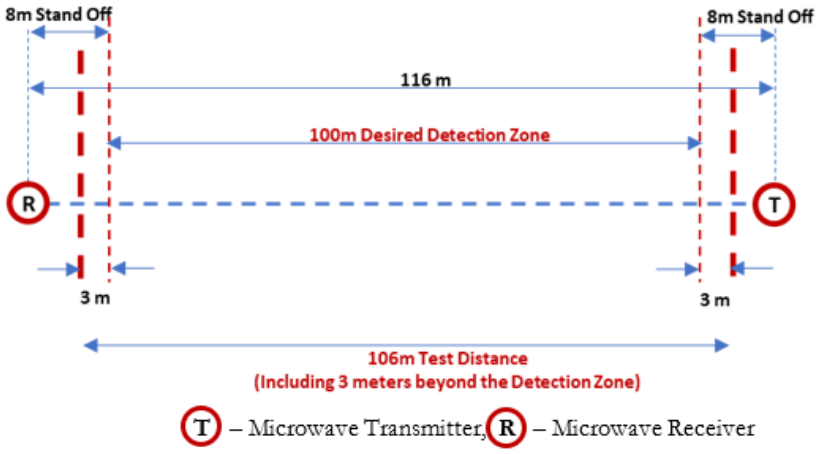
Provide diagram of test layout (grid, photos, settings, etc.)
Purpose is to ensure the reader has information about how to repeat test, if needed

This section should include:

- *Device installation requirements*
- *Test bed*
- *Calibration procedures*

The following sample test configuration diagram is provided as an example

SAMPLE:



4. Test Procedures

<<Highlight this line and start typing here>>

Reiterate which tests are to be performed, to set expectation for reader. If more than one type of test is being conducted (e.g., performance, nuisance alarms, degradation, defeat method, etc.), the description of methodology for each type of test is required.

The following sample text is provided as an example

SAMPLE:

Guided by the requirements cited in Section 1.6, testing was conducted in four phases:

1. Ideal Performance Tests
2. Degradation Tests
3. Defeat Tests
4. NAR Tests

The following sections describe the procedures for each of these tests in more detail.

4.1 Testing Under Ideal Conditions

<<Highlight this line and start typing here>>

This section should consist of a brief introductory paragraph along with a description of the test steps (could be bullets) that tell the reader how to conduct these tests.

If the steps are more than one page, consider placing detailed steps in an appendix.

4.2 Testing Under Degradation

<<Highlight this line and start typing here>>

This section should consist of a brief introductory paragraph along with a description of the test steps (could be bullets) that tell the reader how to conduct these tests.

If the steps are more than one page, consider placing detailed steps in an appendix.

Degradation tests should be reflected in the test matrix. The test matrix will not be classified.

Keep the main report unclassified.

4.3 Vulnerability Tests

<<Highlight this line and start typing here>>

Before writing this section, discuss the defeat tests planned with your supervisor. This section should consist of a brief introductory paragraph along with a high-level

description of the tests conducted (could be bullets). Provide enough detail to allow the reader to duplicate the tests.

Keep the main report unclassified.

4.4 Nuisance Alarm Rate Collection

<<Highlight this line and start typing here>>

- *Describe how you collected nuisance alarm data*
- *Describe how you assessed the cause of an alarm*
- *Describe any tests conducted to cause nuisance alarms*
- *Include the time duration (i.e., how long did you collect nuisance alarm information?)*
- *Describe the equipment used to trigger alarms*
- *Describe the environmental conditions during NAR testing*

5. Results and Analysis

Summarize data results and analysis; move all test results, data tables, and diagrams that may be of interest to some readers but are not crucial to the coherence of the report, to an appendix.

Include results from test types conducted; within test type, group test results per matrix categories, if needed (e.g., results for walk tests, crawl tests, etc.).

5.1 Results from Tests Under Ideal Conditions

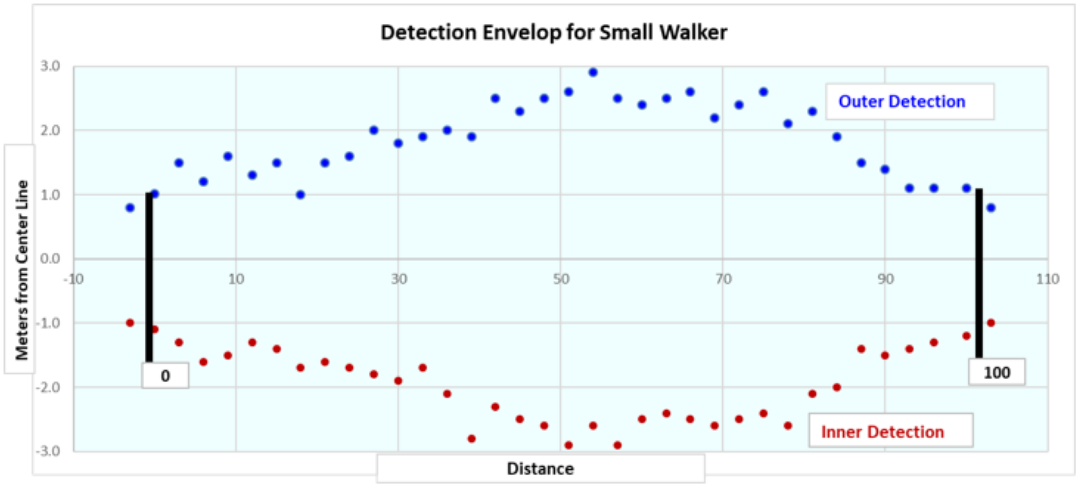
<<Highlight this line and start typing here>>

Summarize the data from the baseline performance tests

The following sample text, figure, and table are provided as an example

SAMPLE PERFORMANCE TEST RESULTS TEXT AND FIGURE:

This section will apply the concepts described in Sections 5.1 through 5.6 to a bistatic microwave exterior sensor. The sensor in this example is a “double stack” sensor, meaning two sensor heads are mounted on a solid base, see Figure 5-11. The lower sensor head will operate at 24 GHz and the upper sensor head will operate at 10 GHz. The following figure is a graph showing the detection envelop for a double stacked microwave motion detection sensor. The small “dots” in the graph represent the data points collected during the detection envelope test, in this case a walker moving across the sensor field at about 0.3 m/second. The red dots represent the location at which detection occurred for the test subject walking from the secure side and the blue dots for the subject walking from the un-secure side.



5.2 Results from Tests Under Degraded Conditions

<<Highlight this line and start typing here>>

Summarize the data from the degradation tests

Indicate changes in performance when subjected to wind, rain, snow

5.3 Nuisance Alarm Results

<<Highlight this line and start typing here>>

Summarize the data from the nuisance alarm tests

The following sample text and table are provided as an example

SAMPLE NUISANCE ALARM TEXT AND TABLE:

Nuisance alarm data was observed and documented while the system was operating during testing (Table X). In this example, a snowstorm occurred during the 30-day NAR collection period and the majority of the nuisance alarms from weather were recorded during the snowstorm, with 38 snow-related alarms out of a total of 40 weather-related nuisance alarms. Based on these results, the average NAR, including those from snow, is estimated at 1.6 per day. This exceeds the requirement of 1.0 per day..

SAMPLE NUISANCE ALARM RESULTS TABLE:

Table X. Nuisance Detection and Alarm Summary

	False Alarms	Nuisance Alarms	NAR Weather	NAR Wildlife	Average FAR Alarms/Day	Average NAR Alarms/Day
Microwave	4	48	40	8	0.1	1.6
	Minus snow-related NAR/FAR from snowstorm					
	4	10	2	8	0.1	0.3
38 of the 48 nuisance alarms occurred during heavy snowfall experienced during snowstorm						
Per discussion w/vendor, treating the microwave dome w/Rain-X will prevent snow from building up on the dome and sliding across the surface						
6 wildlife alarms caused by coyotes; 2 caused by a badger						
1 nuisance alarm from wind that knocked an orange cone over and into the microwave's detection envelop						

6. Conclusions and Recommendations

This section should be 1 or 2 pages. Ensure you have addressed ALL test objectives.

Organize information to address each objective as a separate subsection; for each objective, include:

- *What was learned or determined (observation)*
- *Logical, supported conclusions*
- *Logical, supported recommendations*
- *A high-level summary conclusion addressing the purpose statement*

6.1 Conclusions

<<Highlight this line and start typing here>>

The conclusion answers the question posed by the purpose statement by discussing and interpreting WHAT was learned or determined from completion of each objective.

Do not introduce new information not discussed in the report.
Conclusions are objective; avoid inserting opinions that are not clearly and logically supported.

The following sample text is provided as an example

SAMPLE:

Nuisance alarms were recorded for the sensor under ideal conditions for the first four weeks of the five-week period of monitoring; however, most of the nuisance alarms occurred when the sensor was exposed to a heavy snowstorm. In this example, a snowstorm occurred during the 30-day NAR collection period, and the majority of the nuisance alarms from weather were recorded during the snowstorm, with 38 snow-related alarms out of a total of 40 weather-related nuisance alarms. Based on these results, the average NAR, including those from snow, is estimated at 1.6 per day. This exceeds the requirement of 1.0 per day. These results could make using this technology problematic if installed in a location with frequent snowstorms. If installation of the sensor is planned for an area that does not receive snow, the average NAR would be 0.3 per day and, would therefore, meet the requirements in a snowless environment. Based on these data, the sensor did not perform in accordance with NAR requirements for exterior sensors operating under all environmental conditions.

6.2 Recommendations

<<Highlight this line and start typing here>>

Provide recommendations based on the test data.

The following sample text is provided as an example

SAMPLE:

Additional testing under non-ideal conditions is recommended to determine if sensitivity settings other than those recommended by the manufacturer can be used to reduce the NAR to within acceptable levels without degrading the sensing capabilities.

6.1 Closing Comments

<<Highlight this line and start typing here>>

After discussing conclusions for each objective, (1) answer the question posed by the statement of purpose, and (2) provide final recommendations. Expert opinion may be cited if arrived at through logical, objective reasoning based on concrete data.

The following sample text is provided as an example

SAMPLE

(e.g., if purpose was to determine if the Peter-Piper sensor meets requirements):

The unacceptable NAR discussed above indicates the sensor does not meet requirements for environments where snow is possible. However, it may be possible to reduce the NAR to an acceptable level by altering the sensitivity settings or making other modifications.

References

Include a reference to any document used while preparing for or conducting the test.

Recommended: List by author last name, in alphabetical order (samples below); if same author has more than one publication in a year, use a, b, c, (i.e., 2011a, 2011b, etc.); when referencing in text, reference by last name, year, e.g., (Dolittle, 2009; Cooke et al., 1964).

<<Highlight this line and start typing here>>

SAMPLE:

Cooke, James R., Mark T. Lee, and John P. Vanderbeck. 1964. *Binomial Reliability Table (Lower Confidence Limits for the Binomial Distribution)*. China Lake, CA: U.S. Naval Ordnance Test Station.

Dolittle, John. 2009. Personal communication by phone from John Dolittle, XYZ Corporation, to author, November 30, 2009.

Garcia, Mary Lynn. 2008. *The Design and Evaluation of Physical Protection Systems*, 2nd Edition. New York, NY: John Wiley & Sons.

ICx Technologies, "STS-1400," http://www.icxt.com/products/icx-surveillance/radar/sts-1400/ accessed September 24, 2009.

Riblett, Loren E., and James M. Wiseman. 2007. "TacNet: Mobile Ad Hoc Secure Communications Network," in *Proceedings, 2007 International Carnahan Conference on Security Technology*, IEEE, Piscataway, NJ, pp. 156-162.

Telephonics Electronic Systems Division, "ARSS: Advanced Radar Surveillance System," http://www.telephonics.com/products/arss.pdf, accessed September 23, 2009.

Glossary of Terms (for test plan/report template)

The definitions in the glossary below are for your use, as needed.

30/30 Tests	See 90/95 tests.
90/95 Tests	90 successes in 95 pass/fail trials is the minimum number of pass/fail repetitions for detection to meet requirements for external intrusion detection sensors of 90% detection at a 95% confidence level. This has been interpreted statistically to be equal to 30 successes out of 30 tests (30/30 tests), when conducting 100 tests is not feasible. The binomial distribution (pass/fail) probability is determined using the binomial reliability tables (Cooke, 1964). The resulting probability for 30 successes out of 30 trials yields 90% assurance of success at a 95% confidence level.
Binomial distribution	The discrete probability distribution of the number of successes in a sequence of *n* independent pass/fail tests, each of which yields success with probability *p.*
Characterization	A description of system behavior given specified performance metrics and factors. Characterization goes beyond pass/fail testing and allows the customer to understand the system in order to make a more informed decision concerning acceptability**.**
Controlled Variable	Controllable variables are independent variables that can be consistently changed during testing. These variables contrast with wind or outside temperature, which can vary but are not controllable.
Dependent Variable	Dependent variables answer the question "What do I observe?" It is often referred to as a response variable or performance metric in testing.
Experimental Design	A branch of statistics that outlines a method by which the data gathered in experiments will have statistical value; a set of experimental procedures specifying: the test units, sampling procedures, independent variables, dependent variables, and how external variables are to be controlled.
Independent Variable	Independent variables answer the question "What do I need to change in the test?" Values of the

	independent variable manipulated by the tester determine its relationship to an observed phenomenon (i.e., the dependent variable).
Nuisance Alarm	The alarm produced by an intrusion detection sensor not caused by an intruder (e.g., wind, lightning, thunder, accident, electrical malfunction, etc.).
Performance Metric	See dependent variable.
Principle	A basic generalization that is accepted as true and that can be used as a basis for reasoning or conduct.
Probability of Assessment (P_A)	The probability of an accurate assessment of the cause of an alarm.
Probability of Communication (P_C)	The measure of the probability that the alarm signal will be effectively transmitted to a monitoring/assessment location in order to initiate assessment and the proper response. Also referred to as Probability of Transmission (P_T).
Probability of Detection (P_D)	The P_D of a system is the product of the probability that the sensor will sense abnormal or unauthorized activities by an adversary (P_S), the probability that the alarm signal will be effectively transmitted to an assessment point (P_C), and the probability of accurate and timely assessment of the alarm (P_A). $P_D = P_S * P_C * P_A$ It is the likelihood of detecting an adversary within the zone covered by an intrusion detection sensor.
Probability of Sensing (P_S)	The probability that an intrusion detection sensor will sense an unauthorized action (Garcia, 2008); the measure of the ability of the sensor to perceive a disturbance of the sensor field, depending upon its phenomenology.
Uncontrolled Variable	Environmental factors over which there is generally little-to-no control (such as terrain undulation, vegetation, wind, humidity, temperature, presence of animals, and obstacles inherent to the site). Uncontrolled variables must be held as constant as possible or recorded as uncontrolled factor data for each test.

Performance Characteristics and Definitions of Sensor Tests

The following sections contain descriptions of performance metrics used to characterize performance of an intrusion detection sensor.

Probability of Sensing

Probability of sensing (P_S) is the probability that an intrusion detection sensor will detect an unauthorized intruder within the sensor's detection envelope (see below). Initial testing is performed to assess the sensor's ability to detect an intruder as a function of range. Sufficient data must be acquired in order to determine the P_S for a given sensor with a given statistical certainty. For high-security applications, the sensor and assessment system must achieve a minimum of a 90% probability of detection[10] with a 95% confidence level. Based on values extracted from Binomial Reliability Tables[11], a sensor must detect at least 30 out of 30 attempts in order to achieve this level of performance. Each series of tests (such as walk tests, slow walk tests, or crawl tests) must be conducted independently for statistical accuracy.

Detection Envelope

A detection envelope is the geometry or space that characterizes the extent of a sensor's ability to sense an intruder. Passive infrared sensors (PIRs) and microwave sensors, also referred to as volumetric sensors, have a three-dimensional detection envelope.

If the purpose of the sensor test is to validate a vendor's performance specifications, the advertised and the experimentally determined detection envelopes are compared.

Nuisance and False Alarm Rates

Nuisance alarm rates (NARs) are an integral part of a sensor's performance. Nuisance alarms are caused by a stimulus other than an actual adversary. Nuisance alarms can sometimes be attributed to sub-optimal settings of operating parameters. The number of nuisance alarms is often directly proportional to the detection sensitivity of a sensor and may represent a trade-off in capability. For example, adjusting the sensitivity of a sensor to a more sensitive setting can improve the capability of detecting an adversary; however, the sensor might then be more prone to produce an alarm on stimuli other than an adversary.

NAR is a performance metric that reflects how well a sensor can be expected to perform under various conditions. Nuisance alarm tests are designed to span all conditions to

[10] Probability of Detection = Probability of Sense (P_S) * Probability of Communication (P_C) * Probability of Assessment (P_A). For detection of an intruder to occur, three things must happen: the sensor must work properly (P_S), the intrusion must be communicated to the Central Alarm Station (P_C), and the response force must assess the alarm (P_A). If any of those conditions fail to be met (i.e., the guard ignores the alarm), detection does not occur.

[11] Cooke, James R., Mark T. Lee, and John P. Vanderbeck. 1964. Binomial Reliability Table (Lower Confidence Limits for the Binomial Distribution). China Lake, CA: U.S. Naval Ordnance Test Station.

which a sensor is expected to be subjected. During performance testing of interior sensors, automated systems monitor a sensor constantly (24/7) for nuisance alarms over an extended period, ideally one year. This extended period allows the sensor to be subjected to a range of environmental conditions. Even though interior sensors do not directly experience the weather conditions from the four seasons (as do exterior sensors), they do experience differences in heating, air conditioning, hot or cold windows, and warm or cold air currents resulting from personnel entry or exit. The NAR quantifies the sensor's response to stimuli other than an adversary.

A false alarm is one whose cause cannot be determined by the operator. False alarms are most often the result of equipment failure, which the operator will likely not be able to identify through normal means of assessment. These failures can be caused by failure of internal workings of the device/system or defects in the installation or infrastructure. For example, a BMS on a door could have come loose, generating false alarms with the simple vibration of the door. The false alarm rate (FAR) is a performance metric that should be kept at a minimum. Tolerance for false alarms is normally much less than for nuisance alarms and should be reported to maintenance staff to determine the cause and ensure the detection system is not compromised.

Degradation Factors

Degradation factors detract from the ideal performance of a sensor; for example, an interior volumetric sensor could have its performance degraded by furniture located within the detection envelope. P_S could be significantly reduced, possibly to zero, if an intruder could use strategically placed furniture to allow passage through the detection volume. Improper sensor alignment, improper sensitivity settings, and thermal variations are examples of degradation factors for volumetric sensors. When evaluating a dual technology sensor that employs a configuration that depends on two sensors working on conjunction, degradation to either technology degrades the entire sensor.

Vulnerability to Defeat

Theoretically, all sensors can be defeated. The security system designer uses a sensor's strengths to make the system difficult and costly to defeat. Different types of sensors and sensor models have different vulnerabilities. Identification of vulnerabilities can be accomplished by exploiting the sensor physics, signal processing, installation, degradation factors, or site conditions. Preliminary testing or past experience often indicate vulnerabilities or suggest additional testing to better characterize specific vulnerabilities.

Defeat methods can be described in terms of two categories:

- **Bypassing** defeats a sensor by avoiding the sensor's detection envelope
- **Spoofing** allows an intruder to pass through the sensor's normal detection zone without generating an alarm

"Low cost" or "quick look" vulnerability tests are those that are accomplished within a fairly short timeframe. If the quick look vulnerability assessment reveals potential

vulnerabilities that could preclude the sensor's use at a site, an in-depth vulnerability study is recommended.

Vulnerability tests are not always conducted as part of a system/sensor evaluation. For example, if results from ideal performance tests do not compare well with either the vendor's advertised performance specifications or facility/competent authority performance requirements, vulnerability tests may not be conducted.

Test Plan External Distribution

<<Highlight this line and start typing here>>

List names and addresses of individuals outside your organization who will receive a copy of this test plan

Test Plan Internal Distribution

<<Highlight this line and start typing here>>

List the names and addresses of individuals inside your organization who will receive a copy of this test plan

END OF TEST PLAN TEMPLATE

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Technical Library	01977	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.