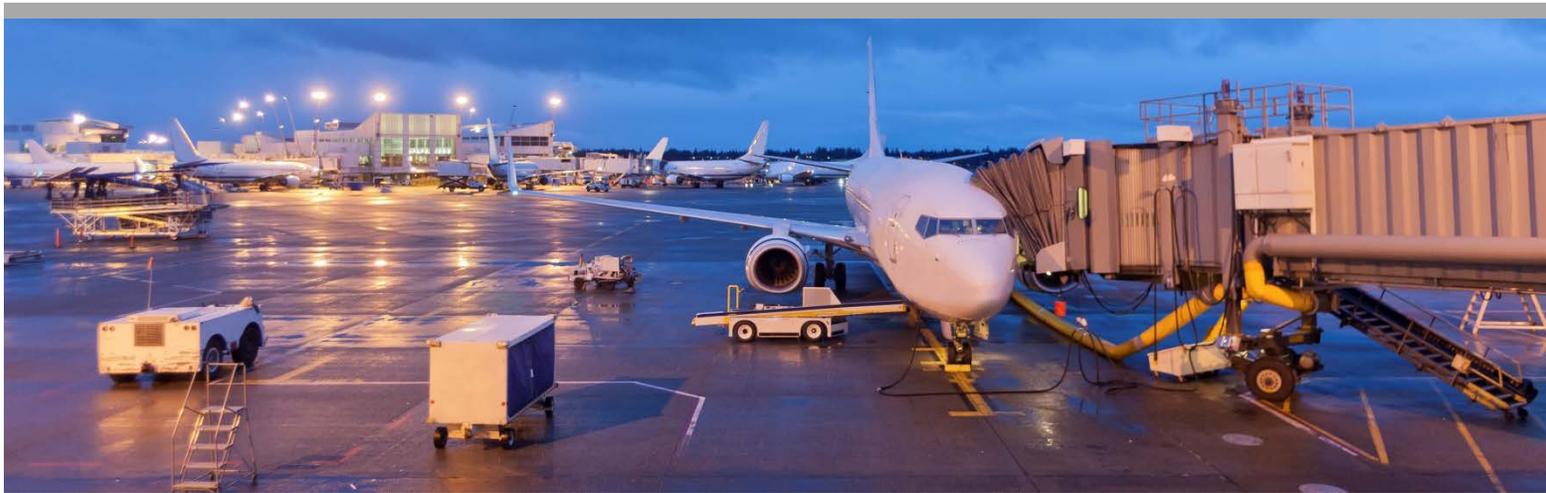




PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY



PARAS 0015

December 2018

Guidance for Airport Perimeter Security

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Ann S. Barry
Ross & Baruzzini
New York, NY

© 2018 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

National Safe Skies Alliance, Inc. (Safe Skies) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply Safe Skies or FAA endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from Safe Skies.

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about airport security technologies and procedures.

Through the Airport Security Systems Integrated Support Testing (ASSIST) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying perimeter and access control security technologies and procedures.

Through the Performance and Operational System Testing (POST) Program, Safe Skies assesses the continued operational effectiveness of airport-owned security technologies.

Through the Program for Appplied Research in Airport Security (PARAS), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies Special Programs Manager*

PARAS 0015 PROJECT PANEL

Jordan Bauer *Boise Airport*
Martina Benedikovicova *Charlotte Douglas International Airport*
Brian Hollis *National Safe Skies Alliance*
Daniel Flynn *Security Radar Integrators, Inc.*
Dawn Lucini *Telos Identity Management Solutions*
Larry “Chip” Monts *Jacksonville Aviation Authority*
Michael Pilgrim *International Security Concepts*
Lisa Rousseau *Port of Seattle*

AUTHOR ACKNOWLEDGMENTS

Ross & Baruzzini would like to acknowledge the following for their contributions in the development of this guidebook:

- National Safe Skies Alliance’s PARAS, which provided funding. Particular thanks are given to the program officer, Jessica Grizzle.
- The PARAS 0015 Project Panel members, who also provided significant review and contributions.
- The airports who provided invaluable input during technology pilots, project implementations, and input through surveys for this report:
 - Baltimore Washington International Airport
 - Dallas/Fort Worth International Airport
 - Los Angeles World Airports
 - Miami International Airport
 - The Port Authority of New York and New Jersey
 - San Francisco International Airport
 - Southwest Florida International Airport (Lee County Port Authority)
- Lastly, this research would not have been possible without the help of Ross & Baruzzini’s network of aviation security experts, design engineers, project managers, and technical writers who provided support throughout the process. In particular, appreciation is given to:
 - Theresa Smith, Project Manager
 - Michael Steinle, Subject Matter Expert – Emergency Operations
 - Mark Crosby, Reviewer and Subject Matter Expert – Airport Operations

CONTENTS

EXECUTIVE SUMMARY	ix
PARAS ACRONYMS & ABBREVIATIONS	x
SECTION 1. INTRODUCTION	11
1.1 Guiding Principles	11
1.1.1 Purpose	11
1.1.2 Scope	11
1.1.3 Applicability	11
1.1.4 Use	11
1.2 Research Methodology	12
1.2.1 Literature Review	12
1.2.2 Systems Engineering Methodology Research	12
1.2.3 Technology Solutions and Applicability Reviews	12
1.2.4 Physical Security Solutions Reviews	13
1.2.5 Operations Procedures Research	13
1.2.6 Stakeholder Engagement	13
SECTION 2. AIRPORT PERIMETER SECURITY PRINCIPLES, CONCEPTS, AND MEASURES	15
2.1 Core Principles	15
2.1.1 Layered Protection	15
2.1.2 Perimeter Protection Components	18
2.2 Perimeter Security Systems – Physical Measures	18
2.2.1 Fencing	19
2.2.2 Walls	22
2.2.3 Gates	23
2.2.4 Security Barriers for Maritime Perimeters	24
2.2.5 Vehicle Intrusion Barriers	25
2.2.6 Crime Prevention through Environmental Design (CPTED)	31
2.3 Perimeter Security Systems – Electronic Measures	33
2.3.1 PIDS Concept	33
2.3.2 PIDS Technologies	35
2.4 Perimeter Security Systems – Operations and Processes	50
2.4.1 Perimeter Patrols	50
2.4.2 Monitoring Perimeter Security Systems	51
2.4.3 Security Processes and Initiatives	53
SECTION 3. IMPLEMENTING PERIMETER INTRUSION DETECTION SYSTEMS	56
3.1 PIDS Project Management	56
3.1.1 Organization of a Project Team	56
3.2 Developing a Business Case for PIDS	58

3.2.1	Conduct a Needs Assessment	59
3.3	PIDS Implementation	62
3.3.1	Best Practices	62
3.3.2	Applying Systems Engineering Methodology	63
3.3.3	Developing a Concept of Operations	64
3.3.4	Develop a System Requirements Document	64
3.3.5	Design and Implementation	65
3.3.6	PIDS Components	65
3.3.7	PIDS Performance Metrics	67
3.3.8	Testing and Commissioning of Systems	68
3.3.9	Staffing Requirements Analysis	69
3.4	PIDS Lessons Learned	70
SECTION 4. CONCLUSION		72
REFERENCES		73
ACRONYMS		75
APPENDIX A: SUPPLEMENTAL CAMERA TECHNICAL INFORMATION		A-1
APPENDIX B: SYSTEMS ENGINEERING METHODOLOGY AND SUPPLEMENTAL INFORMATION		B-1

LIST OF TABLES & FIGURES

Table 1.	Fencing System Roles in Airport Perimeter Security	20
Table 2.	Simple Example of an Options Matrix	61
Table A-1.	Lux Condition Equivalents	A-11
Table B-1.	Basic Elements of a ConOps for Security Initiatives	B-2
Figure 1.	Example of a Best Practice Fence	21
Figure 2.	Anti-Climb Fence	21
Figure 3.	Anti-Climb Fence with Top Barbs	22
Figure 4.	Perimeter Wall with Barbed Wire	23
Figure 5.	Perimeter Pedestrian Gate	23
Figure 6.	Maritime Perimeter Barrier System	24
Figure 7.	Perimeter Keep-Out Zone Buoy Marker	25
Figure 8.	Example of Permanent Bollards	26
Figure 9.	Example of a Single Retractable Bollard System	27
Figure 10.	Typical Delta Wedge Barrier System	28
Figure 11.	Airport Perimeter Gate with Active Vehicle Barrier System	28
Figure 12.	Active Vehicle Barrier Net in Operation	29
Figure 13.	PIDS Concept	34
Figure 14.	Example of Fiber-Based Fence Detection Technology Installation	36

Figure 15. Typical Fence Disturbance System Installations	37
Figure 16. Typical Electric Field Sensor System Installations	38
Figure 17. Typical Microwave System Installations	39
Figure 18. Typical Buried Cable Detection System Installation	40
Figure 19. Typical PIDS Radar System Display	42
Figure 20. Example of a WDR Camera Installation	43
Figure 21. Thermal Camera	44
Figure 22. Thermal Imagery	44
Figure 23. Video Analytics Detecting Persons and Objects	45
Figure 24. Basic PIDS Components	66
Figure A-1. Visual Quality Comparison	A-2
Figure A-2. VSS Performance Guidelines – % of Height of Image	A-3
Figure A-3. VSS Performance Guidelines – H-FOV Width	A-3
Figure A-4. HD 1080p Resolution Comparison	A-4
Figure A-5. Comparison of 4K to HD Video Resolution	A-5
Figure A-6. Cropped Image Views from Single 4K/UHD Image	A-5
Figure A-7. 4K/UHD Camera	A-6
Figure A-8. H-FOV Width for 720p, 1080p, and 4K/UHD	A-6
Figure A-9. OBS FOV Comparison between 1080p and 4K	A-7
Figure A-10. Multi-sensor Camera	A-7
Figure A-11. Example 180-Degree View	A-8
Figure A-12. CMOS Sensor	A-9
Figure A-13. Lowlight Examples	A-10
Figure A-14. Non-WDR versus WDR View	A-12
Figure A-15. Multi-Image Stacking WDR	A-13
Figure A-16. Motion JPEG, MPEG-4, and H.264 Bit Rate Comparison	A-15
Figure A-17. H.264 versus H.265 Storage Comparison (in MB)	A-16
Figure B-1. Methodology for Systems Engineering	B-1

EXECUTIVE SUMMARY

This guide provides aviation professionals with principles, measures, and implementation considerations to address perimeter security at airports. The intention is to offer information that is applicable to airports of various types and sizes in addressing perimeter vulnerabilities and identifying mitigation strategies.

The guide begins by providing an explanation of the need for perimeter security, followed by the introduction to core principles such as layered security and protection components. Perimeter security measures are divided into physical, electronic, and operational categories. Each category is explained and examples of solutions are provided with brief discussions on their advantages, disadvantages, and applicability to certain environments. In addition, the guide discusses the importance of, and provides guidance on, stakeholder engagement in addressing perimeter security.

Guidance is provided on perimeter intrusion detection systems (PIDS) and their effectiveness through the combined involvement of people, processes, and technology. While it is of paramount importance to provide appropriate physical and electronic security measures, it is also equally important to ensure that operations and procedures are in place to augment and support the use of PIDS.

The document offers advice on perimeter security projects and methodologies for needs assessments, business cases, and project management. Finally, the guide provides implementation considerations, best practices, and lessons learned.

Two appendices provide more detailed information on airport perimeter security technologies, processes, and engineering methods.

PARAS ACRONYMS & ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue and Fire Fighting
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

SECTION 1. INTRODUCTION

Though each airport is unique, all airports occupy large parcels of land. Airport operators must ensure that their perimeters are defined and—where necessary based on risk—safeguarded against accidents or perimeter breaches that may have deleterious effects on the airport, its passengers and employees, and aircraft. At commercial service airports, the federal government has established both safety (33 CFR § 139) and security (49 CFR § 1542) requirements. Safety and security also are concerns at general aviation (GA) airports, but on a different scale. The most common way airports protect the perimeter of their airfield is by installing and maintaining a perimeter fence. However, even though a standard airport chain-link fence with barbed wire may slow down a vehicle or a person, it does not notify authorities or completely stop an intrusion. During the last few years, there have been several incidents of vehicles and people entering an airfield and approaching passenger aircraft before first responders could stop them. While these incidents have not been motivated by terrorism, they reveal a potential vulnerability in existing airport perimeter systems and reaffirm the importance of airport perimeter security.

1.1 Guiding Principles

1.1.1 Purpose

The purpose of this document is to guide aviation professionals responsible for perimeter security at airports. While the primary focus of this guidance is on technical aspects of perimeter security and systems, such as perimeter intrusion detection systems (PIDS), the document also addresses important physical security methods as well as procedural and operational security measures to facilitate effective perimeter security.

1.1.2 Scope

This document provides guidance specific to perimeter protection and intrusion-detection technology systems for commercial airports whose security is regulated under 49 CFR § 1542. Although the document is focused on identifying the best practices for this particular layer of protection and facility type, many of the recommendations provided are broadly applicable to GA airports and their operators as well.

1.1.3 Applicability

Recommendations and findings within this guidance are neither mandatory nor applicable to all airport facilities. Organizations responsible for the development, design, refurbishment, integration, and operation of security programs at airports should complete a threat, vulnerability, and risk assessment to identify applicable threats and potential risk-mitigation strategies.

1.1.4 Use

Users of this guidance should be aware that a PIDS is only one component of an effectively layered approach to physical security that should be implemented to ensure the security of an airport. While the concept of integrating technology, physical infrastructure, and operational procedures is described herein, discussion of these security program components is limited to perimeter security.

1.2 Research Methodology

The research methodology used to develop this guidance includes implementation of six independent but interconnected tasks, including:

1. Review of available literature
2. Research into the application of systems engineering methodology to PIDS
3. Technology solutions applicability and review
4. Physical security solutions review
5. Operations procedures research
6. Stakeholder engagement

Additional details regarding each of these tasks are provided below.

1.2.1 Literature Review

The research team identified a significant number of applicable publications, periodicals, reports, standards, guidelines, and manufacturer-provided information to enhance the depth of understanding of perimeter security and PIDS. Prior to inclusion of literature references in this guidance, the research team evaluated each of the identified references to ensure currency and applicability. The evaluation process is critical to ensure that the guidance is valid and usable, both now and in the future.

1.2.2 Systems Engineering Methodology Research

Based on extensive research, planning, specifying, designing, implementing, and testing of various airport perimeter security systems, the research team understands that it is absolutely essential for successful system implementation (electronic or procedural only) to include the basic processes of systems engineering methodology. These processes—such as performing a needs assessment, developing a concept of operations (ConOps), and clearly and concisely defining system requirements—should be implemented prior to considering and choosing technologies to address perimeter protection. If conducted properly, the systems engineering processes will result in the appropriate perimeter technology, operational solutions, and perimeter security measures to meet the unique needs of each airport.

1.2.3 Technology Solutions and Applicability Reviews

Comprehensive PIDS guidance is based on the premise that defense should be layered and detection should be completed through a system of systems. Accordingly, the analysis herein identifies complementary technologies that can be utilized in a layered approach to security. This guidance is not intended to provide individual technology recommendations, but rather to consider the best use of specific technologies in various environments and deployment conditions. Experience indicates that application of these technologies too often is based on ideal conditions for sensor deployment, which are very rarely achieved in a field environment. Evaluation of system effectiveness and continuous improvement is addressed in Section 1.2.5, Operations Procedures Research. It is important to note that, in addition to research, analysis is supported by the applied knowledge of the principal investigator and subject matter experts (SMEs) with substantial experience in PIDS design and implementation.

1.2.4 Physical Security Solutions Reviews

Physical security solutions for perimeter protection are present at all airports. They can be as simple as standard fencing or combined with technology in a more complex implementation. This guidance will examine various physical security solutions, including the strengths and limitations of each.

1.2.5 Operations Procedures Research

Depending on the unique needs of an airport, perimeter security can be achieved in many ways: through the use of physical barriers, by installing technology, by implementing operational procedures, or in any combination thereof. The guidance on security operations is examined and discussed with respect to standalone operations and supportive operations.

1.2.6 Stakeholder Engagement

Stakeholder engagement efforts consisted of surveying a small group of aviation security leaders at medium and large sites. These stakeholders include senior-level security directors and managers.

Several approaches were employed to acquire relevant input across a diverse authorship group. The survey was developed with the input of internal team members encompassing aviation security SMEs executing security threat and vulnerability assessments; security engineering designers; physical security professionals; and public safety and retired law enforcement personnel. This internal team represents a cross section of dominant aviation sector experts, as well as members who are experienced across multiple critical infrastructure sectors, including commercial facilities, communications, emergency services, energy, government, healthcare and public health, and transportation systems. Each of the multiple representatives who provided input contributed to the process of developing the final survey content, which is based on the following framework:

- Introduction
- Instructions
- Facility Classification and Description
- Planning
- Project Management
- Estimation, Procurement, and Commissioning
- Operational Satisfaction
- Future Perimeter Intrusion Detection System Requirements

Content included a combination of structured, partially structured, and rating questions to elicit relevant feedback. A push communication method for the defined stakeholder focus group included an initial request to participate distributed via e-mail, followed by one-on-one consultation with participants to ensure a response.

A portion of the criteria is based on considering property characteristics that are either complex or have more easily defined perimeters. The intention is to acquire a broad spectrum of perimeter security applications. Additional content elicits the existence, frequency, and type of breaches; risk identification methods; action(s) to mitigate; existence of clearly defined objectives; occurrence of benchmarking; development and specifics of design and testing criteria; adherence to schedule and budget; procurement approach; adequacy of funding; participation during implementation; monitoring and control application; adequacy of training; identification of challenges; and lessons learned.

The following is a brief overview of the survey results. The respondents represent a narrower sample of airports and airport managers' views than originally intended.

All respondents had chain-link perimeter fences, and two-thirds had experienced more than one perimeter breach in the last five years. For the most part, the breaches were characterized as persons who accessed, or attempted to access, areas on the airfield mostly without bad intentions, and who were detained before committing a more serious violation. None of the breaches was considered terrorist activity.

Nearly all airports responded that they plan to implement perimeter security improvements in the next year, and all planned to include stakeholders in the planning, development of a ConOps, and identification of requirements for their project. In addition, all anticipated the need for—or in the case of systems already implemented, required—additional staff to operate, maintain, and/or administer their PIDS.

A majority of airport-implemented PIDS are integrated into command-and-control systems located in operations centers with airport police, security personnel, or contract security personnel monitoring the systems' displays. The sensors in those systems were selected specifically to operate within the airports' unique environmental features, including hills, mountains, swamp and wetlands, lakes, and oceans. Nearly all included at least CCTV cameras.

Half of the respondents with PIDS conducted system trials prior to procuring the systems to assess how the system would operate at that airport.

A majority of the PIDS projects took longer than originally scheduled to implement, but all were completed within budget.

SECTION 2. AIRPORT PERIMETER SECURITY PRINCIPLES, CONCEPTS, AND MEASURES

This section provides the basis to establish and maintain airport perimeter security, including core principles, physical security measures, perimeter intrusion detection technologies, and supportive assessment technologies. The goal is to provide guidance in identifying and applying perimeter security that is customized to meet specific airport needs.

2.1 Core Principles

The overarching purpose of an airport perimeter security system is to protect aircraft, people, and airport property as well as to prevent inadvertent entry to the aircraft movement areas by unauthorized persons or vehicles. Furthermore, the perimeter security systems can help provide an improved response and interdiction to perimeter breaches. Because this is so important, the Federal Government requires commercial service airports to have perimeter fences through both safety (33 CFR § 139, administered by the FAA) and security (49 CFR § 1542, administered by the TSA) regulations. Transportation Security Regulation (TSR) §§ 1542.201 and 1542.203 set forth specific requirements to prevent, detect, and respond to the unauthorized entry of individuals and vehicles in secure airport areas, either through natural boundaries or other means such as fencing. Perimeter security at airports can be achieved through a variety of means, and given the unique requirements of each airport, there is not a “one size fits all” solution. The size, location, and environment of an airport will likely dictate its best perimeter protection system. A full perimeter security system (either staffed patrol, physical measures, technology, or any combination thereof) should **deter/delay, detect, assess/classify, locate, and identify** potential or actual breaches of the airport perimeter in a proactive manner, and enhance the efficiency of security personnel in **responding** to security breaches.

Core principles to facilitate effective airport perimeter security, including layered protection, patrols, alarm assessment, communication, and response, are discussed below.

2.1.1 Layered Protection

The primary vulnerabilities of most airport perimeters include the large geographic extent of the perimeter and, in some cases, periodically isolated areas along the perimeter with limited human traffic. To combat these vulnerabilities, a layered protection strategy is recommended. This strategy incorporates people, processes, and technology to decrease security risk through deterrence, detection, denial, delay, defense, and defeat tactics. Meeting the regulatory requirements of CFR 139 and TSR 1542 is the bare minimum. As the number of tools and tactics in the security strategy increase, the probability of successful security intrusion decreases.

Layered protection, also referred to as “rings of protection,” is the concept that multiple independent layers of protection are better than a single protection mechanism. Though not unique to aviation, the concept can be tailored to an airport environment. The layers may be technological, procedural, and/or policy-based, and can be considered as concentric rings of protective measures surrounding an asset. The idea is that if one protective measure is avoided or defeated, additional measures will still be in effect. The protective layers of perimeter security are intended to provide one or more of the following functions:

- Deter (stop an intrusion before it happens)
- Detect (know if an intrusion is taking place)
- Delay (slow down the intrusion to allow for effective law enforcement response)
- Deny/Respond (barriers, stand-off distances, response forces deployment)
- Defend (protect an asset or assets by shielding them from potential harm)
- Defeat (personnel to defeat or neutralize an intruder)
- Response (provide situational awareness information to responders)
- Recover (ensure that all processes and systems are operating in a nominal fashion and that the threat/incident is contained)

2.1.1.1 Deter

A person who is contemplating crossing an airport perimeter but perceives a risk of failure and/or apprehension may be deterred from attempting to breach the perimeter. The effectiveness of deterrence may vary with the person's level of sophistication, state of mind, the asset's attractiveness, and the person's objective. Deterrence begins at the farthest point away from the location of the assets, and should consist of a mix of protective design elements such as physical barriers, lighting, and security systems. The objective of perimeter security elements is to deter the aggressor from even attempting a breach. Deterrence is a psychological approach, and when security is effective, a breach is not attempted.

Applying surveillance technology along a perimeter as a method of deterrence typically requires use of overt, large camera enclosures that make it obvious to all approaching the perimeter that they are under surveillance. Signs saying "no trespassing" or "area under surveillance" also aid in communicating a deterrence message to unauthorized persons. Methods of deterrence may include any of the following:

- Fencing and signage
- Barriers (fencing, walls, bollards, etc.)
- Active patrol and "see something, say something" programs
- CCTV
- Lighting
- Overt technical surveillance

Most airports have a standard chain-link fence with barbed wire to meet the minimum standard as outlined in FAA Advisory Circular (AC) 107-1 issued on May 19, 1972. Ideally, the airport perimeter security designer must consider and weigh the aesthetic aspects of deterrence against the cost and effectiveness. For instance, a highly effective deterrent may be a 20-foot cement wall around the airport, but the airport may not wish to project the appearance of a fortress and most likely will not be able to secure funding from the airlines or FAA to install such an imposing feature. Sections 2.2 and 2.3 of this document provide information on perimeter security deterrence features.

2.1.1.2 Detect

The next layer of protection is detection of a perimeter incident. Detection can be achieved through observers reporting or through electronic means. Most airports have specific perimeter patrols carried out by law enforcement, operations, or security personnel. However, the majority of vehicle traffic is

airline, airport maintenance, air traffic control, fueling, ground handling, and flight kitchen personnel, and members of the public who may be in the area. A healthy “see something, say something” program can provide hundreds of extra eyes for detection. Detection measures provide real-time or near real-time identification of potential acts of aggression (perimeter breach) and communicate appropriate information to a control center, security personnel, or response forces. Electronic detection measures may consist of access control systems, intrusion sensors, and assessment and surveillance systems, either deployed independently or as part of a PIDS. Section 2.3 of this guidance provides significant detail regarding perimeter detection technologies.

2.1.1.3 Delay

To the extent that is safely possible, the objective of a delay measure is to provide sufficient response time for airport law enforcement, operations, or security personnel to respond to alarms and mitigate the threat. This could be as simple as an airport employee verbally telling the intruder to stop and letting them know that they have been seen. Physical barriers also can be used to delay intruders. A perimeter security delay measure commonly used outside the United States is a double fence. The presence of a second, high fence forces the intruder to spend time climbing over a second barrier. Additional measures include asset compartmentalization and target hardening.

2.1.1.4 Deny

The objective of denial tactics is to keep unauthorized persons out while allowing authorized persons to enter. Generally, the deny function at the perimeter consists of fences, barriers, and access control technology, such as biometric or card access system, responding airport law enforcement or security/operations personnel, or a staffed security gate at the point of entry. These methods are found at many airports. Surveillance also may be used to provide visual verification and access denial.

2.1.1.5 Defeat

Most airport protective systems, including perimeter security, depend on law enforcement, operations, or security personnel to defeat or neutralize an intruder. Since intruders can be human, mechanical (unmanned aircraft system), or wildlife, the types of assets used to defeat intruders may vary. The defensive and detection systems designed to support perimeter security should accommodate (or at least not interfere with) operations, security personnel, or response team activities.

2.1.1.6 Response

Response to a perimeter breach incident requires knowledge of the situation and the airport geography. A perimeter security measure is to provide situational awareness (time, location, and general description of the incident) so that an appropriate and effective response can be carried out to address it. The type of intrusion will dictate the response, although multiple agencies often respond. Reports from witnesses or observations from CCTV systems are the best way of helping first responders know the extent and circumstances around the breach. Depending on the severity of the breach, airport operations or law enforcement may choose to set up incident command and an incident command post. Compromised perimeter fences need to be continuously monitored until fixed, and the TSA needs to be notified of the changed condition of security.

2.1.1.7 Recovery

Recovery from a perimeter security incident will vary based on the severity of the breach and whether the perimeter (usually a fence) as identified in the airport security program has been breached. The airport security coordinator (ASC) must notify the TSA if the perimeter was breached. The ASC should work closely with airport maintenance to develop a plan to fix the breached fence, if necessary, and notify the TSA of the plan and timeline for securing the perimeter. A PIDS can support recovery by providing an electronic log of the incident as captured by the system. This can be used to provide incident key performance indicators—incident metrics—such as time and location.

2.1.2 Perimeter Protection Components

Perimeter protection at airports may consist of physical, personnel, and/or electronic systems. Airport perimeters are lengthy and often include numerous vehicle and pedestrian access points that add to the challenge of determining authorized entries versus unauthorized intrusions. Some airports may only require law enforcement officer or security personnel patrols of the perimeter while others may require a full PIDS. A needs assessment (discussed in Section 3.2.1) will help an airport determine the appropriate perimeter security measures for its facility.

The following sections discuss the physical and electronic components of airport perimeter security. It should be noted that National Safe Skies Alliance manages the Airport Security System Integrated Support Testing (ASSIST) program, which helps airports assess technology. The ASSIST program includes testing of security systems at airports, with the goal of providing an objective evaluation of the technology's performance in the potential deployment environment. ASSIST reports are posted to the Department of Homeland Security's Homeland Security Information Network, to provide ASCs at all US commercial service airports with objective data that will support their security programs.

2.2 Perimeter Security Systems – Physical Measures

Every US airport with commercial service has a fenceline and other physical security measures. Physical security measures are essential for regulatory purposes and to deter, delay, or otherwise slow the progress of adversaries attempting to breach an airport's secure perimeter. Perimeter security systems are generally composed of several types of physical automated or static protection systems deployed throughout an airport. The level of physical security measures required is determined by considering several factors, including, but not limited to, the following:

- Potential threat type, capabilities, and equipment
- First response capabilities, equipment, accessibility, and response time to the perimeter being protected
- Distance and estimated time for an adversary to travel the distance from the perimeter to the nearest critical asset

The focus of the research is on identifying and sharing optimal deployment strategies for each measure, as well as identifying key environmental factors to consider. Barrier types addressed include fencing, walls, gates, maritime security barriers (for airports with water perimeters), and vehicle intrusion barriers. When implementing physical security measures, the potential for obstruction of view, reduction in natural surveillance, and impacts on mechanical/technological surveillance should be considered.

Given the diverse nature of airport operations, environmental conditions, topographical composition, and other factors, any single solution will not be effective for every airport.

2.2.1 Fencing

The FAA initially established guidance for fencing in Aviation Security – Airports AC 107-1. This circular recommended:

- Fencing of 10-gauge, galvanized steel, chain-link fabric that is at least eight feet in height should be installed.
- A three-strand, 12-gauge barbed wire topper should be installed at a 45-degree angle from the horizon toward the exterior of the fence with strands no more than six inches apart.
- For areas requiring high security, double apron overhang barbed wire and fencing in excess of eight feet is desirable.
- Fence posts should be installed at 10-foot intervals on center.
- Top and bottom selvages of the fence should have a twisted and barbed finish. The bottom of the fence should be installed within two inches of hard surfacing or stabilized soil; however, in areas where unstable soil conditions are prevalent, the fabric should be installed to extend at least two inches below the surface or embedded in concrete curbing.
- All fencing should be grounded, and metallic fencing should not be installed where it will interfere with the operation of navigation aids.
- Where traverse culverts, troughs, or other openings larger than 96 square inches in the perimeter are unavoidable, the openings should be protected by fencing, iron grills, or other suitable barriers to preclude unauthorized access into the area. These barriers should be composed of materials at least equal in strength and durability to the fence, and should be installed in a manner that deters unauthorized entry but does not deter drainage;
- Fencing should be installed to within two inches of any wall that forms a part of the perimeter.
- If practical, where property lines, location of facility buildings, and adjacent structures permit, the fence should be located no less than 50 feet from any interior structures.

While this circular has been canceled by the FAA, given the shift of responsibility for security to the TSA, the guidance within the document continues to be the unofficial industry standard. Much of this guidance is carried over in PARAS 0004 *Recommended Security Guidelines for Airport Planning, Design, and Construction*, which details recommendations for perimeter protection and barriers. There are some advancements and modernizations noted in the following excerpt, including the advent of anti-cut/anti-climb (AC/AC) fencing: “Fencing is available in several designs that are difficult to climb or cut; or are provided with motion, tension, or other electronic sensing means. For fences with sensors, either mounted on the fencing or covering areas behind the fencing, there are other security system elements for monitoring the sensors and responding to intrusion alarms.” (TransSecure, Inc. 2017)

The emergence of newer fence fabrics, including AC/AC fencing, has gained some degree of prevalence in recent years. Often, this fencing type is selected as a means of providing higher security for an area while attempting to avoid the use of difficult-to-maintain security fence toppers such as barbed, razor, or concertina wire. This subject will be discussed in further detail below.

Regardless of the fencing manufacturer, the spacing between individual wires plays a critical role in frustrating adversary attempts at intrusion. Airports should work with manufacturers to determine the optimal mesh size for individual applications.

Additionally, expanded metal fencing has found favor at critical infrastructure sites, such as electrical substations in the Midwestern United States, due to the higher potential level of security when compared

to chain link fabric, and the typically higher cost efficiency when compared to wire mesh AC/AC fencing. Similar expanded metal fencing products may provide an effective middle ground for use at airports.

Table 1 details the potential pros and cons of using fencing systems as a barrier.

Table 1. Fencing System Roles in Airport Perimeter Security

Factor	Potential Benefits and / or Applicability
Deter	Fencing systems provide significant deterrence to untrained adversaries. The systems themselves serve to clearly identify perimeter boundaries, establish the principle of territorial reinforcement, and may provide a visual and psychological barrier to entry. Fencing also provides structure for security signage to be interspaced (usually in 50-foot intervals) along the perimeter as a means of reinforcing property ownership, safety and security concerns or processes, and legal penalties for trespass on the airport property.
Detect	Fencing systems may be utilized as mounting surfaces for several types of intrusion detection sensors, in addition to providing an identifiable pathway for security patrols tasked with perimeter security. PIDS can be installed to facilitate outward-looking sensors to improve the effectiveness of delay and response.
Delay	Proper installation, design, and structure of fencing systems can contribute to delaying an adversary's entrance to the secure area. Fence height and the inclusion of a security topper are critical to delay. However, delay effectiveness may be limited with respect to trained adversaries.
Assess	Fencing systems may be utilized as mounting surfaces for infrastructure, camera systems, and other technologies that are capable of supporting assessment of PIDS alarms and for active perimeter monitoring by security personnel.
Communicate	Fencing conduit may support communications infrastructure, including network cabling associated with alarm communication and display systems.
Respond	Fencing does not play a role in response with the exception that limited delay may allow time for responders to initiate response and move toward interdiction before critical assets are compromised. Early detection is an important factor in response effectiveness.

Typical fencing examples are discussed below. This guidance remains as product-agnostic as practical; however, it is important to note that there are a variety of manufacturers offering competitive products within the AC/AC fencing space.

The most common fencing at airports is chain-link fencing topped with three strands of barbed wire¹ on angled outriggers. If properly maintained, this type of fence is both effective and cost efficient. For the most part, chain link fences can easily follow varying terrain, are weather resistant, and are widely available through several different manufacturers.

Figure 1 shows a vinyl-clad, chain link fence with 1-inch links and topped with double three strands of barbed wire. A close-up view of the small links is shown as an embedded picture. The small links make it very hard to grip with hands or feet. In addition, the fence has a cement Jersey barrier foundation and is accompanied by perimeter down-lighting. This is an example of a best practice fence because it combines anti-climb characteristics of one-inch links with the cement foundation anti-ramming feature and lighting. The fence is also reinforced with a railing at the bottom that prevents moving or displacing

¹ FAA AC 150/5370-10, Standards for Specifying Construction of Airports contains additional information on the uses and types of barbed wire as part of airport fencing.

the chain link to allow access under the fence. This fence installation serves to deter and delay, and the lighting can assist with detection of a potential perimeter breach.

Figure 1. Example of a Best Practice Fence



Other types of fencing include anti-climb fencing as shown in Figures 2 and 3. While these fence types are more difficult to scale than standard (2-inch link) chain link fences, they are also more expensive.

Figure 2. Anti-Climb Fence



Source: Ameristar Fence

Figure 3. Anti-Climb Fence with Top Barbs

Source: Cochran Fences

An additional type of fence installation is a dual fence line to provide for extended delay. Typically, US airports do not have the necessary real estate to support this type of installation.

If possible, airports should also consider modifying the area on the public side of the fence to make it more difficult for a person or vehicle to breach it. For example, if an angled culvert is in front of the fence, it may make it more difficult for a person or vehicle to breach the fence.

It is recommended that airports determine their need for a specific type of fence by considering the vulnerability of the assets they are protecting. The following questions may be helpful for airports to answer in assessing their need for a non-standard fence:

How close is the asset to the fence? This will provide an indication of the amount of time it would take a potential intruder to reach the asset. Time is a metric that can be used to determine detection probability, response requirements, and level of vulnerability. For instance, a breach over a remote fence line that is several hundred yards from an asset will allow for more time to detect the intruder, and to develop a response to prevent the intruder from reaching the asset, than a breach over a fence located adjacent to an asset.

Is there a lot of activity near the fence? Is it in a high-traffic area where there are often airport employees present? This may help in determining the type of fence, in that the high-activity area can serve as a deterrent and therefore reduce the need for a costly AC/AC fence.

2.2.2 Walls

Walls can serve as physical perimeter barriers as long as they do not present a means for easy climbing. Walls also provide screening and privacy that may be desirable when there is a busy public area abutting

the secure Air Operations Area (AOA). It is recommended that any wall be at least 8 feet high and be topped with multiple strands of barbed wire, as shown in Figure 4.

Figure 4. Perimeter Wall with Barbed Wire



2.2.3 Gates

Perimeter gates can serve as access points for both vehicles and pedestrians; the number of gates should be kept to a minimum. Pedestrian gates typically are used by airport and airline employees. Best practice pedestrian gates are one-way, full-height turnstiles with access control and CCTV coverage. An example of a pedestrian perimeter gate is shown in Figure 5.

Figure 5. Perimeter Pedestrian Gate



The two turnstiles on the right-hand side are landside-to-airside gates. They only turn one way, have access control readers on the gates, and are monitored by CCTV cameras. The left-hand side gate is an exit gate. The gates are topped by barbed wire and about 8-foot high fencing.

Vehicle gates are commonly used for AOA access by maintenance personnel, law enforcement, fuel vehicles, aircraft catering services, and occasionally cargo vehicles. Perimeter vehicle gate barriers are discussed in Section 2.2.5.

2.2.4 Security Barriers for Maritime Perimeters

Airports with waterfront perimeters have a unique challenge. In some cases, the water itself is enough of a boundary and deterrent that the airport may not need anything more than its natural setting. In other instances, where the waterfront perimeter is easily accessible and/or in a high-use maritime area, the airport may choose to set a stand-off boundary or set up a physical barrier.

For airport installations, maritime barriers are best suited to water areas that are relatively narrow, such as an inlet, primarily because they are costly. The need for the installation of a barrier system along a shoreline that is several hundred feet long can be weighed against the perceived threat of a waterfront breach coupled with the value of the nearby assets being protected.

Figure 6 is an example of a typical maritime barrier system installation.

Figure 6. Maritime Perimeter Barrier System



Source: Harbor Offshore Barriers

A stand-off boundary is most appropriate and cost effective for long waterfront perimeters. Stand-off boundaries are areas of “keep-out” zones that form a buffer between the public waterway and the airport perimeter area. Several measures must be in place to effectively implement this boundary. First, a series of static buoys should define the area and serve as a demarcation line. Property boundaries need to be considered when defining the “keep out” zones. Second, the airport needs to establish procedures to execute once the “keep out” zone has been breached.

Figure 7 is a photograph of a buoy (one of many) used to define an airport waterfront “keep-out” zone. This is a relatively cost-effective means of providing waterfront perimeter protection. However, airports need to be aware that buoys will drift, and so routine maintenance is necessary to maintain the correct buffer zone.

Figure 7. Perimeter Keep-Out Zone Buoy Marker



2.2.5 Vehicle Intrusion Barriers

Many types of vehicle intrusion barriers exist. Selection of a specific vehicle barrier type and rating should be based on location, geography, the types of vehicles that regularly access the gate, and the specific threat at that location. Barrier ratings should be assessed via vector analysis using different vehicle speeds, vehicle weights, and vehicle vectors. Gates that regularly have construction vehicle traffic may receive different consideration than a gate that only allows first responder access. Specific types of vehicle intrusion barriers are described below.

2.2.5.1 Passive Vehicle Barriers

Passive Vehicle Barriers (PVB) are typically bollard-type barriers but can also be planters and other landscape elements. Two bollard-type PVBs are prevalent:

- **Permanent:** Permanent bollards (shown in Figure 8) are constructed in place, embedded in a concrete foundation, and not removable. If damaged, these bollards must be excavated from the concrete and replaced in their entirety.
- **Removable:** Removable bollards are used to protect areas where maintenance vehicles and/or equipment must be able to pass through the perimeter barrier system to access an area inside the barrier, such as a mechanical or electrical equipment room. Removable bollards are generally placed in steel-sleeve bases that are installed in concrete, and are secured by padlocks and chains, depending on the configuration. Such bollards are removed only by authorized personnel to allow access for limited and scheduled amounts of time. When these bollards are removed, a secondary security measure in the form of a maintenance vehicle or a temporary barrier should be used so the security of the perimeter is not compromised.

Figure 8. Example of Permanent Bollards



2.2.5.2 Active Vehicle Barriers

Active vehicle barriers (AVB) are operable barriers placed at ingress and egress points to allow or deny vehicle access into or out of an area. The barriers can be electronically or hydraulically operated bollards, wedge devices, net devices, barrier arms, roll-down grills, or swing or butterfly gates that can be activated locally or remotely by security personnel or automatically via access control system (ACS) devices. While an operable barrier arm, an operable roll-down grill, or an operable swing or butterfly gate may be part of a barrier system, they are used primarily to deter access through a barrier point, not prevent it.

2.2.5.3 Active Vehicle Barrier Bollard System

Multiple AVB bollards installed to control a single access way should function as one operable bollard system group or set, with all bollards in the group operating in unison (see Figure 9). Typical AVB bollard features include:

- Traffic lights (red/green/amber) to notify the driver when it is safe and unsafe to proceed
- Road loops for detecting vehicle presence for automatic operation and monitoring of the barrier in the quantity described by the sequence of operation
- Debris screens to prevent road debris from getting under the ground plate and into the underground barrier mechanisms
- A drainage system intended to keep water and other fluids from accumulating in the underground pit into which the bollards retract

Figure 9. Example of a Single Retractable Bollard System

Source: Venta FAAC Road Pillars

It should be noted that retractable (active) bollards are sensitive to certain environments. These bollards are not suitable for extremely dry areas where soil or sand can accumulate in the retraction cylinder and impede its operation. In addition, while the cylinders often have accommodations for drainage, installation in extremely wet environments is not recommended, as accumulated water from frequent heavy precipitation can affect the operation of the bollard.

2.2.5.4 Active Vehicle Barrier Wedge System

An operable wedge barrier is a shallow, below-grade frame assembly cast into a concrete foundation with a heavy steel ramp weldment (plate) capable of rotating to an above-grade position. Typical wedge barrier features are:

- A reflective strip along the face of the barrier that is exposed to a driver while in the secure position
- A red light-emitting diode (LED) strip along the face of the barrier that is exposed to a driver while in the secure position; the red LED strip flashes at a consistent rate
- A “traffic light” (red/green/amber, as noted in the sequence of operations) to notify the driver when it is safe and unsafe to proceed; each barrier or set is equipped with its own light that is designed to operate per the sequence of operation
- Road loops for detecting vehicle presence for automatic operation and monitoring of the barrier in the quantity described by the sequence of operation
- Debris screens to prevent road debris from getting under the ground plate and into the underground barrier mechanisms
- A drainage system intended to keep water and other fluids from accumulating in the underground pit
- Rubber pads, nylon blocks, and other manufacturer-recommended measures to minimize noise produced by the wedge barrier when it is in operation and comes to a rest

A standard wedge barrier is shown in Figure 10. These heavy barriers typically operate by hydraulics and are crash-rated (different systems have different ratings) to stop certain tonnage vehicles traveling at certain speeds. They are extremely effective but must be replaced after impact.

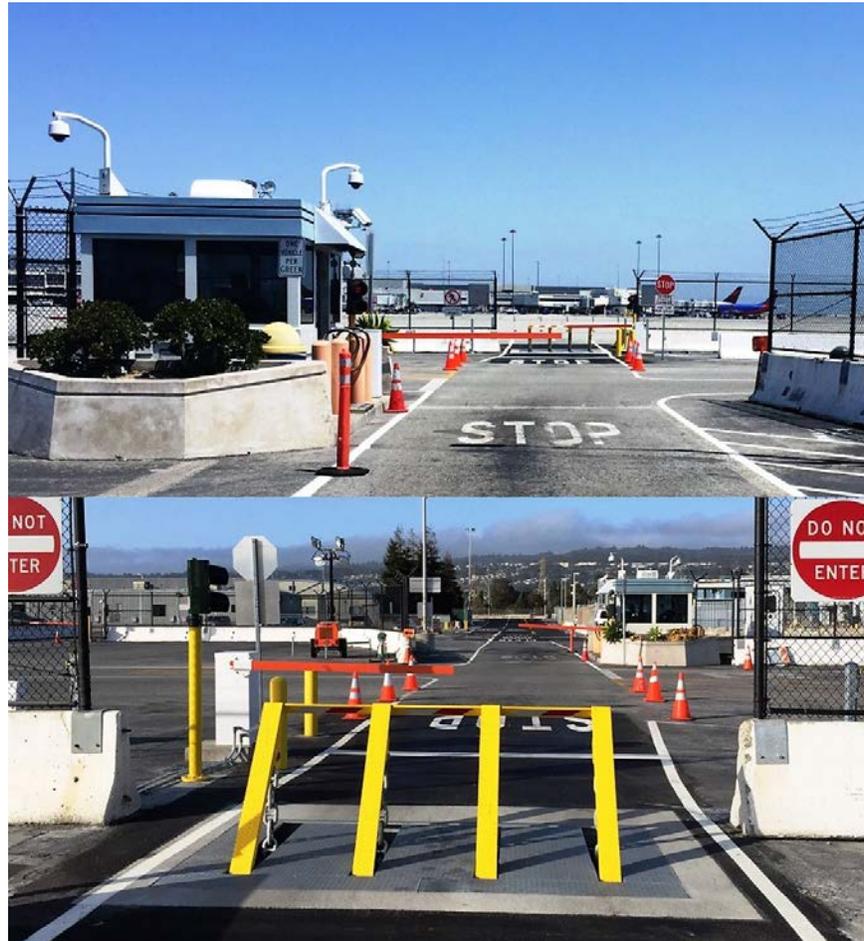
Figure 10. Typical Delta Wedge Barrier System



Source: Delta Scientific

Active vehicle barriers are often deployed at airport perimeter vehicle gates and are used in concert with other intrusion barriers. Figure 11 shows a perimeter vehicle gate from the public side (top) and the same gate from the airside (bottom). A vehicle is stopped at the guardhouse by a drop-arm gate. Credentials are checked and, if approved, the guardhouse drop-arm gate is raised and the vehicle proceeds forward to a second drop-arm gate with a traffic light that signals the vehicle to stop or proceed. The first drop-arm gate is lowered. The traffic light will remain red until the moving vehicle barrier is dropped and the second drop-arm gate is raised, allowing the vehicle access to the airside.

Figure 11. Airport Perimeter Gate with Active Vehicle Barrier System



The need for a wedge system must be weighed against the cost of operating and maintaining the system. In addition, these systems should not be deployed in high-traffic areas where they will need to be lowered and raised hundreds of times per day, as they are not designed for this type of operation.

2.2.5.5 Active Vehicle Barrier Net System

A net system is an active vehicle barrier that deploys nets from below the pavement (see Figure 12). The net barrier is flexible and absorbs energy during an impact, reducing the risk of injuring a driver. The energy absorption systems reset automatically after an impact; normally there are no parts to replace or downtime after a typical impact.

The AVB net barrier retracts into a below-pavement housing equipped with a protective lid to keep out debris, trash, snow, and ice, and protecting the cable net from salt water environments. Below-pavement housings are typically capable of supporting a 32,000-pound axle load or a 16,000-pound wheel load, and have dampers that minimize sound from vehicles crossing the lid when closed. The housing follows the slope in the road and is equipped with a drainage system intended to keep water and other fluids from accumulating in the underground housing.

The AVB net system is equipped with a mechanism that allows the net, or the connection of the net to its supports, to fail when subjected to the defined failure load input.

Figure 12. Active Vehicle Barrier Net in Operation



The photographs show the net fully engaged (top), as it drops (center), and finally as it is fully disengaged to allow vehicle passage (bottom).

While the system is costly, only a pin for the hydraulic arms needs to be replaced if the system is used to halt an oncoming vehicle. It is recommended that the airport undertake analysis to determine the cost versus benefits of such a system.

2.2.5.6 Active Vehicle Barrier System Accessories

TRAFFIC SIGNALS

Each set of operable barriers can be equipped with a means of displaying a red and green signal light (as defined under the sequences of operation) that is visible to the vehicle operator during all times of the day and in all weather conditions. The intent of the light is to alert vehicle drivers of the vehicle arrestor position. The green light indicates that the vehicle barrier is fully down, and the driver may proceed with caution; the red light indicates that the vehicle barrier is not fully down (either in the motion of lowering, in the motion of rising, or fully up) and the driver should not proceed. Lights should be provided on both the secure and non-secure side of the barrier to signal a vehicle operator approaching from either direction.

SAFETY SENSORS

Operable barriers may be equipped to detect vehicle presence either for safety reasons or for triggering another function of the barrier system. Examples of safety sensors for operable barriers include:

- Photoelectric beam detector (non-reflective) for detecting the presence of a vehicle
- Vehicle loop detector installed in the ground for detecting the presence of a vehicle
- Vehicle probe detector based on magnetometer technology

MASTER AND SECONDARY CONTROL PANELS

Operable barriers may be equipped with a hydraulic power unit to operate the barrier, and a remote secondary control panel located near the barrier system for manual operation of the barrier with a separate connection back to a master control panel in a central control center. Lockout capabilities can also be accommodated via a three-position key switch: automatic, local, and remote.

2.2.5.7 Emergency Lighting/Power Systems

Airports often have backup power systems to support airfield lighting, and consideration should be given to backup power for the vehicle gates and lighting systems around the perimeter. When there are power outages, it is critical for the airport to know the default setting for the vehicle gates so that there is not an inadvertent breach in the perimeter, especially if no CCTV coverage is on the gates.

Lighting often is necessary for nighttime visual surveillance. In addition, lighting can serve as a deterrent along perimeters and enables physical monitoring and response to security alarms. The Illumination Engineering Society Handbook provides recommended minimum average illuminances for specific areas and purposes.

To support perimeter security systems, alarm assessment, and central control center functions, emergency power should be supplied via emergency generators. In addition, a three-phase continuous-duty, on-line, double-conversion, solid-state uninterruptible power supply (UPS) should be considered.

The UPS should operate in conjunction with the existing electrical system to provide power conditioning, back up, and distribution of conditioned power for critical electrical loads.

Emergency lighting should also be linked to emergency generator power. If the generator fails, runs out of fuel, or if the area of the airport is cut off from emergency generator power, emergency backup lighting power should be provided by power-inverter-connected backup battery packs. Emergency generator power systems should be monitored at the central control center and tested regularly.

2.2.6 Crime Prevention through Environmental Design (CPTED)

Under the crime prevention through environmental design (CPTED) concept, “the proper design and effective use of the built environment can lead to a reduction in the fear of crime, and the incidence of crime, and the improvement of the quality of life.”² Research on the impact of the built environment on human behavior reveals steps that can be taken by facility designers and owners to increase the potential adversary’s perception that their activity may be observed, reported, and/or responded to.

It is recommended that airports consider CPTED concepts when determining their overall protective strategy and, in particular, when developing their perimeter security programs. There are several factors to consider, depending on resources or methodologies used when implementing the CPTED program. In our experience, the model utilized by the National Institute of Crime Prevention in the United States is effective. CPTED, as adopted by ASIS International, includes five principles, which are described below.

2.2.6.1 Natural Surveillance

Natural Surveillance increases the threat of apprehension by taking steps to increase the perception that someone’s activities will be observed.

To enhance Natural Surveillance, exterior lighting should be provided in as many public spaces at the airport as possible. There are recommendations to limit lighting near movement areas, but all pedestrian pathways, terminal frontages, parking areas, and approach roadways should be lit for both safety and security reasons.

Exterior lighting applications should be implemented in accordance with Illumination Engineering Society of North America (IESNA) standards to include IESNA RP 33-99.

LED is the preferred security luminaire type due to its directional capabilities, elimination of re-strike timing, and high color rendition index, which supports both natural and technological surveillance.

Ground-level vegetation, where practical, should be maintained to prevent creation of areas that could screen or conceal potential adversaries.

2.2.6.2 Natural Access Control

Natural Access Control physically guides people through the site through the strategic design of streets, sidewalks, building entrances, and landscaping.

² The term CPTED was first used by C. Ray Jeffery in his book *Crime Prevention through Environmental Design* (Thousand Oaks, CA: Sage Publications, Inc., 1971). Tim Crowe and Lawrence J. Fennelly used it in the third edition book *Crime Prevention through Environmental Design* (Boston: Butterworth-Heinemann/Elsevier, 2013).

Design of airport terminals should provide a clear main entry that leads passengers and airport visitors to the preferred entry point into the facility. This preferred entry concept can be accomplished using a variety of techniques, including installation of distinguishing sidewalks and pavers, lighting, and differences in paint or facade.

Clearly marking walkways, providing signage restricting passengers and personnel to pathways, and ensuring that effective wayfinding signage is utilized throughout the airport can contribute to natural access control.

Natural boundaries can limit perimeter access, too. A clear example of airport water boundaries are those found at BOS, JFK, and SFO. Each of these airports have water along significant portions of their perimeters. In some cases, the airports have fencing along the perimeter waterways, but not in all cases.

2.2.6.3 Territorial Reinforcement

Territorial Reinforcement provides the perception that airport property is controlled. While not traditional in the application of CPTED, large walls, gate houses, and reinforced fences provide a distinct degree of territoriality for the airport. This concept can also be applied to individual facilities within the airport's perimeter. Individuals who are traversing the interior of the airport should be able to clearly identify when they are transitioning into a higher security area.

To enhance Territorial Reinforcement, enlist a landscape architect to assess region- and function-specific vegetation that can be maintained in such a manner to clearly demonstrate transitions from the exterior of the airport perimeter to restricted or other protected space.

2.2.6.4 Maintenance

Maintenance allows for the continued use of the space for its intended purpose. Airport maintenance personnel must ensure that lighting, vegetation where applicable, cameras, windows, doors, and other elements contribute to the sense of ownership and that activity observation are effectively maintained.

Ensure that lighting, surveillance systems, fencing, vegetation (as applicable), and other security-related items are appropriately maintained throughout the life of the facility. Ideally, recurring maintenance agreements and/or a proprietary maintenance force, supported by a work-order tracking system, is recommended.

Consider implementing a hotline or other notification process whereby security and/or facilities management personnel can be notified of maintenance issues identified by passersby.

Address incidents of vandalism, graffiti, broken windows, and other signs of disrepair that may be representative of a lack of site ownership.

Consider retractable lighting poles for easier access to lighting systems and/or cameras, eliminating the need for bucket trucks or cherry pickers to conduct maintenance.

2.2.6.5 Target Hardening

Target Hardening is the use of physical barriers to entry (bollards, vehicle barriers, boulders, fountains, etc.) and enhanced technological security to mitigate risks. It is typically applied in high-risk areas where the threat of terrorism and/or violent criminal activity is expected.

It is our experience that dependence on physical security alone will be limiting when the goal is to mitigate objectionable behavior.

The application of measures that deter crime, including the threat of observation, may also serve to disrupt portions of the terrorist attack cycle, including target selection, surveillance operations, and rehearsal of attacks. If any of these activities is detected, disrupted, or otherwise deters the planner, a different target may ultimately be selected.

In cases where CPTED strategies conflict with the required physical security measures, it is the physical security measures that should be implemented.

2.3 Perimeter Security Systems – Electronic Measures

The primary measure of success in deploying airport perimeter security is the degree to which it meets its intended purpose and stakeholder needs. Based on the research, airport perimeter security should consist of layered protection of policy, procedures, and physical and technology measures working in concert to employ effective airport perimeter security. Electronic systems deployed for the protection of airport perimeters form the foundation of PIDS. A PIDS can be as simple as several perimeter CCTV cameras or as complex as multiple sensors that are integrated, correlated, and interfaced to a display system.

2.3.1 PIDS Concept

The availability and complexity of security technology has grown substantially during the past 20 years. As a result, there is a tendency to define PIDS by looking first to technology. This approach often results in an application that is 1) substantially more expensive than planned; 2) not risk appropriate; and 3) ineffective.

Methodologies that encompass core principles include the initial step to define perimeter security needs by evaluating the airport's unique needs and security environment, identifying gaps and opportunities, and developing recommendations for adoption of improvements. In short, the problem should be clearly defined before a solution is implemented in lieu of seeking a technology solution first.

A secondary methodology is to evaluate the cost of improvements in order to determine the best course of action consistent with an estimated budget. Ultimately, cost evaluation may result in a phased approach to address both short-term and long-term solutions.

Finally, it is vital to understand that complex technology solutions are interdependent on other systems that are often found in an airport environment, such as ACS and CCTV. In addition, airport operators should be active in defining business processes that effectively integrate and drive the final perimeter security solution to mesh with existing airport security systems.

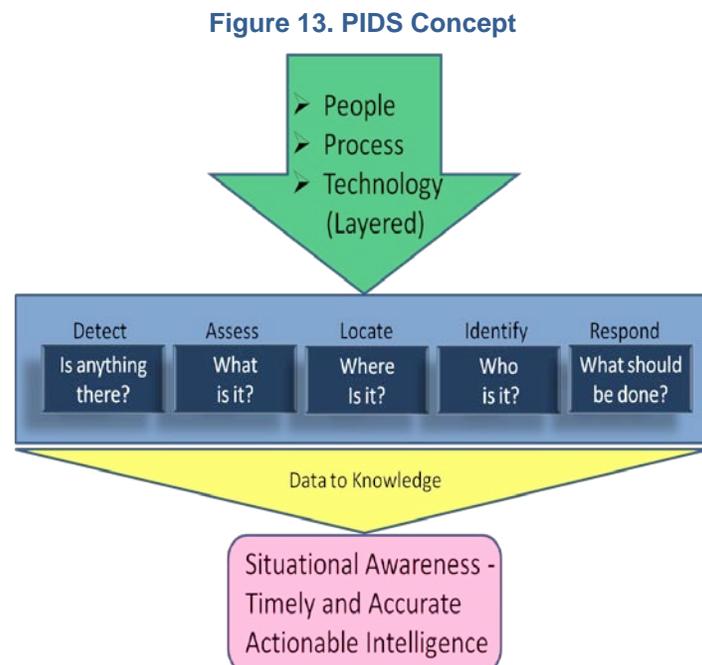
Ideally, a full PIDS should continuously and passively monitor the perimeter and other designated areas using detection methods to eliminate the need for constant human monitoring of video screens. On detection of an intrusion attempt, alert warnings and audible warning signals should be presented directly to security or public safety personnel at an alarm monitoring command-and-control location (operations or communications center) to notify and dispatch the appropriate first responders. At a minimum, the PIDS objectives and scope should include real-time detection, location, assessment, and alarm capabilities. As such, a PIDS should serve as a situational awareness tool to aid airport police, local law enforcement, operations, first responders, and security personnel in their mission.

Effective perimeter security involves people, processes, and technology. A PIDS must include personnel to monitor system alarms and report on potential incidents, as well as the personnel who may report and/or respond to the perimeter incidents. In addition, while it is of paramount importance to provide appropriate electronic security and surveillance systems, it is also equally important to ensure that procedures are in place to support the use of the systems, to validate alarms, and to centrally monitor and dispatch first responders. Fundamentally, *people* comprise the organization and represent various stakeholder functions. These include, but are not limited to, airside and landside operations, aviation security, law enforcement, aircraft rescue and firefighting, maintenance, air carriers, aircraft servicing, and other airport tenants. As its core function, the PIDS will allow highly trained airport personnel to facilitate daily operations and respond to incidents or events that require immediate action.

The implementation of a PIDS will require (possibly new) clear and common *processes, practices, and procedures* that will drive effective and efficient operations through the control, management, and dissemination of timely and accurate data and information. Policies supporting new PIDS-driven SOPs must be drafted, vetted, and adopted by PIDS stakeholders. These SOPs are defined during the development of a ConOps.

Finally, the *technology* of the PIDS must ensure highly effective and efficient security operations, and be deployed and integrated to enhance security operations, communications, information access, knowledge capture, system performance, and infrastructure and process automation. It should be built on an open architecture to allow for ease in selection and upgrading of components. In addition, the system must allow for the incorporation of existing legacy systems.

Figure 13 represents the essential inputs, functional components, and desired results of a PIDS.



At a minimum, a PIDS should detect, assess, locate, and alert security personnel of a perimeter breach, and it is imperative that the PIDS provides this information as timely alarms to airport first responders.

The principal concept of a PIDS is to form an integrated “system of systems” that will provide situational awareness for the airport. A system of systems is a distinctive amalgamation of people, processes, and layers of individual technologies or systems that, when combined, achieve a greater level

than the sum of the individual parts. The combination and layering, through integration and correlation of the sensor technologies, results in a system that maximizes the strengths of the components while minimizing their individual limitations. In addition, the integrated layering of multiple sensors/technologies to detect a potential perimeter breach will increase the probability of detection and reduce the probability of false or nuisance alarms by ensuring that more than one sensor detects an object—therefore verifying the detection—before an alarm is generated.

A PIDS can only effectively achieve these functions when its requirements are clearly and unambiguously defined early in the planning process. The importance of a clear set of requirements is paramount to systems design and testing. These requirements not only define the system's function, but also are used in testing to determine if the system meets the intent of its owner and/or stakeholders. The first step in developing requirements is to define how the system will operate from the user's point of view. In understanding and documenting the system user concept—or ConOps—the developer will ascertain the system operational requirements and describe how the system will operate from the user's point of view.

2.3.2 PIDS Technologies

Perimeter security technologies fall into several categories based on their intended function: perimeter detection technologies, assessment technologies, and command-and-control technologies. Each set of technologies has a specific purpose in the detection, assessment, and response chain of actions.

2.3.2.1 Detection Technologies

PIDS detection technologies consist of sensors that are able to determine *if* something is happening and often the location of the incident, but they are not capable of assessing *what* is happening. For example, a radar system will provide information on an object in the area of interest and can provide approximate location information; however, the radar cannot usually provide (the visual) assessment capabilities that can be provided by CCTV.

In general, perimeter detection systems are a range of technologies that provide reliable detection of an intruder, and, in conjunction with a video surveillance system, allow for visual verification of the intrusion, and assessment for appropriate security or operational response.

Numerous technologies may be employed as part of a PIDS. Each technology has advantages, disadvantages, and varying costs associated with them. Because of the varied threat, nature, and location of the perimeter around the facilities, there will likely be different technologies used for different areas or zones based on the character of the zone, the lighting in the area, the visibility of the area, and the possible threat that a breach in the area would pose. The following are technologies that could be applied, either independently or in conjunction with other technologies, to improve detection and assessment. A brief description of each technology is provided as well as some the pros and cons of that technology.

- Fence Disturbance Sensors
- Microwave Motion Detection
- Electric Field Sensors
- Buried Cable Detection Systems
- Ground Based Radar
- Optical Based Detection/Analytics

FENCE DISTURBANCE SENSOR TECHNOLOGY

Cable-based fence detection systems can be installed on existing fence line locations to detect instances of cutting, climbing, crawling under, or otherwise manipulating the fabric of the fence. These systems are considered to be terrain-following point-of-detection (non-volumetric) sensor systems.

Fiber optic systems consist of processor modules that transmit a laser through a fence-mounted fiber optic cable that is sensitive to a wide range of conditions that will signal an intrusion attempt, including vibration, flexing, compression, and cutting of the fabric of the fence. Another type of system uses heavy duty cabling with embedded accelerometers capable of detecting movements or disturbances along the fence line. The processors on these systems use digital signal processing and algorithms to minimize nuisance disturbances caused by natural events such as wind, rain, or vehicle traffic, while alarming on potential breaches that exceed pre-set conditions and thresholds. Because this type of system can detect the alarm area within 3 meters of the disturbance, it can be used for very large or long zones. The fiber optic systems are not susceptible to electromagnetic interference (EMI) or radio frequency (RF) interference and are intrinsically safe as no power is transmitted through the cable. But, similar to accelerometer cable systems, the fiber optic system is susceptible to nuisance alarms from any disturbance of the fence by animals, high winds, heavy rain, sleet, hail, etc. In addition, it is important to note that these systems are only effective if the fence fabric is touched or otherwise manipulated. The system will not detect an intruder who crosses the fence line without actually touching the fence.

Like most PIDS technologies that do not employ visual sensors, cable-based fence disturbance sensor systems will require the implementation of CCTV cameras and/or analytics to enable assessment of alarms on the perimeter. While integration of these multiple technologies is important to reducing nuisance alarms for the operator, it also requires both detailed calibration and operator training to properly use the system. System calibration or “fine tuning” includes correlation both in time and space of each system’s alert. For instance, a CCTV system using analytics needs to report with a pre-determined level of accuracy the time and location of a “seen” intruder. The fence detection system needs to report a similar time and location of the event as the CCTV analytics in order for the systems to work in harmony. This can be a time-consuming process.

Examples of fence disturbance technologies are illustrated in Figures 14 and 15.

Figure 14. Example of Fiber-Based Fence Detection Technology Installation

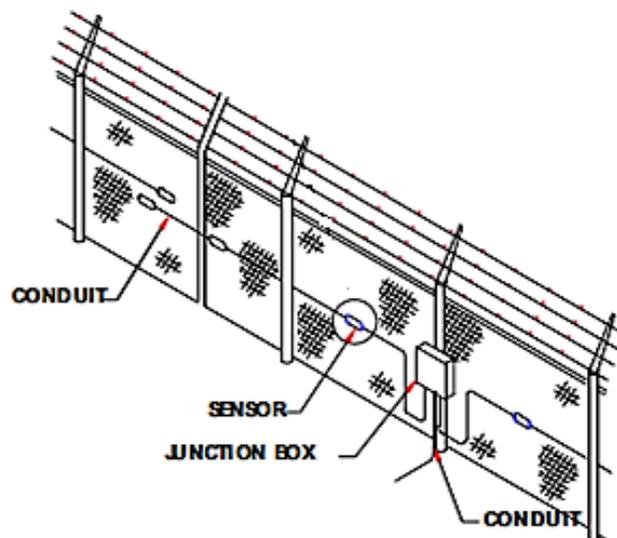


Figure 15. Typical Fence Disturbance System Installations

Source: Senstar, Inc. (left image)

Advantages

- Simple installation along existing fence lines
- Suitable for lengthy perimeters
- Terrain-following
- High probability of detection within 3 meters or better precision
- Fiber – Immunity to EMI (lightning)
- Can utilize adaptive algorithms to minimize nuisance alarms as well as classify alarm events (climbing, cutting, etc.)

Disadvantages

- Proper sensor performance is largely dependent on the condition of the fence
- Susceptible to nuisance alarms caused by disturbances to the fence (animals, wind, hail, large vehicles, etc.)
- Detection location within approximately 100 feet.
- Non-volumetric, so it can be bridged or tunneled
- Calibration and training

ELECTRIC FIELD SENSOR TECHNOLOGY

Microphonic-based fence detection systems can be installed on existing fence line locations to detect instances of cutting, climbing, crawling under, or otherwise manipulating the fabric of the fence. The systems consist of processor modules that receive a signal through a fence-mounted microphonic sensor cable sensitive to the sounds associated with a wide range of conditions that will signal an intrusion attempt, including vibration, flexing, compression, and cutting of the fence fabric. The processors use digital signal processing and algorithms to minimize nuisance disturbances caused by natural events such as wind, rain, or vehicle traffic while alarming to potential breaches that exceed pre-set conditions and thresholds.

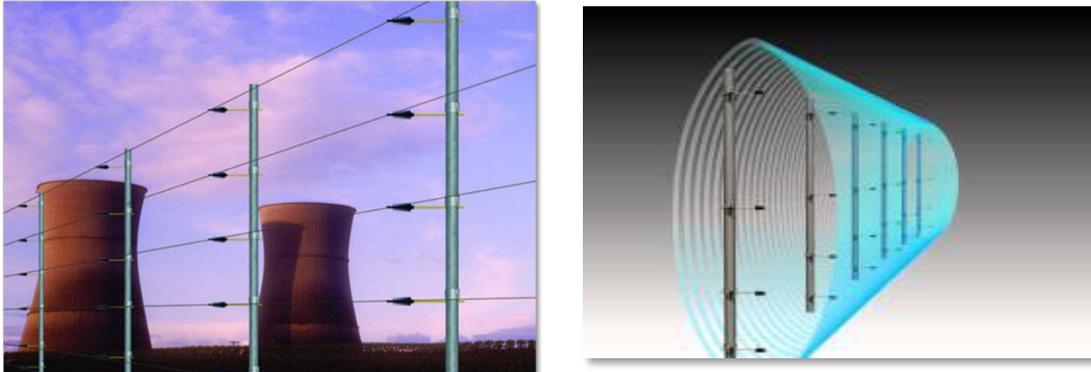
These systems tend to have a single zone for long distances, which makes assessing a specific alarm difficult due to the low level of resolution that these systems provide to pinpoint an alarm. Microphonic systems are susceptible to nuisance alarms caused by vibrations from traffic, EMI and RF interference, or any disturbance of the fence by animals, high winds, heavy rain, sleet, hail, etc. Also, it is important

to note that these systems are only effective if the fence fabric is touched or otherwise manipulated. These systems will not detect an intruder who crosses the fence line without actually touching the fence.

Similar to most PIDS technologies that do not employ visual sensors, microphonic-based systems will require the implementation of CCTV cameras to provide assessment of alarms on the perimeter.

Figure 16 shows some typical Electric Field Sensor system installations.

Figure 16. Typical Electric Field Sensor System Installations



Source: Senstar, Inc.

Advantages

- Terrain following
- Free standing or fence-mounted wires
- Suitable for lengthy perimeters
- Easily configurable detection pattern that can be adapted to fit many situations
- Well contained detection zone

Disadvantages

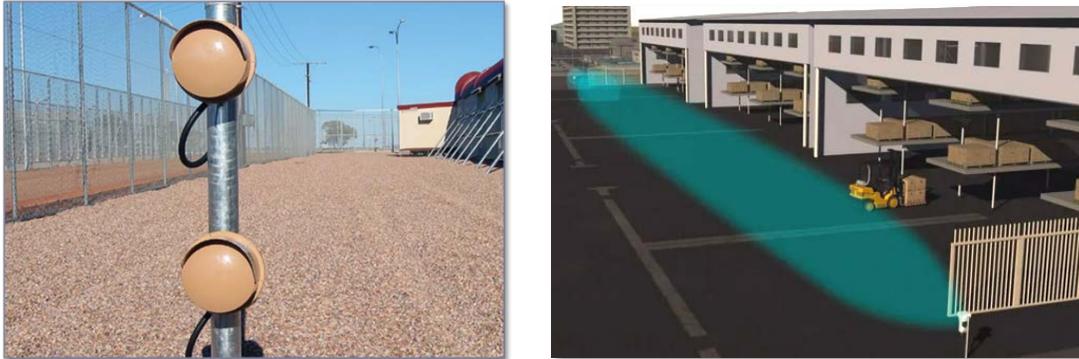
- Requires meticulous grounding of all metal objects in the vicinity
- Heavy rain will cause initial nuisance alarms before the system adapts
- Large moving metal objects (vehicles) near the sensor can cause nuisance alarms
- Microphonic cable is susceptible to EMI and RFI
- Not suitable near roads

MICROWAVE MOTION DETECTION, INFRARED, AND LASER BEAM TECHNOLOGY

Microwave sensors can detect walking, running, or crawling human targets in an outdoor environment. They do not provide visual coverage of detections, and so airports may wish to consider deploying CCTV assessment cameras in conjunction with the microwave sensors. The sensors are deployed in a point-to-point fashion; the sensors generate an electromagnetic field between transmitter and receiver, creating an invisible volumetric detection zone. When an intruder enters the detection zone, changes to the field are registered and an alarm occurs.

Microwave sensors are effective for the protection of open areas, gates or entryways, and rooftop or wall applications, as shown in Figure 17. They provide high probability of detection, low nuisance alarms, and resistance to rain, fog, wind, dust, falling snow, and temperature extremes.

Figure 17. Typical Microwave System Installations



Source: (left image) PT. Kantata Mega Mahesa; (right image) Senstar, Inc.

Infrared (IR) and laser beam technologies are deployed and used in a similar fashion to microwave technology. The devices transmit energy in a point-to-point fashion, thus forming an electronic trip wire. If an object breaks the beam, an alarm is sounded. These technologies can be deployed in single instance as described, or more complexly with multiple beams forming a web of trip wires.

Advantages

- Microwaves are volumetric with a large detection pattern
- Laser/IR beams can be used in tight areas because of very narrow beams
- Weather is typically not a concern, but heavy rain can cause nuisance alarms
- The protection pattern is not known
- Appropriate for long flat areas

Disadvantages

- Requires flat terrain, susceptible to crawlers, not suitable for varying terrain
- Not suitable for rainy climates with poor drainage
- As with any point-to-point technology, the space between sensors must be kept clear of vegetation, debris, and any objects that would preclude a clear line of sight

BURIED CABLE DETECTION SYSTEM TECHNOLOGY

Buried cable detection systems offer covert protection, and detect and report on intruders walking, running, crawling, or otherwise traversing the protected area along a perimeter. Systems can operate on detection of vibrations or disturbance of volumetric electromagnetic fields.

Typical vibration detection systems consist of cabling that is buried along the perimeter. The cable carries a signal (electronic or optical) of a specified frequency. If the area above the perimeter cabling is disturbed by walking persons or even vehicles, the frequency of the signal in the cable is changed, which the system converts into an intrusion alarm. Detection location and reporting is similar to that of volumetric systems discussed below.

Volumetric systems consist of processor modules that transmit a signal through a buried cable that creates an invisible electromagnetic detection field sensitive to disturbances caused by a target's size and speed signatures. The processor uses digital signal processing and algorithms to discriminate nuisance disturbances caused by natural events such as wind, rain, or snow while alarming on potential breaches that exceed preset conditions and thresholds. The typical buried cable will detect an object passing over it or within 1.5 meters on either side of the cable. These systems allow for a very precise detection area based upon the cable placement, but do not provide flexibility for changes as the cable needs to be physically relocated if the target detection area changes.

Buried cable systems will work in a variety of surface materials, including soil, asphalt, or concrete. However, they can have nuisance alarms caused by shifting of soil, ponding of water, and other changes. Though the systems can be tuned to ignore objects under a specified size, they cannot differentiate between a person, large animal, or vehicle. These systems can also be affected by vibrations from traffic or large vehicles, and are vulnerable to EMI and RF interference. Overall, buried systems are typically not used in areas with high traffic or greater than normal EMI and RF interference and are typically not used for long perimeters because of the installation cost.

Similar to most PIDS technologies that do not employ visual sensors, buried cable-based systems will require the implementation of CCTV cameras to provide assessment of alarms on the perimeter.

Figure 18 shows typical installations of buried cable detection systems.

Figure 18. Typical Buried Cable Detection System Installation



Source: (left image) Southwest Microwave; (right image) Technicontrol

Advantages

- Covertness forces intruders to guess the location and presents a more aesthetic installation
- Precise detection – most systems can locate an alarm within a 3-meter window
- Can be installed under a variety of areas
- Effective at detecting crawling intruders

Disadvantages

- Can be susceptible to nuisance alarms from soil shifting, ponding of water, and vibrations
- Susceptible to EMI and RF interference
- Cannot differentiate object size as well as other systems (animal, person, or vehicle)

GROUND BASED RADAR TECHNOLOGY

RADAR is an acronym for Radio Detection and Ranging; the name applies to both the technique and the equipment used. Radar is a sensor whose purpose is to provide estimates of certain characteristics of its surroundings that are of interest to a user, most commonly the presence, position, and motion of objects in its vicinity such as aircraft, ships, vehicles, or in some cases people. Radar operates by transmitting electromagnetic energy into the surroundings and detecting energy reflected by objects.

Radar systems provide real-time, volumetric surveillance and serve as all-weather detection and tracking sensors. Radar systems in PIDS can search a wide area, detect and track an object approaching a secure area, and provide accurate object location information, usually within seconds. They are an attractive PIDS surveillance option because of their high coverage efficiency (i.e., their coverage-to-cost ratio).

The best deployment environment and use of a radar system for perimeter intrusion detection is in an open area. An advantage of radar compared to fence line PIDS technologies is that it is able to provide detection beyond the perimeter, therefore allowing for early warning, possible predictive analysis, and mitigation. Additionally, radar is able to track detected threats from beyond the perimeter and, after a breach, inside the perimeter. Tracking of a threat may allow for more effective resolution as the location information can aid incident responders.

Generally, there are three primary types of radar systems for use in intrusion detection systems. These systems are defined by the methods each system employs to form detections on objects: (1) detection based on the movement of an object, known as Doppler radar; (2) detection based on the amplitude or strength of the returned signal of an object, referred to here as a non-Doppler radar; and (3) detection based on a continuous wave (non-pulsed) and frequency-modulated signals, known as frequency modulated continuous wave (FMCW) radar. Doppler and FMCW radars are most commonly used for airport perimeter security.

FMCW radar systems transmit a continuous (not pulsed) wave of energy, but over multiple frequencies or phases. The frequency (or phase) modulation allows the system a means to measure reflected target range and velocity.

Because Doppler radar systems form detections based on the movement of an object, they are incapable of detecting stationary targets or targets that move in a radially constant arc—a constant distance—around the system. A way to address the latter is to install multiple Doppler systems that have overlapping fields of view so that if the target is not detected by one radar system, it will be detected by another system. While these characteristics are important to note, it should also be noted that threats to breach airport perimeters are not likely to move in this fashion.

A radar system's detection range (distance of the detected target from the radar antenna) and azimuth (angular location of the target) resolution are dependent on system characteristics such as operating frequency, pulse width, radiated power, and antenna beam width. PIDS radars use a wide range of frequencies; however, those using higher frequencies have smaller antennas and their processing allows for higher resolution.

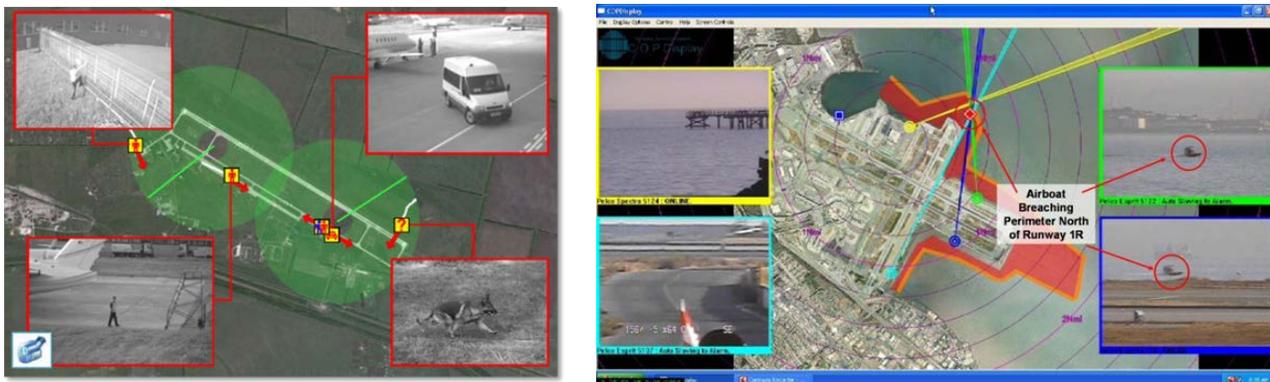
The radar system's resolution determines its ability to distinguish between closely spaced targets. This is important in being able to differentiate between multiple targets and when detecting targets near objects such as fences or buildings. Both range and azimuth resolution are constant when measured in distance (e.g., yards/meters) and angular (e.g., degrees) units, respectively. However, azimuth resolution increases as the distance from the radar increases. As a result, range-azimuth cells farther from the radar are larger in azimuth than cells closer to the radar. A narrower antenna beam width results in a higher-resolution system.

PIDS radars should be high resolution in both range and azimuth to enable detection and tracking of small, closely-spaced targets. The PIDS designer should look for a radar system with a narrow azimuth beam width and high range resolution due to processing. Commercial radar systems are now available with azimuth resolution of less than 1 degree and range resolution of less than 1 meter, which provide reliable detection and tracking.

Radar is good for detection, but other technology is required for assessment of alarms. Similar to most PIDS technologies that do not employ visual sensors, radar will require the implementation of CCTV cameras to provide assessment of a detected target. The radar detection information can be used to slew a CCTV camera to the location of the detected target so that an operator can see the target. It should be noted that many commercially available PIDS radar systems now are sold as integrated units with a radar and a CCTV camera in a single component.

Figure 19 shows examples of typical airport radar system displays.

Figure 19. Typical PIDS Radar System Display



Advantages

- Effective in day and night
- Tracks detected targets – outside and inside the perimeter
- Works well in fog and most weather
- Real-time, accurate volumetric detection of objects

Disadvantages

- Not terrain-following
- Detection, but no assessment unless integrated with pan-tilt-zoom (PTZ) – many available systems are fully integrated with a PTZ
- Susceptible to clutter and multipath when used in confined areas – best used in wide open spaces

OPTICAL BASED DETECTION/VIDEO ANALYTICS TECHNOLOGY

CCTV cameras are best used for assessment functions; however, they can be effective detection sensors when coupled with video analytics technology. Video analytics (VA) is a technology in which images from a camera are analyzed and processed to recognize and report on specific events in the scene. VA has many capabilities, but one that is especially useful for airport perimeter security is the detection of

the image of a person crossing into (or out of) a predetermined area in a scene. It is a way to define virtual boundaries and detect if a person crosses that boundary.

While VA for perimeter protection may be effective, it is important to note that the cameras providing the images for perimeter protection analytics should be capable of providing images 24/7; the cameras need to work in daylight as well as in darkness. Wide-dynamic range (WDR) cameras (see Figure 20) and thermal/IR cameras (see Figure 21) can provide video images for analytics day or night. WDR cameras are capable of lowlight imaging and backlight compensation to ensure clear views in dynamic lighting conditions. Thermal and IR cameras detect and form images based on the heat of an object, and do not rely on light for imaging (see Figure 22). More detail on camera technologies is found in Section 2.3.2.2 Assessment Technologies, and in Appendix A on Supplemental Camera Technology Information.

It should be noted that illumination can greatly affect the ability of a camera to provide usable video. Shadows, high contrast, and backlit scenes make it difficult to provide usable video to the necessary levels. Lowlight cameras and cameras with WDR are designed to perform well in situations where the available light is not consistent or adequate for traditional cameras. In outdoor perimeter surveillance, it is important to consider that the sunlight shifts in intensity and direction throughout the course of a day. Weather conditions will also affect lighting and reflection. Fog and wet tarmac, for example, will intensify the reflected light, while rain will absorb much of the reflected light. Most black-and-white cameras have a lower lux rating than their color counterparts, but most airports desire color video when possible. To overcome this issue, many manufacturers have developed cameras that switch to a black-and-white mode to allow for lower-light video but will offer full color when the lighting level is adequate.

The following are the advantages and disadvantages of WDR cameras, thermal cameras, and video analytics (see Figure 23) for use in detection of potential perimeter intrusion targets. Section 2.3.2.2 Assessment Technologies has more detailed information on WDR, IR, and thermal camera technologies.

Figure 20. Example of a WDR Camera Installation



Advantages

- Day/night cameras provide full-color images when light levels are sufficient
- When light levels fall below a certain threshold, these cameras can make use of near infrared to provide black-and-white images

Disadvantages

- Without additional illumination of the target, day/night cameras will lose the image even in night mode once the light levels are low enough
- Since these cameras use visible and near-visible light, they are susceptible to environmental issues (rain, fog, or snow)

Figure 21. Thermal Camera



Source: SightLogix, Inc.

Figure 22. Thermal Imagery



Source: FLIR, Inc.

Advantages

- Thermal cameras view a spectrum of energy that relates to emitted heat
- Thermal cameras provide detection capabilities without additional lighting
- Thermal cameras are less susceptible than visible-spectrum cameras to fog, heavy rain, snow, and dust

Disadvantages

- Thermal cameras are typically low resolution and cannot see through glass
- Thermal cameras may have difficulties in warm climates where the ground temperature becomes close to human body temperature – this can make it difficult for an operator to see the intruder, and may make affect the ability of video analytics to function as needed

Figure 23. Video Analytics Detecting Persons and Objects



Source: Irvine Sensors

Advantages

- Analytics enable CCTV cameras to be used as detection sensors
- Analytics can be used to detect activities beyond intrusion, providing pre-alarms of suspicious activities
- Precise detection zones can be implemented using analytics and modified simply through software
- Digital signal processing can be used to stabilize images and filter environmental motion to allow video analytics to operate more efficiently and with fewer nuisance alarms

Disadvantages

- Analytics can be susceptible to nuisance alarms, especially complex analytics like “object left behind”

2.3.2.2 Assessment Technologies

The assessment function is vital to the success of an airport perimeter security program. Assessment of an alarm is the process by which the operator can determine the validity of the alarm. The assessment process should answer the question, “what is it?” when something is detected by the system. For instance, operators can determine whether an intruder is human or animal. Animals often will cross an airport’s perimeter, and a detection of such an event would be considered a nuisance alarm rather than a true alarm. Once it is determined that the alarm is a true alarm, the incident information is communicated to dispatch and an appropriate response is coordinated. Most airport staff who would be monitoring and assessing these alarms also have responsibilities to monitor other systems, so it is important to simplify the assessment process as much as possible.

Camera systems have advanced rapidly so that highly capable cameras are often systems in and of themselves. Below is information on various assessment cameras. For more detailed information, please refer to Appendix A on Supplemental Camera Technology Information.

CAMERA TECHNOLOGIES

The introduction of digital IP-based cameras and video management systems (VMS) into the security market revolutionized the industry, and these systems are now the driving force for all future innovations. Systems that utilize analog technology at any point in the chain (camera, recording, monitoring, etc.) are destined for obsolescence. IP-based systems now provide a host of benefits over analog systems, at a price that has become comparable. Below are some of the advantages of IP-based camera technology.

- **Image Quality:** IP cameras offer better image quality over their analog counterparts, even between cameras of equal resolution. IP cameras have the advantage of digitizing the incoming image once, at the time of image capture. Analog camera systems have to convert signals from analog to digital many times in the process and are susceptible to image degradation each time, as well as through the transmission of the signals. IP video has no image degradation due to distance traveled by the nature of the IP/Ethernet transport.

Additionally, all camera development is migrating to high-resolution IP cameras. IP cameras are pushing into 2–30-megapixel ranges, which are many times greater than standard analog video resolutions. The IP standards are in place to handle these increases as they occur; the same cannot be said for the analog standard.

- **Future-Proofing Technology:** IP systems are quickly moving to open platforms based on industry standards, which will provide greater levels of integration, longevity, and scalability. Key to this concept is the idea that no single entity (camera, software, manufacturer, integrator, etc.) can force a proprietary system outcome.
- **Scalable/Flexible:** IP-based systems offer the ability to add cameras, workstations, servers, and storage with relative ease—referred to as plug-and-play. Given available network connectivity, any of these devices can be added without requiring any additional downstream cost. Analog systems typically have single points of concentration that often require upgrades to bring on additional devices. IP-based systems also offer the ability to add devices by simply connecting the devices to the local telecommunications equipment room as opposed to having to run cable back to a central surveillance equipment room.
- **Intelligence:** IP cameras and encoders offer the ability to maximize the capabilities of security video surveillance by using video intelligence (such as motion detection and event management that allows the camera to take on some of the system thinking), thereby condensing the information shown to observers, and recording it for future use.
- **Remote Viewing/Redundancy:** IP-based systems allow video streams, live and recorded, to be viewed potentially anywhere in the world. This capability can be used at remote or mobile locations within the facility, or off airport property such as at a key staff member's home. The same ease of transmission over the network makes system redundancy a simple task.

High Resolution Cameras

As with consumer electronics, the resolution of surveillance cameras has continued to advance to the point that high-resolution cameras, those above 1080p, are becoming more commonplace and serving vital roles. In an outdoor environment, high-resolution cameras can be effectively utilized in key areas to provide high-quality coverage of airport perimeters. Cost is a factor, but high-resolution cameras can potentially replace lower-resolution versions at a 1:2 ratio or better (1 higher-resolution camera in place of 2 or more lower-resolution cameras).

4K/ultra-high-definition (UHD) cameras represent a 4-fold increase of resolution when compared to standard 1080p-resolution cameras. In areas where high pixel density is necessary or where large areas need to be covered, this increase in resolution can have a significant impact.

However, these high-resolution cameras create substantial confusion for end users, in that more is not always better. Lens quality, lowlight sensitivity, frame rates at maximum resolution, and storage capacity have become major concerns with high-resolution cameras. Camera specifications should be based on thoroughly tested resolutions that offer balanced performance and are readily available from the majority of manufacturers.

Fixed versus PTZ Cameras

The advent of megapixel fixed cameras has brought forth the idea of doing away with relatively expensive PTZ cameras in favor of high-resolution cameras with forensic zoom capabilities. However, the reality is that current market offerings of this newer technology cannot compare to PTZ flexibility and coverage capacity.

Fixed cameras offer constant coverage of specific areas. For this reason, fixed cameras should be used at entrances, exits, and areas of interest. On the other hand, PTZs offer the ability to cover general areas from a “home” position during normal operation, then automatically focus on predetermined areas during alarm events or by manual operation.

Panoramic Megapixel Cameras

Panoramic megapixel cameras are becoming a popular topic in surveillance systems, chiefly because they seem to provide an answer to a common surveillance design question, “How do you effectively cover large areas, such as parking lots?” Taking the discussion in the section above a little further, panoramic cameras offer high-resolution images spread over wide fields of view, commonly 180–360 degrees. Their high resolution is purported to make up for the PTZ’s superior optical zoom and, unlike a PTZ, they can see and record everything.

Panoramic cameras offer an enticing option, but current market solutions have critical flaws that make their use in some situations, such as parking lots, unjustifiable:

- **Frame Rate:** To handle the multiple high-resolution images that make up a panoramic image, the processors are typically limited to low numbers of frames per second (fps). Typical frame rates are in the 1 to 3 fps range compared to the recommended frame rate minimum of 15 fps.
- **Poor Nighttime Performance:** High megapixel cameras pack large quantities of pixels into chips the same size as their lower-resolution predecessors. The simple physics of this mean less light hits each pixel, thereby causing light harvesting issues in these cameras. In general, these cameras are not reliable during lowlight situations.
- **Fixed Focal Length:** Typically, these cameras have fixed focal lengths. The lenses are set to provide a wide depth of field, but the lenses are focusing 50 to 75 feet away. Objects farther away will not have critical focus.
- **Waste Area:** A camera that is covering a full 360-degree field of view will have a high percentage of unnecessary views. As compared to fixed megapixel cameras that focus on specific areas, the panoramic cameras will view and record high quantities of wasted area, including areas blocked by the mount.
- **VMS Acceptance:** The level of integration of panoramic cameras into VMS systems varies greatly between the different manufacturer offerings. The benefits of a panoramic camera may be heavily dependent on the choice of VMS, and may not be compatible.

Panoramic cameras are an attractive option, but the technology does not yet provide a full solution to large-area coverage.

Wide-Dynamic Range and Day/Night Cameras

Illumination can greatly affect the ability of a camera to provide usable video. Shadows, high contrast, and backlit scenes all make usable video difficult to capture. The use of lowlight cameras or WDR cameras is desired in situations where the available light is not consistent or adequate. With exterior surveillance, it is important to take into account that the sunlight shifts in intensity and direction throughout the course of a day. Weather conditions will also affect lighting and reflection. Snow and wet parking lots, for example, will intensify the reflected light, while rain will absorb much of the reflected light. Most black-and-white cameras have a lower lux rating than their color counterparts, but most airports desire color video when possible. To overcome this, many manufacturers have developed day/night cameras that switch to a black-and-white mode to allow for lowlight video, but will offer full color when the lighting level is adequate.

Day/night cameras are designed for exterior applications where lighting levels can vary significantly. During the day, lighting is sufficient; but after dusk, lighting levels can drop drastically. To account for these varying lighting conditions, certain manufacturers have packaged imagers and filters into a single camera so that when lighting deteriorates, the camera automatically adjusts. Sufficient lighting results in standard high-resolution color performance, whereas lower lighting results in monochrome imaging or IR filtering. It should be noted that night use provides lower performance than day.

Infrared Cameras

IR cameras refer to specially designed imagers that can see into the low IR light bandwidth; sometimes they are referred to as starlight cameras because of their nighttime viewing capabilities. These cameras should not be confused with using IR lamps to brighten scenes for both IR and traditional cameras. The use of IR lighting may incur long-term service and maintenance costs.

IR illumination as part of a camera solution allows cameras to provide full and accurate video information in lowlight situations. The active IR illuminators may be part of the actual camera or part of an additional device that is added to the camera enclosure. The advantage of IR cameras is that they provide improved penetration of fog, smoke, and haze, which results in better video and ability to detect and track possible targets. In addition, the area of illumination is not in the visible light spectrum, so intruders may not realize they are visible. However, the IR illuminators have a limited range, so this is not suitable for use in long-range applications that typically occur on a PIDS-type system. Also, these types of cameras do not work as well during inclement weather, limiting their use to specific applications.

Thermal Cameras

Simply put, thermal cameras see heat, not light, regardless of how bright or dark the scene appears to the human eye. Although identification of colors and detail (such as license plates) is impossible with thermal cameras because they view temperature only, these cameras are especially useful in viewing dark scenes for objects that have heat signatures. Thermal camera technology can cost anywhere from 7 to 12 times that of traditional cameras, while the previously cited IR and day/night technologies have a much lower premium.

Because thermal cameras see emitted thermal energy instead of reflected light, they can be used in any lighting condition, including absolute darkness. Cameras of this nature can be used to perform detection-level activities over long distances, but are limited in their ability to provide any level of recognition or identification because of the type of video image provided. Typically, for identification or recognition-

level performance, a thermal camera would be paired with a PTZ assessment camera to provide additional situational awareness during an event.

Similar to IR cameras, thermal cameras provide an invisible detection field. These types of cameras tend to be low resolution, cannot see through windows or glass like traditional CCTV cameras, tend to have a shorter life expectancy, and have a higher initial cost per camera. However, they can be used effectively for detection, and can save significant energy costs because they do not require lighting. Also, these devices work well in conditions that are difficult for visible light cameras or IR cameras, such as fog, rain, low or no light conditions, etc.

Additional camera information can be found in the Appendix A: Supplemental Camera Technical Information at the end of this document.

VIDEO SURVEILLANCE SYSTEMS

The VSS can be an important tool to monitor airport perimeters to deter and detect intruders, and support fast, effective response during a security incident. The VSS can be configured to ensure continuous monitoring and to allow security personnel to quickly view areas, assess situations, and respond promptly and with an appropriate level of force to observed problems or nonstandard situations. With respect to security alarms and monitoring, the VSS has the following components and functions:

- A digital video camera system, which collects video information to provide remote users with detailed images of scenes for monitoring and positive situational assessment
- Underlying infrastructure for communications, video transmission, and power
- Video analytics software to analyze video information by scanning video images for particular behaviors to detect a variety of unauthorized actions
- Displays for viewing video information in the central control center on individual operator consoles, on the central control center video wall, and at remote locations
- A VMS to record, archive, and play back video

Through these functions, video from any camera in the system can be reviewed to ascertain vital information about an event such as who, what, where, and when. The VSS can provide security coverage with a minimal amount of staff or security personnel.

Coupled with video analytics software, the VSS can enable cameras to analyze video images to detect particular behaviors such as intruding into non-public areas, leaving objects behind, and stopping a vehicle or loitering. Video analytics software can be set to create an alarm condition based on an established behavior or activity. Also, when properly interfaced, an alarm input from any type of sensor can trigger cameras and initiate recording of the event. Upon alarm activation, recording begins, and the video image of the alarm scene is directed to the central control center monitoring stations. This feature supports quick and direct response by security personnel by allowing them to quickly view the scene, assess the situation, and respond accordingly.

Site lighting should be coordinated with the VSS to ensure that adequate lighting has been provided, particularly in critical surveillance areas, to improve the quality of images received at night.

2.3.2.3 Command-and-Control Technologies

The command-and-control technologies are addressed in Section 2.4.2 Monitoring Perimeter Security Systems.

2.4 Perimeter Security Systems – Operations and Processes

2.4.1 Perimeter Patrols

Airports are required by the TSA to “prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within” the designated restricted areas of the airport (TSR § 1542.201 and 203). The perimeters of airports are miles long and cross all types of geography, so implementing a comprehensive perimeter patrol program is important. As with all things security, a layered approach will increase its effectiveness. Airports should consider the following factors when developing a comprehensive security perimeter patrol program:

- **Who:** The staff used to conduct perimeter patrols will vary by airport size and organizational structure, but usually includes staff from airport law enforcement, operations, security, contract security, wildlife management, and maintenance. The entity primarily responsible for patrols should document these patrols. The other entities who are on the airfield and frequently drive around the perimeter should also have secondary responsibility for observing the fence line and reporting problems with its integrity.
- **When:** Written protocols should be created that dictate the frequency and thoroughness of perimeter patrols and which entity is responsible for each. Patrols should be completed several times a day in high-traffic and high-threat areas, preferably at random times. Patrols also should be directed after power surges or failures and storms, as retractable vehicle gates can be especially vulnerable after these events.
- **How:** The accessibility of a perimeter fence will often dictate how the patrols are conducted. Patrols can be performed while in a vehicle, on foot, or more recently, by drone. If drones are considered for perimeter patrols, additional research should be conducted on regulatory requirements (14 CFR § 107) before implementation. While vehicle patrols are efficient and can provide one layer of the security program, it is strongly recommended that a patrol walk the perimeter fence line periodically to be more thorough, especially for those fences on unpaved surfaces. Often, wildlife burrow under fences and can be hard to detect when the fence is surrounded by vegetation.
- **What:** To avoid a breach in the perimeter, equipment and climbable structures should be a minimum of 5 feet away from the fence, and vegetation should be regularly landscaped. While conducting patrols, personnel should look for items that could be used to help a potential intruder get over or under the fence, and ensure that anything found is mitigated or removed.

From a competency standpoint, whether airport or contract security employees are used, the airport can and should set standards for their security officers. Officers should have the following individual capabilities:

- Understand airport security rules and applicable portions of the airport security plan
- Understand the purpose and authority of the security guard function at the airport
- Monitor and assess security situations
- Know how to respond appropriately, seek guidance and assistance when needed, and know how to verbally de-escalate a situation
- Comply with organizational requirements and sound safety practices
- Be capable of using all issued equipment

- Maintain security and safety equipment and protective devices in sound operating order
- Understand and follow all security operating procedures
- Be capable of summoning assistance and issuing instructions in emergency situations

Officer training is an intrinsic part of attaining and maintaining these capabilities. Any standards set for officer responsibilities should be defined along with the training and rate of refresher training needed to maintain the standards.

2.4.2 Monitoring Perimeter Security Systems

PIDS technologies should provide personnel with situational awareness of the perimeter incident and the information necessary to effectively and safely respond and recover from an incident. If an airport is considering developing an airport operations center (AOC), the following types of systems could be useful for monitoring perimeter security systems.

CONTROL CENTER VIDEO WALL

To support alarm assessment, it is useful to have audiovisual systems within the central control center to display content from computers that run applications to manage various security technology systems. While this may only be feasible for larger airports, it can significantly improve situational awareness and complement other AOC systems. Typical applications include displaying security feeds and building system(s) status, managing alerts or trouble notifications, and managing the operation of the IP network. Display is achieved by transmitting computer video information to various control stations or to a large central display (video wall) at the front of the room. Additionally, audiovisual systems could include a conference/situation room equipped with local presentation systems, access to information displayed within the operations center, and audio/video teleconferencing capabilities.

Based on the number of central control center operators and use of the facility, multiple large (55-inch) flat panel video displays are recommended in addition to smaller displays for general use and information sources (cable news, local news, etc.) The purpose of these displays is to provide systems monitoring, alarm assessment, and situational awareness during emergency operations for control center personnel. Video inputs to the video wall can be managed and controlled through a video matrix router. Software is available to manipulate video displays as desired by end users within the central control center.

PHYSICAL SECURITY INFORMATION MANAGEMENT SYSTEM (PSIM)

Physical security information management (PSIM) system software allows integration of a number of separate systems under one user interface platform. Its purpose is to provide a single common operating display that shows all pertinent information from multiple security technologies on a single dashboard, instead of individual system displays. The PSIM dashboard can sit above these systems as the software prioritizes incoming alarms based on approved business rules programmed into the PSIM.

The PSIM can provide a single interface to central control center operators by integrating disparate security systems. It can capture and correlate information from a variety of security sensors, cameras, and subsystems into a cohesive interface for situational awareness. The system can correlate and analyze input data quickly and efficiently to identify, assess, and respond to situations in real time, enabling central control center operators to investigate events and incidents. The system can automatically provide the central control center operators with predefined procedures and response plans (workflows) for a variety of incidents and events, which will assist them in emergency response. In addition, the PSIM can provide central control center operators with a reporting tool to generate investigative and

operational reports. The PSIM application can integrate with and support detection, assessment, and other systems as described in this document.

In addition to system integration, the PSIM can provide situation awareness, situation management, and situation reconstruction:

- Situation awareness is knowing what is going on within and around the tactical area of responsibility. When a system generates an alarm, the PSIM sends that information quickly to the forefront, prioritized above other information that is less important. The PSIM can provide the operator with a constant flow of current information throughout an incident.
- Situation management refers to what is done once it is known that a problem or incident has arisen. The PSIM allows for the automated display of standard operating procedures and responses to an event. In other words, if X happens, then the system will do Y, and the operator should do Z. Displaying standard operating procedures and responses ensures consistency in emergency protocol, regardless of the level of experience or competence of an operator. The PSIM's features can ensure that each central control center operator is kept in sync with the same and right amount of information.
- Situation reconstruction means reviewing the incident after the fact. For example, an unauthorized entry is attempted at a remote location along the airport perimeter and airport management requests a full report. The report can be generated through the PSIM, including the date, time, and synopsis of the incident, the call for security assistance, when security personnel arrived on the scene, actions taken in response to the incident, and incident closeout. If audio and video recordings of the incident are available, they would be included in the report in addition to any available recording of emergency communications. Any importable videos taken by employees can also be added to the report. When reconstructing an incident to discover what happened and assess what went wrong, what was done well, and where there were struggles, all of the information from all systems involved should be collected. The PSIM is capable of compiling all situational data.

It should be noted that careful consideration should be taken when procuring, configuring, and implementing a PSIM, as it is not always best to integrate everything. It is important to understand what an airport wants the PSIM to do and how it will be used. It is recommended that airports develop a ConOps for their PSIM to identify its use, limitations, and operational requirements; this information will be used to configure the system to work in the fashion that is defined by the airport.

EMERGENCY COMMUNICATIONS SYSTEM/MASS NOTIFICATION SYSTEM

Emergency communications systems/mass notification systems (ECS/MNS) provide critical communication resources to support alarm validation, emergency response, and situational awareness. ECS/MNS functions may include the following:

- Coordinate notification of emergency conditions
- Coordinate receipt and verification of emergency conditions
- Coordinate appropriate notification processes based on incident type
- Coordinate notification of necessary personnel based on incident type
- Coordinate notification of first responders
- Provide notification of necessary personnel based on the nature and severity of the emergency

The primary function of the ECS/MNS is to coordinate emergency communications manually and automatically through a human interface when information is received that identifies a threat or an emergency requiring occupant notification. In many cases, the ECS/MNS is composed of one-way and two-way emergency communication components to convey emergency information throughout an airport. The one-way ECS typically broadcasts emergency information to people in one or more specified indoor or outdoor areas, and is conveyed by audible, visible, and/or textual means via systems such as Emergency Voice/Alarm Communications System, Mass Notification System, Open Air Public Address System, Distributed Recipient Mass Notification System, and Two-Way Emergency Communication System.

Responding to potential perimeter intrusions in a timely manner and in the proper location increases the probability of effective response and mitigation of security threats. Interoperable communications play an important role in response and tactical communications. The US DHS provides guidance on interoperability in the National Emergency Communications Plan.

2.4.3 Security Processes and Initiatives

An operational security plan (OSP) to support perimeter security response should provide a framework of protocols for day-to-day monitoring of the perimeter, response type, and total incident time. This information may also be included in the airport security plan (ASP). Recommended OSP objectives may include the following:

- Identify, deter, detect, disrupt, and prepare for perimeter security threats (among other hazards and threats)
- Reduce perimeter security vulnerabilities (as well as other critical assets, systems, and networks)
- Provide tactics, training, and resources to mitigate or manage the potential consequences of security incidents (as well as other emergencies that may occur) in conjunction with an Airport Emergency Plan (AEP)

The OSP should provide perimeter security guidance for the airport in the following activities:

- Assess and analyze threats, vulnerabilities, and consequences related to perimeter security intrusions to inform risk-management/mitigation activities
- Secure infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk
- Enhance resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective response protocols
- Share actionable and relevant information with appropriate stakeholders to build awareness and enable risk-informed decision-making

The OSP should assist in prioritizing perimeter security activities based on the criticality of affected infrastructure, costs of activities, and potential for risk reduction. Some risk-management activities address multiple aspects of risk while others are more targeted to addressing specific threats, vulnerabilities, or consequences. Activities can be divided into the following recommended approaches:

- Identify, deter, detect, disrupt, and prepare for threats and hazards
- Reduce vulnerabilities through proactive mitigation
- Build security and resilience into the design and operation of assets, systems, and networks

- Develop and conduct training and exercise programs to enhance awareness and understanding of common vulnerabilities and possible mitigation strategies
- Leverage lessons learned and apply corrective actions from incidents and exercises to enhance protective measures
- Establish and execute emergency operations and continuity plans to facilitate continued performance of critical functions during emergencies
- Address cyber vulnerabilities through continuous diagnostics and prioritization of high-risk vulnerabilities
- Rapidly identify, assess, and respond to cascading effects during incidents
- Manage and mitigate consequences

Activities listed above are examples of *risk mitigation* activities undertaken to achieve airport security and resilience. Prevention activities are most closely associated with *efforts to address threats*; protection efforts generally address *vulnerabilities*; and response and recovery efforts help minimize *consequences*. Mitigation efforts transcend the entire threat, vulnerability, and consequence spectrum. Five mission areas including prevention, protection, mitigation, response, and recovery provide a useful framework for considering risk management investments.

2.4.3.1 Situational Awareness

Development and maintenance of capabilities to prevent or respond to an incident require access to comprehensive information and data from multiple diverse systems to allow credible situational awareness. Core systems that can support situational awareness include access control systems, video surveillance systems, PIDS, and other related processes, including personnel observations. These data sources may include multiple sensor outputs, information correlation and fusion, and emergency plans, as well as geographic data/imagery, and dynamic data such as incidents, threats, and weather. To avoid information overload, data sources should be prioritized via the PSIM based on response requirements. Real-time data from these systems and sensors can provide significant insight to heighten situational awareness and to support security response. The OSP may contain response procedures for the security analyst or monitor to direct collection, analysis, and use of situational awareness data points.

Situational awareness allows the security analyst to know what is happening, where it is happening, when it is happening, and other ancillary information to help fully understand day-to-day operations or operations during an incident. It is an analytical process that can be enhanced using technology to access, analyze, and present information to have a greater understanding of existing conditions and how they will change over time. Having comprehensive information relevant to the specific location of an incident and related surrounding areas, as well as the locations of public safety resources and personnel, is an example of how dynamic and spatial data are combined to create situational awareness.

Situational awareness is defined as:

- Knowing and understanding an ongoing emergency or critical event that is occurring, through multiple sensors and systems integration
- Having an established response protocol to mitigate the potential effects of the event
- Adapting to how it will change over time

These are important concepts for understanding which technology is required to achieve desired results. Situational awareness and its dynamic nature require the availability of sensor outputs, rules-generated processing of sensor output, correlation and fusion of information, and informed response to the event. Having the ability to understand the severity of the circumstances in advance of or during an emergency can make a significant difference to how the response is executed.

2.4.3.2 Transition to Emergency Operations

The transition from OSP procedures to emergency operations should generally proceed as indicated below:

- The OSP is activated at the onset of an alarm indicating a breach of perimeter security
- OSP protocols and procedures continue as necessary
- If the incident escalates, additional security support is summoned, and an incident commander is activated
- The incident commander begins transition to emergency operations, including summoning additional staff (command and general staff under the incident command system) and resources and establishing multi-agency communications, as needed
- Protocols and procedures for the specific threats are initiated upon direction from the incident commander

2.4.3.3 Emergency Operations

All commercial service airports are required to have and exercise an AEP by Federal Aviation Regulation § 139.325. Response procedures, which are documented within the AEP, allow airport stakeholders to better integrate with other local, state, and federal agencies during multi-jurisdictional response. Homeland Security Presidential Directive 5 requires adoption of National Incident Management System (NIMS) by state and local organizations as a condition for federal assistance in preparedness, response, and recovery, and use of NIMS during incident management and emergency prevention, preparedness, response, recovery, and mitigation activities. While airports are not required to adopt NIMS, it is recommended that they become familiar with the system because it provides a consistent nationwide template for federal, state, local, and tribal governments, and private-sector and non-governmental organizations to work effectively and efficiently together. NIMS offers guidance on how best to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

SECTION 3. IMPLEMENTING PERIMETER INTRUSION DETECTION SYSTEMS

Airport perimeter security systems can range from simple fences to complex systems that reflect an airport's requirements and budget. In each instance, the airport must evaluate its need—as dictated by risk—and weigh that against its available budget. This section is focused on providing guidance to any airport that is considering implementing perimeter technology in a PIDS.

3.1 PIDS Project Management

Project management has evolved for the purpose of planning, coordinating, and controlling complex and diverse activities of modern security projects (Patterson 2004). It is through competent project management that effective and successful design and implementation of PIDS will be achieved. While many airports already have processes in place for project management, the intent of this section is to provide guidelines for best practices of project management.

3.1.1 Organization of a Project Team

The project management team should be determined early in the process by project stakeholders. Stakeholders include any personnel within the organization, or directly associated with the organization, with a direct interest (financial, operational, regulatory, and potential end users) in the project outcome.

3.1.1.1 Project Sponsor

The project sponsor is the primary financial controller for the PIDS and perimeter security enhancement efforts. In most cases, the project sponsor will be the airport owner, which may be a city government or governmental authority.

3.1.1.2 Project Manager

To ensure successful project completion, the sponsoring organization (financial stakeholder) should appoint an experienced and capable project manager (PM). The PM should have demonstrated qualifications, including management of complex security systems projects of similar size and scope. From an internal employee standpoint, it may be difficult to identify an individual with requisite project experience. Among other reasons, the PIDS project is likely to be the largest effort, from a security standpoint, that the airport has undertaken. In the case of internal personnel, the project stakeholders should select an individual who is knowledgeable of the current and desired state of the security systems, well organized, and analytical.

The selection of the right PIDS PM is a critical choice, as the PM will be responsible for managing the day-to-day activities including leading meetings, establishing and imposing scheduling deadlines, and monitoring the financial aspects of the project.

3.1.1.3 Project Stakeholders

To support airport perimeter security and the general security mission, formal procedures for stakeholder engagement and cooperation are recommended. A formalized stakeholder engagement plan identifies recommended procedures for governance and cooperation among airport management and relevant stakeholders to support advancing the security mission.

To provide structure to the governance and cooperation process, a PIDS working group (PWG) is recommended. This group will support effective implementation, maintenance, and review of security and emergency response initiatives, and provide airport management with a formalized process to interact with stakeholders in support of security initiatives. The PWG may also provide a forum to discuss development and modifications of security-related agreements, as well as resource needs and procedural changes that may be required over time. If the airport already has a recurring meeting for key airport security stakeholders, it may consider forming a subcommittee to address the PIDS project. This section provides recommendations about membership, roles, and responsibilities of a PWG. Airports can take the framework outlined below and adapt it to their unique organizational structure to make it work for them.

PIDS WORKING GROUP

Through the PWG, airport management should bring together stakeholders to assign roles and responsibilities for implementation, maintenance, and review of security-related matters. As a formal, ongoing initiative to support the airport safety, security, and emergency response initiatives, the PWG should be led by an assigned airport management official. A framework for the PWG, which outlines the PWG's recommended roles and responsibilities, is identified in the following sections.

Committee Framework

The assigned airport PM will lead and approve all activities and actions taken by the PWG. While stakeholders should be organized in a manner that aligns with airport needs, the model provided herein divides stakeholders among three tiers based on their roles in supporting implementation and ongoing management and maintenance of security initiatives. A representative list of potential stakeholders is identified below; actual stakeholder entities should be customized based on the operations of the airport, among other considerations:

- Tier 1 – Stakeholder Response and Regulatory Agencies (Airport Law Enforcement, TSA)
- Tier 2 – Airport/Airfield Operations (Airport Operations, Airlines, FAA, and selected Airfield Operational Tenants)
- Tier 3 – Retail Tenants and Non-Airline/Airfield Tenants

Advisory subcommittees to the PWG are recommended for Tier 1 and Tier 2 to support tier- and function-specific needs. A subcommittee is not recommended for Tier 3. Security needs for retail and other non-airfield related tenant activities should be coordinated through lease agreements or other contractual means. Based on a review of best practices, recommended PWG activities³ include:

- Governance Activities:
 - Evaluate and maintain the PWG governance structure
 - Assign roles and responsibilities and lines of reporting within the PWG
 - Review and comment on the airport's asset inventory, asset maps, and technology descriptions, as needed
 - Confirm security responsibilities and segregation of duties
 - Review and comment on compliance requirements and maintain compliance
 - Review and comment on data flows based on operational and response needs

³The activities list was adapted from *Governing for Enterprise Security Implementation Guide*, Julia H. Allen Jody R. Westby, Carnegie Mellon University, 2007.

- Participate in threat, vulnerability, and risk assessments
- Identify operational criteria
- Provide review comments and assist in maintaining safety, security, and emergency preparedness policies
- Participate in formal audits to support capital planning, including the security business case, benefit/cost analysis, and return on investment for proposed security capital budget expenditures
- Operations Activities:
 - Implement and maintain security-related controls
 - Support security training
 - Implement and maintain the security procedures and emergency plans
 - Implement and maintain security-related stakeholder and vendor requirements
 - Review and comment on proposals to update security system architecture
- Evaluation Activities:
 - Implement and maintain key security-related performance indicators and metrics
 - Review and comment on assessment of asset-specific security configurations
 - Implement and maintain training and exercise plans
 - Support the conduct of tests and exercises and use the test results to evaluate plans and procedures, vendors, and security systems
 - Support review of incidents to identify any beneficial modifications to processes, policies, procedures, or resources
 - Support monitoring and enforcement of security-related policies, procedures, and plans
 - Support development and implementation of improvements to security-related processes and procedures

3.2 Developing a Business Case for PIDS

The primary measure of a successful airport perimeter security program is the degree to which it meets its intended purpose and stakeholders needs. The first question to be answered is, “Why should we undertake this project?”

It is often the responsibility of the PIDS PM to develop or manage the development of a business case, and the intent of the business case is to provide senior management enough information to make informed decisions. As a minimum, the business case should address these basic elements:

- Why: Defining the problem statement to justify the project
- What: Considering potential options, alternative solutions, benefits, costs, risks, and opportunities
- When: Establishing a desired timeline or duration
- Value: Identifying the benefits to be realized from the program

The goal of an airport perimeter security business case is to evaluate the current environment, identify and document performance gaps and opportunities, and document suggestions for improvements that can be adopted on both a short-term and long-term basis. Lessons learned and best practices should all work in concert to craft recommendations.

Airport officials typically cite cost and staffing as limitations to achieving PIDS effectiveness. The cost of installation, ongoing operation/maintenance, and managing technology updates and migrations for legacy solutions are common challenges. Conducting a business case reduces inherent risks for complex projects that must incorporate people, processes, and technology. Similarly, focusing on ROI increases the probability that stakeholders' needs are met by identifying the cost benefit before executing a solution.

A needs assessment can address the following topics and can be used as the foundation for a business case.

- Security Needs/Evaluation
- Options/Alternatives
- Priorities/Phasing
- Preferred Alternative(s)
- Proposed Cost
- Recommendations

3.2.1 Conduct a Needs Assessment

The business case identifies the problem to be solved, how to achieve the desired result, and the deliverable to convey the findings. A key component is conducting a needs assessment to capture the current state, desired future state, and identify the differences that exist between the two.

To enhance the security posture, airports should begin by identifying stakeholder needs through interviews, a detailed physical perimeter inspection, and SME analysis of the data acquired coupled with current technology trends and aviation security industry standards, guidelines, and best practices. Refer to Section 3.1.1.3 Project Stakeholders for the recommended tiers of participation.

The purpose of a needs assessment is to evaluate the current security environment, identify and document performance gaps and opportunities, and develop recommendations where improvements can be adopted and the preferred sequence for doing so. The following are suggested steps in a needs assessment process:

Step 1: Stakeholder Interviews/Workshops

Interviews and workshops are preferred methods for gathering information. Both activities consist of eliciting opinions and attitudes to gain basic information. Objectives to achieve in either forum include:

- Describing current security practices
- Describing existing systems and system operations
- Identifying existing regulatory requirements
- Identifying industry trends or lessons learned
- Identifying potential new systems requirements
- Identifying significant assumptions and constraints
- Identifying overall information technology requirements

Successful information-gathering techniques:

- Determine basic domain knowledge before engagement so that time is used effectively
- Provide an agenda ahead of the scheduled session (whether an interview or workshop)
- Enumerate all user activities with general and specific follow-up questions
- Confirm how user activities are performed
- Trace interconnections with other users
- Uncover issues that determine and affect performance of user tasks
- Follow up on exceptions, the unusual activities that are unlikely to occur during observation

Step 2: Physical Perimeter Inspection

Conduct a perimeter inspection with appropriate law enforcement, security, and operations personnel, supplemented by facilities, planning, engineering/construction, and maintenance staff for information-gathering requirements. Collaborate with security personnel to understand the intent of the ASP for context. Review the following site elements:

- Fencing
- Gates
- Guard Posts/Vehicle Access Points/Pedestrian Access Points
- Tenant/Cargo Facilities
- Other Perimeter Considerations: operations and perimeter patrols

Step 3: Define Options/Alternatives/Estimated Cost

A list or matrix of perimeter security options for the airport should be developed after gathering the appropriate information in Steps 1 and 2. As mentioned earlier in this guidance, the airport needs to weigh its risks (threats plus vulnerabilities) against the cost of perimeter security options.

Consultants can provide recommendations and cost estimates of various perimeter security solutions based on the specific need/environment. It is important to consider the cost of supporting infrastructure and installation as well as ongoing maintenance costs. All of these considerations need to be included in the options matrix. If desired, an analysis can be conducted to estimate an ROI—by comparing the expected benefits with the costs—for various options. It is important to note that if the airport conducts an ROI analysis, it needs to use the system lifetime cost rather than the one-time capital cost of acquiring the system.

Options can range from alternative recommendations (perhaps different technology types) for the same area to breaking the perimeter into multiple zones and weighing the importance/solution for each individual area. An example of this would be to separate the perimeter fence line into remote areas (far away from the terminal areas and protected assets), close-in areas abutting the terminals and secure areas, and cargo building areas. Different procedures and/or perimeter security measures may be appropriate for each different area. Airports can identify the areas and measures and then prioritize them based on their criteria (e.g., risk and cost).

Table 2 is a simple example of an options matrix.

Table 2. Simple Example of an Options Matrix

Option	Description – including other components	Location/ Characteristics	Need/Requirement	Estimated Capital Cost	Life Cycle Cost	ROI
Fence Option 1	Fence hardening to include bottom rail and replacement of 3-strand barbed wire	Areas near the terminal building that currently have chain link fence	Deter potential perimeter fence breaches Past breaches in location: 3	\$XXX	\$YYY	\$ZZZ
Fence Option 2	New fiber- based fence detection system plus CCTV Communications and power infrastructure Monitoring capabilities	Remote fence line (subset of full fence — should be shown on a map)	Deter, detect, and alarm on remote perimeter fence breaches Past breaches in location: 1	\$XXX	\$YYY	\$ZZZ
Fence Option 3	CCTV, communications, and power infrastructure Monitoring capabilities	Fence lines near cargo facilities that are the responsibility of the airport (not its tenants) Usually accompanied by patrols	Assess any potential breach Past Breaches in location: 2	\$XXX	\$YYY	\$ZZZ
Fence Option 4	Increased Patrols	Full perimeter	Deter and detect perimeter fence breaches Past breaches in location: 4	\$XXX	\$YYY	\$ZZZ

The need/requirement, capital cost, ROI, and life cycle cost column entries could be weighted (by importance) to help sort the options. Also, it is important to note that ongoing maintenance (life cycle) costs can be significant and are often not considered in the prioritization process.

Step 4: Priorities/Phasing/Preferred Alternatives

The airport can prioritize options by using the assigned weights to sort the options matrix. If an airport's primary constraint is budget, then the cost item would be weighed more heavily than other items.

Once the matrix is prioritized based on an airport's specific criteria (cost, risk, and ROI), the airport can use the options matrix to consider if/what project(s) should be proposed. Projects can be subdivided into phases based on constraints such as fiscal years or ongoing other projects, for instance. Phasing considerations should include the potential for dovetailing with other projects. For example, if another project is already scheduled to install conduit and pull fiber, it might be economical to install fiber for the perimeter security project at the same time, even if it will not be needed in the immediate future.

Step 5: Recommendations

The business case for perimeter security recommendations will rely heavily on the prioritized options matrix. Justification for the proposed perimeter security recommendation should include information on the risk that is being addressed, the financial and logistical aspects of the proposed project, and the expected schedule.

3.3 PIDS Implementation

Perimeter security is a difficult problem in a taxing and harsh environment. Systems must operate 24/7 and in all weather conditions. Airports are large in physical size with perimeters that run from thousands of feet to multiple miles in length, with borders of diverse characteristics. In addition, the potential for nuisance alarms is ever present from surrounding wildlife and normal activity.

3.3.1 Best Practices

Over the past few decades, airports have deployed a multitude of perimeter security technology solutions. Some have been successful, and others have not performed as anticipated. Based on these experiences, airports and industry have acquired knowledge of effective practices in implementing PIDS. These best practices range from procurement strategies to technical implementation issues, and are discussed below.

- Be cognizant of the requirements and cost of supporting IT and communications infrastructure
- Implement business processes and procedures to complement the PIDS
- Develop intelligent integration of layered PIDS technologies
- Design PIDS to support an open architecture
- Incorporate legacy systems into PIDS

IT AND COMMUNICATIONS INFRASTRUCTURE

When planning, procuring, and implementing a PIDS, it is important that the airport be aware of the IT and communications infrastructure needed to support the PIDS technology solution. If that infrastructure is not in place before the PIDS installation, it will need to be planned, designed, and implemented as part of the PIDS project. If sensors are going to be located along the perimeter, infrastructure will need to be available to provide communications and power to/from those locations and to/from system head-ends and displays. It should be noted that current camera technology supports power-over-Ethernet (PoE), allowing for only fiber out to the perimeter locations. A best practice is to use existing infrastructure and/or minimize the need for new infrastructure wherever possible. The cost and complexity of trenching for new conduit and deploying the new infrastructure can end up being as much as, or more than, any PIDS technology. Airports can consider wireless connectivity for communications, but it is not a means for providing power to remote sensors, devices, or components.

BUSINESS PROCESSES AND PROCEDURES TO COMPLEMENT THE PIDS

The development of business processes and procedures to complement the PIDS is considered a best practice, because these facilitate the most effective security posture and use of the system. Business processes and procedures can range from the development of a full ConOps, discussed in Section 3.3.3 Developing a Concept of Operations, to developing manual procedures to report, respond to, and close out a perimeter incident.

PIDS-supporting procedures should identify how the system should be used, by whom, and specific actions to take in certain instances. It should define the relationship between the system and the airport's security personnel responsibilities. An example is SOPs that document an approved sequence of actions, responses, alarm escalation, and acknowledgment during a perimeter security incident.

DEVELOP INTELLIGENT INTEGRATION OF LAYERED PIDS TECHNOLOGIES

The integration of PIDS technologies is discussed in Section 3.3.7.1. The importance of intelligent integration is that the process can enable the discrete PIDS sensors, operating in concert, to perform in a more operationally effective way by providing more reliable alarm information. Individual sensors can produce a number of unwanted nuisance alarms. When the individual parts are intelligently integrated, the number of nuisance alarms is greatly reduced (though not eliminated), meaning that the majority of alarms generated by the PIDS are true alarms.

DESIGN PIDS TO SUPPORT AN OPEN ARCHITECTURE

Open architecture is a framework that enables individual components to be easily integrated into a PIDS because the interfaces to the components are standardized and published. Proprietary systems require customized interface development and introduce risk to the PIDS installation.

INCORPORATE LEGACY SYSTEMS INTO PIDS

Legacy systems are those systems that already are installed and used by the airport. A common example of this best practice is the design and implementation of a PIDS that incorporates existing airport CCTV cameras and/or an existing airport VMS for CCTV viewing and storage.

It is recommended that an airport perform an analysis on the incorporation of legacy systems into their PIDS. Some of the questions that should be addressed in the analysis are as follows:

- Is the legacy system near the end of its useful life?
- Can the legacy system be integrated into the PIDS either via an existing interface or with minimal development?
- Will the integration of the legacy system into the PIDS jeopardize the legacy system's warranty (if in existence) or maintenance contract conditions?
- What is the estimated cost of integrating the legacy system versus procuring a new system to work in concert with the PIDS?

Where possible, and if the analysis supports, it always makes sense to use technology systems that are currently in use. It saves money and time while allowing the airport to continue using existing procedures in place to maintain the systems.

3.3.2 Applying Systems Engineering Methodology

The availability and complexity of security technologies have grown significantly since September 11, 2001. As a result, there is a tendency to start the process of defining a PIDS by looking first at technology and working backward. This approach often results in a system that is substantially more expensive than planned, not risk appropriate, and ineffective. One of the most important lessons learned is to clearly define the problem before implementing the solution.

The primary measure of a successful security system is the degree to which it meets its intended purpose and the needs of the system's stakeholders. Systems engineering is a standardized practice and a means

to guide and enable the realization of a successful system implementation, with success measured by how well the implementation satisfies the needs of the people who will use it.

The practice of systems engineering reduces the risks inherent in complex projects, and increases the probability that the final system will meet user needs by clearly and measurably defining the system before implementing the solution.

The process starts by asking the team to define the problem they are trying to solve rather than by describing the solution. It encompasses identifying the discrete system life cycle steps, such as problem definition, ConOps, design, implementation, maintenance, and others. Systems engineering processes are described in Appendix B: Systems Engineering Methodology and Supplemental Information.

3.3.3 Developing a Concept of Operations

Melding physical security measures with technology systems, processes, policies, procedures, and personnel through a ConOps improves the efficacy of the security program and reduces risk. Moreover, the planning and design process yields a more accepted security approach and improves operational success by engaging stakeholders, including the FAA, TSA, and other concerned agencies; airport tenants; and law enforcement, emergency management agencies, and airport operations and maintenance personnel. (TransSecure, Inc. 2017).

Development of a ConOps to support any security initiative should be premised on three fundamental objectives:

1. Provide an effective organization and align stakeholder groups and/or functions to support security and response functions
2. Define operational activities and functions, and improve and enhance coordination, collaboration, management, and event response
3. Ensure that people, processes, and technology are merged and synthesized to implement an operational and systems approach to achieve timely and accurate situational awareness, incident management, and business process activities

A ConOps should serve as the foundation of the operations for a PIDS. It should describe the way the PIDS will work from the operator's perspective. It will include the user description and will summarize the needs, goals, and characteristics of the system's user community. The ConOps is a document that defines the environment in which the system is to operate, including the relationship between the system and the airport's responsibilities, the physical environment, and performance expectations. As such, it should answer the who, what, when, where, how, and why of the PIDS. The ConOps is discussed in more detail in Appendix B: Systems Engineering Methodology and Supplemental Information.

3.3.4 Develop a System Requirements Document

A system requirements document is intended to state the system's functional objectives in a narrative form to allow stakeholders to understand and have an opportunity for input at a very early point in the process. When feasible, the objectives should be specific, measurable, achievable, realistic, and time-based.

The importance of identifying and documenting requirements is that they will be used both in the design of the system and in the development of system testing. The requirements will instruct the design by specifying what the system needs to achieve. For instance, a PIDS requirement may read, "The PIDS shall display the location of an intruder detection on a map of the airport." The design process will

specify how the system will execute that function. That same requirement will then be used at the end of the PIDS implementation to develop test cases for the PIDS to ensure the system displays the location of a detected intruder on a map of the airport.

3.3.5 Design and Implementation

Design and implementation of the PIDS is based on the operational requirements as identified in the ConOps, and on the functional system requirements as defined in the system requirements document. The requirements should answer the question of *what* the PIDS needs to do, and the design should address *how* the PIDS will do it. The design will evolve through several phases. Components may include:

- Develop Basis of Design
- Design Development
 - Specifications
 - Design Drawings and Equipment List
 - Estimate
- Procurement and Contract Implementation
 - Vendor Identification and Analysis
 - Installation Monitoring
- Staffing Requirements Analysis
- Training
- Testing and Commissioning

3.3.6 PIDS Components

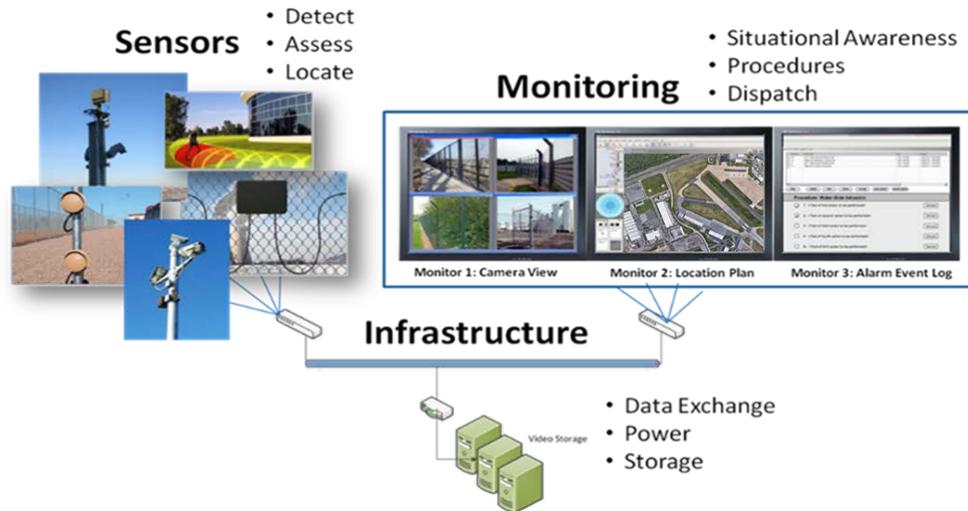
A PIDS is composed of three basic functional components: sensors, monitoring command and control, and supporting infrastructure. The sensors usually are placed at the perimeter (though there are some exceptions) and are responsible for providing detection, location, and assessment information to the PIDS. PIDS sensor technologies, their uses, and implementation considerations are addressed in Section 2.3 Perimeter Security Systems – Electronic Measures.

The PIDS infrastructure consists of power and communications, but also may include the system head-end servers that provide processing and storage. Alternate PIDS infrastructure options, such as wireless and solar technologies are discussed below.

Lastly, the PIDS includes a monitoring capability that can provide situational awareness to security personnel through video display, mapping, alarming, contextually appropriate procedures, and dispatch communications. PIDS monitoring is discussed in Section 2.4.2 Monitoring Perimeter Security Systems.

Figure 24 depicts a representation of each of the basic PIDS components.

Figure 24. Basic PIDS Components



A PIDS does not require a full array of constituent parts for each component—it should be scalable to fit the airport’s unique needs. However, it should include at least one item in each of the sensor, monitoring, and infrastructure categories to be an effective electronic perimeter security system. For instance, not all airports need multiple sensor systems integrated together and displayed on a complex display. An airport may only require CCTV cameras (sensors) interfaced to a video display (monitoring) and a fiber network to provide support to all components and connect them to a VMS for video storage (infrastructure).

Conventional infrastructure can be a costly component of a PIDS. In some cases, alternate methods such as wireless and solar technologies may be appropriate; wireless and solar technologies should be considered when wired infrastructure is not available. Wireless point-to-point communications technologies are widely available and can be implemented with encryption to allow for safe, secure communications. It should be noted that the location of the send/receive antenna needs to be carefully considered to avoid interference or obstruction, as the airfield is a dynamic environment. Wireless communications work well in most environments. They often rely on several communications frequencies to minimize interference, both electrical and weather-related. Most systems are rated to work in a broad temperature range (-40°C to $+60^{\circ}\text{C}$), are resistant to salt corrosion and dust, and are highly reliable.

The use of solar power to wirelessly power security technologies is somewhat limited in that most solar technologies are tightly coupled with specific sensors. Other solar sources (large solar arrays at airports) still require the use of cabling to provide wired power to remote sensors. Therefore, the focus of this discussion is the use of solar power to negate the need for wired infrastructure.

The most common solar-powered security sensors are CCTV cameras. These cameras are IP-based and available in different resolutions, including high-definition (HD 1080p). The amount of power generated and available for operation of the camera is dependent on the size of the solar panel used to collect sunlight, the amount of sunlight, and the size/capacity accompanying rechargeable batteries. One of the clearest benefits of solar-powered cameras is flexible installation locations. The accompanying solar arrays should be mounted relatively nearby and oriented toward the maximum sunlight angle. The panels are sensitive enough to generate power on cloudy days but require the stored battery power for nighttime or rainy-day operation. While these systems are reliable, it is recommended that they not be

used in areas that regularly have sustained periods of rain or are in critical areas requiring 24/7/365 CCTV coverage.

The design of an electronic PIDS and selection of its sensor components needs to consider the deployment environment of the system. Where possible, the PIDS should combine both CPTED and electronic components. Sensor selection should include consideration of performance along with the installation location, terrain, and operating conditions. For instance, sensors that require point-to-point communication (e.g., microwave, laser, or IR beam) should not be installed in hilly environments. If fences will be used for sensor mounting, the fence needs to be in good condition (i.e., chain link should be taut and anchored at the top and the bottom of the fence) and well maintained. Sensors that have temperature sensitivity should not be used in extreme hot or cold environments. The systems engineering methodology discussed in Section 3.3.2 should help in studying the full spectrum of considerations when designing a PIDS.

3.3.7 PIDS Performance Metrics

There are three primary performance metrics associated with PIDS: probability of detection, false alarm rate (or probability of false alarm), and nuisance alarm rate. These metrics are defined as follows:

Probability of Detection (P_D) is the likelihood, expressed as a percentage, that the system will **correctly detect a security violation** as detailed in the PIDS requirements. P_D provides an indication of sensor performance in detecting the presence of an object (or target) within a zone covered by the sensor. P_D involves not only the characteristics of the sensor, but also the environment, method of installation and adjustment (calibration/threshold), and assumed behavior of an intruder.

False Alarm Rate (FAR) indicates the expected rate of occurrence of alarms that are not attributable to intrusion activity (actual sensor detections of personnel, conveyances, or nuisances). These alarms may be generated by the system itself as a **result of electrical noise**.

Nuisance Alarm Rate (NAR) is an alarm event expressed as a percentage of actual sensor detections that occur as a result of an external source that simulates intrusion by personnel, conveyances, **animals**, etc. These can be caused by natural phenomena such as precipitation, wind, vegetation, etc.

PIDS PERFORMANCE GOAL: HIGH P_D WITH A LOW NAR

A major goal of an integrated PIDS is to provide a low NAR and FAR and a high P_D .

The measures of P_D and NAR are affected by the sensitivity setting (or detection threshold) of the sensors, so they must be considered in tandem rather than individually. As an illustration, a system may achieve a very high P_D ($0.99 = 99\%$ chance of detecting an intruder) by setting the detection threshold so low that it detects absolutely everything in the environment (wind-blown debris, rain, poorly installed signage), none of which are true intrusions. That detection threshold will almost guarantee detection of the intruder, but will also detect everything else. On the other hand, a system can appear to have a very low nuisance alarm rate by setting the detection threshold so high that the system will not detect any nuisance alarms—nor will it detect an intruder.

The proper design/calibration and measurement technique is in balancing the P_D and NAR requirements through optimization of the sensitivity threshold so that the system is sensitive enough to detect intrusions but insensitive to nuisances such as environmental conditions. In addition, PIDS P_D and NAR can be improved through intelligent PIDS integration.

3.3.7.1 PIDS Integration

PIDS technology should be composed of the proper selection of sensors and systems, installation of supporting infrastructure (communications and power), and the careful integration of the disparate subsystems into a holistic system. A PIDS will only be as good as the knowledge (actionable intelligence) it provides to the end user and the applicability of the SOPs to couple the knowledge with clear and directed actions. True security knowledge is achieved through the full implementation of the three layers of systems integration:

- Physical integration – the actual physical connection of disparate components.
- Logical integration – the connection of systems through common communication protocols and interface formats. This layer focuses on allowing systems “to talk to one another” and is often where integration ends.
- Knowledge integration – structuring of the data provided via logical integration into context-specific situational awareness knowledge for the end user. This layer of integration involves the correlation of security information (sensor data, events, and incidents) as well as procedural information to provide security end users with the knowledge they need to be proactive, react to, and/or interface with third parties to mitigate threats and incidents. The value of knowledge integration is realized when systems are brought together into a common operating picture that will allow for true situational awareness in a single view.

Integration of complementary technologies will result in better PIDS performance. Systems can be designed so that each technology serves as a subsystem that provides input to a fully integrated PIDS. That means individual subsystems can generate individual alerts that do not become system alarms unless a second subsystem verifies the alert. In other words, if two (or more) of the sensor subsystems report the same incident (an intrusion at the same location at the same time), the PIDS will declare an intruder alarm. For example, trash caught on a fence and blowing in the wind may cause a fence-mounted sensor subsystem to alert, but if the PIDS integrates that system with a video analytics system that does not report the trash on the fence as an alert, the PIDS will not declare an alarm.

3.3.8 Testing and Commissioning of Systems

There are two primary types of PIDS testing that airports should be familiar with: functional system testing and system acceptance testing.

Functional system testing evaluates the PIDS against the system requirements as defined in the requirements document. A test plan is developed to describe the PIDS test methodology, approach, testing sequence, and specific tests to be conducted to verify the successful performance of the PIDS. The test procedures should be designed to verify the attributes, performance, and functional requirements of the system as identified in the PIDS requirements document. The testing should be rigorous (all requirements tested) and should be performed under different weather conditions and at different times of the day. Each test should be performed multiple times to determine statistical data trends, and all functional tests must be successfully completed for the PIDS test to succeed.

System acceptance testing should consist of the PIDS operating for a pre-determined period of time to observe the system’s performance over time (often 30 or 60 days). If the PIDS fails during the predetermined time period, the failure must be documented and corrected, and the test must start anew for the full period of time.

3.3.9 Staffing Requirements Analysis

Each airport has its unique staffing assignments and responsibilities. However, personnel play a key role in the detection, assessment, communications, and response elements of the PIDS. Since PIDS monitoring most likely will be performed by staff with other responsibilities, one of the decisions airport management has to make when installing a PIDS is where the system will be monitored. Larger airports may already have a staffed communications or operations center that dispatches first responders, monitors access control and fire alarm systems, and responds to customer service and maintenance calls. But smaller airports may have to rely on the on-duty operations manager, who will likely be roaming the airport and not be in a fixed location most of the time. Airport staff will have to decide if the workload added by a PIDS is enough to justify adding staff.

Improvements in technology integration, automation, and artificial intelligence (AI) are expected to reduce human interface and staff monitoring time. Despite advancements in these technological solutions, human analysis currently provides the greatest opportunity for effective target identification and assessment. As a result, one of the primary responsibilities of PIDS operators is to perform assessment of reported alarms.

Operator staffing should be established to be commensurate with the operational requirements of the PIDS. Airports should consider all the systems these operators are expected to monitor and make an assessment whether additional staffing is needed. Management needs to consider the critical role operators play in overall PIDS effectiveness to determine their respective workloads prior to assigning additional tasks and responsibilities to them. The topic of personnel/staffing also is addressed in the survey of stakeholders conducted as part of this research program.

3.3.9.1 Personnel Training and Exercises

Successful and effective PIDS depend on the proficiency of individuals who use the system. It is imperative that individuals responsible for operation, administration/management, and maintenance of a PIDS and other perimeter physical security measures are equipped with the proper training. Personnel who operate, maintain, and administer the system should receive training in their respective disciplines initially and on a recurring basis. The airport needs to determine the most effective frequency of training, but at a minimum, it is recommended that recurrent training take place at least annually. Recurrent training will help personnel maintain proficiency while also allowing for instruction on new features and functions resulting from system upgrades.

As part of daily airport operations, security management and/or associated stakeholders should conduct ongoing exercises with operators to build and maintain competencies around the use of and response to the PIDS and PIDS alarms. Simple, realistic, operational drills should be conducted to maintain these competencies, identify gaps, and provide a lessons-learned approach to security management. DHS provides valuable guidance in developing and conducting exercises through the Homeland Security Exercise and Evaluation Program.

In addition, many airports conduct tabletop exercises to simulate security incidents. While these exercises are not training in the strictest sense, they provide personnel with opportunities to participate in simulated events and learn what does and does not work.

As mentioned earlier, PIDS training also should include training for system administration activities and for those responsible for maintaining the system. Both functions are equally critical to the airport security mission.

3.4 PIDS Lessons Learned

Not every airport needs a PIDS. At many airports, existing perimeter security measures—usually fencing—fulfills their requirements. At other airports, a combination of measures, fencing, and other physical barriers such as bollards and/or vehicle barriers may be appropriate. For the airports that require a PIDS, the following lessons are based on airports that have documented their experiences in implementing and operating a PIDS.

Airports should consider their individual security threats and experiences with perimeter breaches. These should form the foundation of an airport's requirements. A needs assessment (addressed in Section 3.2.1 Best Practices) will help to determine the necessity for a PIDS and should examine options and costs.

It is in an airport's best interest to determine and document how it intends to use a PIDS. What information is needed to respond to perimeter breaches (or attempts)? Who will see the information (a PIDS operator)? How does the information (PIDS alarms) need to be conveyed (visually on a map, by text, or by auditory means)? What does the PIDS operator do with the PIDS alarm information (SOPs)? All of this information should be captured in a ConOps (Section 3.3.3). The answer to these questions (and others) will be used to identify an airport's PIDS operational requirements, and those requirements should inform the PIDS design process.

An effective PIDS will use multiple technologies that are layered and appropriate to operate in a complementary fashion to achieve effective security (Sections 2.1.2 and 2.3). Every technology has strengths and weaknesses. One of the goals in layering the technologies is to pair the strength of one technology with the weakness of another. Careful layering of technologies results in a PIDS that is more effective than its constituent parts.

In addition, the airport should consider the facility's environment and select the appropriate technologies for its unique setting. Technologies that follow the terrain along a fence line (such as fence disturbance technologies) are better suited to uneven, hilly topologies than those sensors that operate point-to-point requiring straight lines of sight.

PIDS should be designed based on open architecture components (Section 3.3.1) that have established interfaces, and airports should avoid proprietary components that require customization. Airports also should avoid one-off components that are not widely available. Customized software is not field hardened, and often requires code changes to support other system upgrades. In addition, an airport can get locked in to using a single support/maintenance vendor because of the unique, customized software. Open architecture allows for system upgrades so that the PIDS can continue to evolve as its technology evolves.

PIDS maintenance is essential and includes system maintenance as well as physical perimeter maintenance where the PIDS sensors are installed. For most airports, a PIDS will be considered a critical system. While each airport has its specific service-level agreements, it is good practice to employ on-site technicians who are able to address PIDS issues in a timely manner. In addition, regular PIDS maintenance should be performed and should include preventive maintenance and system upgrades. All PIDS upgrades should be performed in a way that ensures harmonization of all components. In other words, airports should not perform a software upgrade to one component without knowledge of how all other PIDS components will interact with the upgraded component. The PIDS perimeter sensors will also require regular maintenance. Infrastructure needs to be inspected for its integrity, and individual sensors will require maintenance or cleaning. For example, perimeter cameras that are mounted near salt water may require frequent lens cleaning.

The airport perimeter must be maintained for effective PIDS operation. Perimeter inspections should be performed regularly to identify any perimeter issues—this is true for airports both with and without PIDS installations. If the PIDS includes fence-mounted technology, it is essential that the fence remains taut and without any debris or growing vegetation. Objects should be kept clear of the fence.

The success of a PIDS is dependent on the working relationships and effective collaboration among its stakeholders (Section 1.2.6). Airport perimeter security stakeholders may include police/first responders, FAA, TSA, and other concerned agencies, airport tenants, emergency management agencies, and airport operations and maintenance personnel. All stakeholders have essential input to the operation, response, maintenance, and life cycle of the PIDS. Including them all from the beginning of the project allows for a wide spectrum of views to consider many options, promotes broad ownership, and helps to ensure the smooth operation of the PIDS.

SECTION 4. CONCLUSION

Every airport has a unique environment and the protection of each airport's perimeter will require measures appropriate to the individual facility. An airport's perimeter protection may be provided by its surrounding terrain or environment (e.g., large body of water), fencing, walls and buildings, electronic PIDS and/or any combination of the preceding. This guide is intended to provide information and best practices that can be used by airports in assessing, evaluating, and implementing the right perimeter protection to meet their needs, in their environment, and within their budget.

REFERENCES

- Barry, Ann S. 2009. *Perimeter Security at San Francisco International Airport: Leveraging Independent, Existing Systems to Form an Integrated Solution*. IEEE International Conference on Technologies for Homeland Security.
- Barry, Ann S. 2008. *Airport Perimeter Security: Where we've been, Where we are, and Where we're going*. IEEE International Conference on Technologies for Homeland Security.
- Barry, Ann S. 2008. *The Secure Perimeter Awareness Network (SPAN) at John F. Kennedy International Airport*. International Carnahan Conference on Security Technology
- Barry, Ann S. 2006. *Mobile Raven: Intrusion Detection and Tracking with Organic Airport Radar and Video Systems*, IEEE International Carnahan Conference on Security Technology.
- Barry, Ann S. 2002. *Surveillance for Airport Perimeter Security*. 2nd Integrated Communications, Navigation and Surveillance Conference Proceedings.
- Barry, Ann S. 2000. *Ground Surveillance Radar for Perimeter Intrusion Detection*. 19th AIA/IEEE Digital Avionics Systems Conference Proceedings.
- Crowe, Tim and Fennelly, Lawrence J. 2013. *Crime Prevention through Environmental Design*. Boston: Butterworth-Heinemann/Elsevier.
- GAO, US Government Affairs Office. 2016. *GAO-16-632 Aviation Security*. Washington, D.C.: US Government Affairs Office (GAO).
- Garcia, Mary Lynn. 2008. *The Design and Evaluation of Physical Protection Systems - 2nd Edition*. Amsterdam: Elsevier/Butterworth-Heinemann.
- International Association of Oil and Gas Producers. 2015. *Effective Guard Force Management Principles and Guidelines*. London: International Association of Oil and Gas Producers (IAGP).
- Jeffery, C. Ray. 1971. *Crime Prevention through Environmental Design*. Thousand Oaks, CA: Sage Publications, Inc.
- Khairallah, Michael. 2006. *Physical Security Systems Handbook*. Oxford: Elsevier / Butterworth Heinemann.
- National Emergency Communications Plan, U.S. Department of Homeland Security, 2014.
- National ITS Architecture Team. 2007. *Systems Engineering for Intelligent Transportation Systems*. Washington D.C.: US Department of Transportation Office of Operations.
- National Safe Skies Alliance. 2016. *Airport Perimeter Breach Classification PARAS 0005*. Alcoa, TN: National Safe Skies Alliance.
- Patterson, David G. 2004. *Implementing Physical Protection Systems A Practical Guide*. Alexandria, VA: ASIS International.
- Price, Jeffrey C. and Forrest, Jeffrey S. 2009. *Practical Aviation Security*. Oxford: Elsevier / Butterworth Heinemann.

RTCA. 2017. *Standard for Airport Security Access Control Systems (DO-230H)*. Washington, DC: RTCA, Inc.

Sennewald, Charles A. 2003. *Effective Security Management - 4th Edition*. Oxford: Elsevier / Butterworth Heinemann.

TransSecure, Inc. 2017. *Recommended Security Guidelines for Airport Planning, Design and Construction (PARAS 0004)*. Alcoa, TN: National Safe Skies Alliance, Inc.

ACRONYMS

AC	Advisory Circular
AC/AC	Anti-Cut/Anti-Climb
ACS	Access Control System
AEP	Airport Emergency Plan
AOC	Airport Operations Center
ASC	Airport Security Coordinator
ASIS	American Society of Industrial Security
ASP	Airport Security Plan
AVB	Active Vehicle Barriers
CMOS	Complementary Metal-Oxide-Semiconductor
ConOps	Concept of Operations
CPTED	Crime Prevention through Environmental Design
ECS/MNS	Emergency Communications Systems/Mass Notification Systems
EMI	Electromagnetic Interference
FAR	False Alarm Rate
FMCW	Frequency Modulated Continuous Wave
FOV	Field of View
fps	Frames per Second
GA	General Aviation
HD	High Definition
H-FOV	Horizon Field of View
IESNA	Illumination Engineering Society of North America
IR	Infrared
LED	Light-Emitting Diode
NAR	Nuisance Alarm Rate
NIMS	National Incident Management System
OSP	Operational Security Plan
PAL	Phase Alternating Line
P_D	Probability of Detection
PIDS	Perimeter Intrusion Detection System
PM	Project Manager
PoE	Power over Ethernet
PSIM	Physical Security Information Management
PTZ	Pan-Tilt-Zoom
PVB	Passive Vehicle Barriers

PWG	PIDS Working Group
RADAR	Radio Detection and Ranging
RF	Radio Frequency
SME	Subject Matter Expert
SSP	Sector Specific Plan
TSR	Transportation Security Regulation
UHD	Ultra High Definition
UPS	Uninterruptible Power Supply
VA	Video Analytics
VMS	Video Management System
VSS	Video Surveillance System
WDR	Wide Dynamic Range

APPENDIX A: SUPPLEMENTAL CAMERA TECHNICAL INFORMATION

A.1 Design Process

The design process for closed-circuit television (CCTV) camera systems should focus on the intended purpose of the surveillance to achieve specific security goals and objectives. The first questions are why and where, not necessarily how. Resolution, image quality, storage retention, etc. are all valid topics, but they are inconsequential without an understanding of the objectives, a means to quantify quality, a categorization of intended objectives, and a well thought out plan for coverage application intended to achieve those objectives.

The initial focus of the design process should be the operational requirements of the system, as identified by the stakeholders. These requirements should be used to inform guidelines for the more technical aspects of the design.

Step 1 - Operational requirements: Through stakeholder interviews and site investigation, a list of objectives is generated. These objectives are listed in terms of area and objective/purpose.

Step 2 - Design guidelines: Image quality is matched to each security objective thereby generating a video surveillance system (VSS) design guideline that is intended to capture all coverage requirements and inform the future application of cameras to the site during subsequent design phases. This guideline should capture all agreed upon coverage goals, and is the starting point for any future value engineering efforts.

Step 3 - Application: Using the VSS design guideline, preliminary coverage and field of view (FOV) exhibits are developed. Coverage exhibits express high-level coverage goals while FOV exhibits take a more granular approach by applying cameras to the site/facility to meet the coverage goals.

Step 4 - Technical recommendations: The application of devices to the airport is used to guide the technical recommendations for the cameras and field devices. Base camera performance specifications will be developed.

Step 5 – Infrastructure requirements: Once camera application and technical requirements are developed, the next step is to develop requirements for the supporting infrastructure. This includes review and recommendations regarding the impact of the additional cameras on the network backbone, VSS existing head end, and electrical/mechanical impact and recommendations.

Step 6 – Estimation and prioritization: With a more precise understanding of the scope and scale of the project, the overall estimate is completed with sufficient clarity to inform future project design stages. Based on the estimate, prioritization takes place to ensure areas of coverage are ranked within budgetary constraints.

A.2 Quantifying Quality and Performance

Ultimately, the quality of an image produced by a given surveillance system is the result of many factors, including lighting, camera resolution, video compression, and camera dynamic range. It can be difficult to quantify the quality of views, but this is an imperative aspect of any successful surveillance project implementation. A baseline for quality and coverage must be set. Lowlight performance, video compression, and dynamic range are aspects of the camera quality and will be discussed in more detail. This leaves resolution as a key design variable that can be directly connected to design objectives.

VSS performance guidelines are defined as a baseline for coverage quality that are used in conjunction with the VSS coverage guidelines to inform the application of the cameras to the site. The performance guidelines are based on performance objectives as set forth in the UK's Home Office Scientific Development Branch Publication 28/09 and in the International Civil Aviation Organization (ICAO) Document 8973. These guidelines include five general observation categories for cameras: monitor, detect, observe, recognize, and identify. These categories are defined as follows:

Monitor: From this level of detail, an observer should be able to monitor the quantity, direction, and speed of movement of people across a wide area, provided their presence is known; i.e., they do not require a search.

Detection: After an alert, an observer would be able to search the display screens and ascertain with a high degree of certainty whether or not a person is present.

Observation: At this scale, some characteristic details of the individual, such as distinctive clothing, can be seen, while the view remains sufficiently wide to allow some activity surrounding an incident to be monitored.

Recognition: Viewers can say with a high degree of certainty whether or not an individual shown is someone they have seen before.

Identification: Picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.

Figure A-1 illustrates the difference in quality between identification, recognition, and detection at the level of a pedestrian. It should be noted that the quality of image required for a vehicular target differ from that of a pedestrian, but the same levels are used for clarity. A level of recognition for a pedestrian is roughly equivalent to that of identification for a vehicle.

Figure A-1. Visual Quality Comparison



Source: Axis Communications

When these guidelines were first developed in 2005, all video was based on National Television System Committee and Phase Alternating Line (PAL) analog video standards; metrics were based on the percentage of screen height occupied by the image. With the advent of higher resolution cameras, the metrics have evolved to a pixels-per-foot or pixels-per-meter metric. This metric defines the expected

pixels per foot or meter at the expected viewing distance for the camera. For example, if a camera is focused on viewing a door, the minimum resolution at the door should meet the metrics for the view guideline at the door. The expected minimum pixels per foot are depicted in Figures A-2 and A-3 below.

Figure A-2. VSS Performance Guidelines – % of Height of Image

FIXED CAMERA VIEW TYPE	Abbreviation	% HEIGHT OF IMAGE (BASED ON 6ft TARGET)				
		PIXELS PER FEET (ppf)		720P RESOLUTION (720H X 1280W)	1080P RESOLUTION (1080H X 1920W)	4K/UHD RESOLUTION (2160 X 3840W)
		TARGET	RANGE			
IDENTIFICATION	ID	125 ppf	100 - 150 ppf	83%	55%	35%
RECOGNITION	REC	55 ppf	35 - 100 ppf	46%	31%	20%
OBSERVATION	OBS	24 ppf	15 - 35 ppf	21%	14%	10%
DET	DET	12 ppf	8 - 15 ppf	10%	7%	5%
MONITOR	MON	5 ppf	4 - 8 ppf	4%	3%	2%

Figure A-3. VSS Performance Guidelines – H-FOV Width

FIXED CAMERA VIEW TYPE	Abbreviation	APPROXIMATE FOV WIDTH				
		PIXELS PER FEET (ppf)		720P RESOLUTION (720H X 1280W)	1080P RESOLUTION (1080H X 1920W)	4K/UHD RESOLUTION (2160 X 3840W)
		TARGET	RANGE			
IDENTIFICATION	ID	125 ppf	100 - 150 ppf	10ft	15ft	31ft
RECOGNITION	REC	55 ppf	35 - 100 ppf	23ft	35ft	70ft
OBSERVATION	OBS	24 ppf	15 - 35 ppf	53ft	80ft	160ft
DETECTION	DET	12 ppf	8 - 15 ppf	107ft	160ft	320ft
MONITOR	MON	5 ppf	4 - 8 ppf	256ft	384ft	768ft

The identification level has traditionally been defined as the ability to identify a person in a manner that would be admissible in a court of law. As the original definition included the entire person in the image, identification was not based exclusively on the face of the person, but also included the overall person and clothing. For this definition, 100 pixels per foot (325 pixels per meter) is adequate.

In recent years, the definition of identification level has begun to evolve and is now being used by many manufacturers as being able to identify a person based on facial features alone. Based on this revised definition, industry leaders note that 120 pixels per foot (400 pixels per meter) is a viable metric, with 150 pixels per foot (500 pixels per meter) being a metric to be applied to video with challenging conditions. Challenging environmental conditions include factors such as insufficient lighting, or people, objects, and vehicles moving at high speed.

A.3 Camera Technologies

Camera technologies should be evaluated via a number of technical aspects important to the stakeholders and installation sites under consideration, including:

- Compatibility with the existing video management system (VMS)
- Resolution requirements
- Lighting performance
- Fixed versus pan-tilt-zoom (PTZ)
- Frame-rate and bandwidth
- Resiliency and miscellaneous recommended features
- Minimum camera specifications

A.3.1 Compatibility

Any and all new cameras implemented in the design will more than likely be required to be compatible with the airport's existing VMS. This is an important consideration in designing CCTV systems.

A.3.2 Resolution

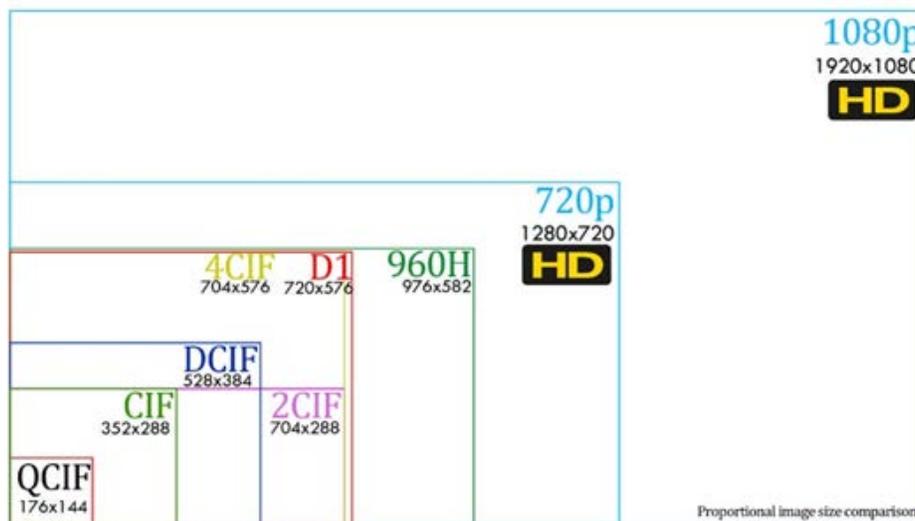
All other things equal, camera resolution and, more important, pixels on target are considered the most objective means to evaluate camera quality and camera views. Until recently, the use of cameras providing beyond 720p resolution was expected to come with trade-offs in lowlight performance, frame-rate, bandwidth, and storage. These issues are no longer a constraint.

Current recommendations are to set the baseline for all cameras at high-quality 1080p, to use high-resolution cameras where effective, to establish 4K/UHD as the standard for high-resolution, and to consider the use of panoramic cameras for interior areas where practical.

Minimum 1080p Resolution Cameras

The days of 4CIF 704 x 576 px cameras are effectively over. Advances in chip technology and video compression have fueled a constant increase in camera resolution. This progress has also consistently lowered cost and reduced the impact on storage to a point where the current baseline for video resolution is considered 1080p. Figure A-4 illustrates the difference in camera resolutions.

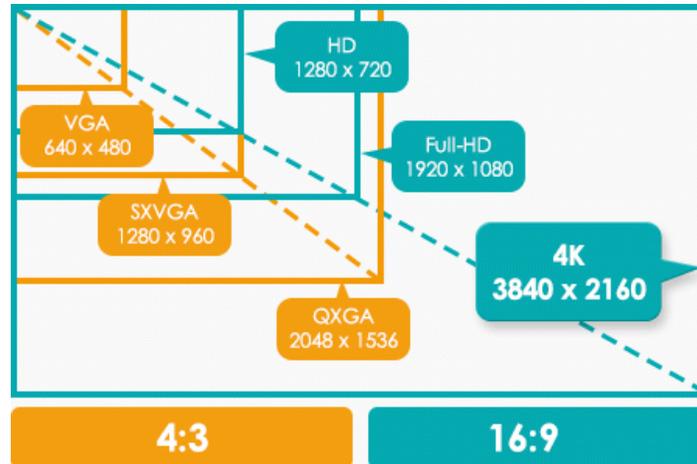
Figure A-4. HD 1080p Resolution Comparison



Source: Camvex Video Surveillance

As shown in Figure A-4, above, HD 1080p provides a significant increase in resolution over other legacy resolutions. Figure A-5, below, illustrates the relationship between HD and 4K resolutions.

Figure A-5. Comparison of 4K to HD Video Resolution



Source: Panasonic

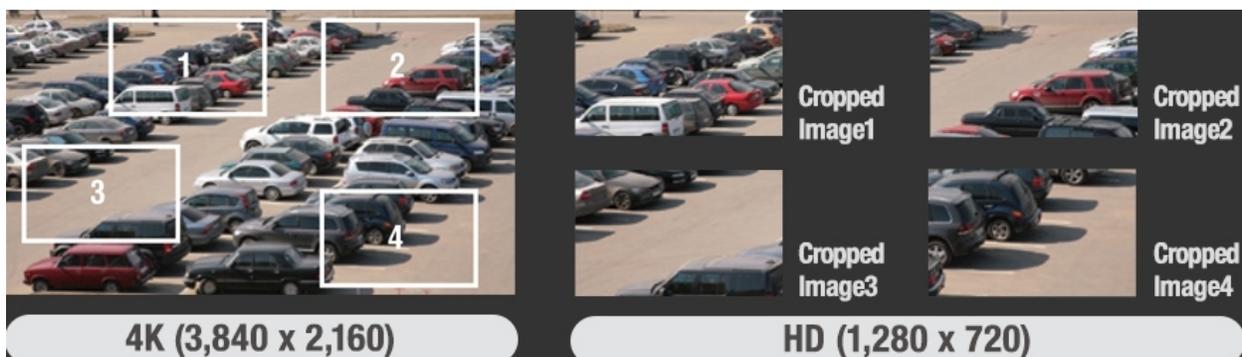
High Resolution Cameras

As with consumer electronics, the resolution of surveillance cameras has continued to advance to the point that high-resolution cameras (those above 1080p) are becoming more commonplace and serving vital roles. In an outdoor environment, high-resolution cameras can effectively provide high-quality coverage of large areas. Though cost is a factor, high-resolution cameras can potentially replace lower-resolution versions at a 1:2 ratio or better (1 high resolution camera in place of 2 or more lower-resolution cameras.)

Advances in camera chip technology, onboard processing, and lens quality have continued to increase the resolution of surveillance cameras while at the same time improving the quality of video that can be captured. Issues that once plagued the high megapixel market, such as poor lowlight performance, have steadily been solved, allowing high-resolution cameras to be effective tools for covering large areas.

A high-resolution camera can provide surveillance of an entire area, allowing for forensic investigation of the area adjacent within the camera FOV. It is also possible to zoom and pan within the image, creating a virtual PTZ within live or recorded video as shown in Figure A-6. This can also allow for the ability to record multiple views within an overall view, to provide higher resolution for that specific area while recording the overall scene at a lower resolution to save recording resources.

Figure A-6. Cropped Image Views from Single 4K/UHD Image



Source: Panasonic

4K/UHD Resolution Cameras

High-resolution cameras, as defined above, can include anything from 2 megapixels to 30 megapixels. As with HD and Full HD (720p and 1080p, respectively), there are additional standards for color quality that are implied in the designation of 4K/UHD (see Figure A-7). Resolutions near this standard include 5 megapixel and 6 megapixel cameras, which can be considered equivalent.

Figure A-7. 4K/UHD Camera



Source: Panasonic

Ultra-high resolutions such as 30 megapixels should only be considered when warranted. These resolutions are non-standard in the surveillance industry, with just a few manufacturers (Axis and Avigilon) providing solutions. In addition, the high resolution of these cameras impacts their ability to access important features such as multi-image wide dynamic range, and their impact on storage and bandwidth can be significant.

4K/UHD versus 1080p

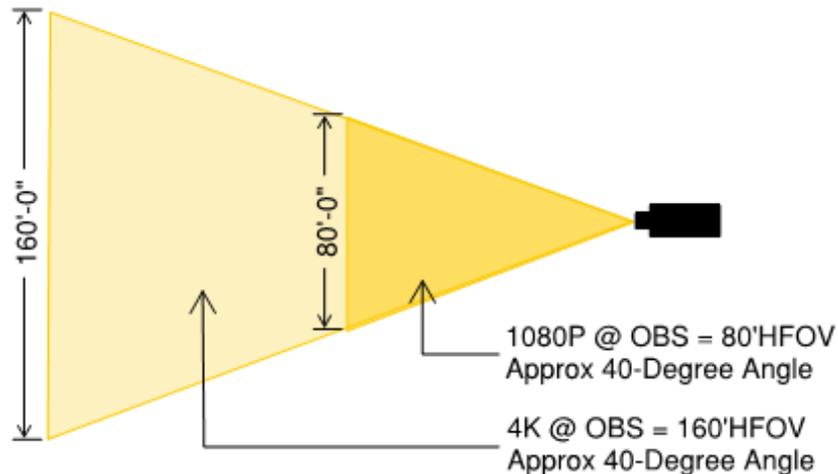
4K/UHD-resolution cameras represent a 4x increase of resolution when compared to standard 1080p-resolution cameras. In areas where high pixel density is necessary or where large areas need to be covered, this increase in resolution can have a significant impact. As shown below in Figure A-8, a 4K/UHD camera can double the effective horizontal field-of-view (H-FOV) from 80 feet to 160 feet while maintaining the same quantity of pixels per foot.

Figure A-8. H-FOV Width for 720p, 1080p, and 4K/UHD

FIXED CAMERA VIEW TYPE	APPROXIMATE FOV WIDTH		
	720P RESOLUTION (720H X 1280W)	1080P RESOLUTION (1080H X 1920W)	4K/UHD RESOLUTION (2160 X 3840W)
IDENTIFICATION	10ft	15ft	31ft
RECOGNITION	23ft	35ft	70ft
OBSERVATION	53ft	80ft ←	→ 160ft
DETECTION	107ft	160ft	320ft
MONITOR	256ft	384ft	768ft

This increased coverage can be used to effectively cover large areas while minimizing the total number of cameras implemented. Figure A-9 illustrates the impact that this increased coverage capability would have on a sample area. The area would require multiple 1080p cameras to provide what one 4K camera can provide. Real-world issues such as physical obstructions and mounting locations will impact this ideal situation, thereby limiting the application of these cameras as noted below.

Figure A-9. OBS FOV Comparison between 1080p and 4K



Because high-resolution cameras have some inherent issues that impact their use in all situations, the recommendation is that they be used in key locations only. Relative to lower-resolution cameras, these issues include the following:

- Reduced performance in lowlight situations due to pixel density on the chips
- Limitations to FOVs due to physical obstructions, limiting the overall effectiveness
- Increased demand on video storage
- Increased demand on network bandwidth
- Increased cost

Panoramic/Multi-sensor Megapixel Cameras

Panoramic megapixel cameras are becoming a popular option in surveillance systems, chiefly because they provide enhanced capabilities for covering large, open areas. Panoramic cameras offer high-resolution images spread over wide FOVs, commonly 180–360 degrees. Unlike PTZ cameras, panoramic cameras can see and record everything within the FOV; however, PTZ cameras have superior optical zoom capabilities. Multi-sensor cameras (as shown in Figure A-10) draw very little power (5.5 watts maximum using power over Ethernet [PoE]) as compared to a PTZ camera, which can draw more power (19 watts maximum). Three multi-sensor cameras can be implemented for each PTZ camera without adding any power requirements for the overall system.

Figure A-10. Multi-sensor Camera



Source: Arecont Vision

Panoramic cameras offer an attractive option to PTZ cameras, but current market solutions have limitations that must be considered prior to implementation:

Frame Rate: Because of the high resolution of images that are stored on a panoramic camera, the processors may be limited to lower frame rates at full resolution. While frame rates have improved, the cameras often cannot achieve 30 frames per second (fps) at full resolution, making them less than ideal for some applications.

Poor Lowlight Performance: High megapixel cameras pack large quantities of pixels into chips the same sizes as their lower-resolution predecessors. The simple physics of this means less light hits each pixel, thereby causing light harvesting issues. As a result, these cameras should not be relied on for lowlight situations.

Fixed Focal Length: Typically, these cameras have fixed focal lengths. The lenses are set to provide a wide depth of field, but the lenses are typically focusing 50 to 75 feet away. Objects further away will not have critical focus.

Waste Area: A camera that is covering a full 360-degree field of view will have a high percentage of unnecessary views. When compared to fixed megapixel cameras focused on specific areas, the panoramic cameras may view and record areas that are not of interest, effectively wasting storage on video that will not be viewed.

VSS/VMS Acceptance: The level of integration of panoramic cameras into VMS varies greatly among the different manufacturer offerings. The benefits of a panoramic camera may be heavily dependent on the VMS platform and may not be fully compatible. In addition, multi-sensor cameras may require licensing per sensor and/or cropped view.

Storage: Panoramic cameras provide high resolution throughout the camera view. For a 360-degree panoramic camera composed of four individual sensors (see Figure A-11), each sensor will have higher resolution than a PTZ camera. This means that each panoramic camera will provide more than four times the data as a PTZ. The use of the panoramic camera will increase the overall storage requirements over the traditional PTZ camera.

Figure A-11. Example 180-Degree View



Source: Arecont Vision

Panoramic cameras are not recommended for exterior coverage. Their lowlight performance and mounting requirements make them, in general, a poor fit for these situations.

Panoramic cameras are considered a more viable solution for interior coverage and are recommended where the camera's abilities align with unique coverage requirements.

A.3.3 Lighting

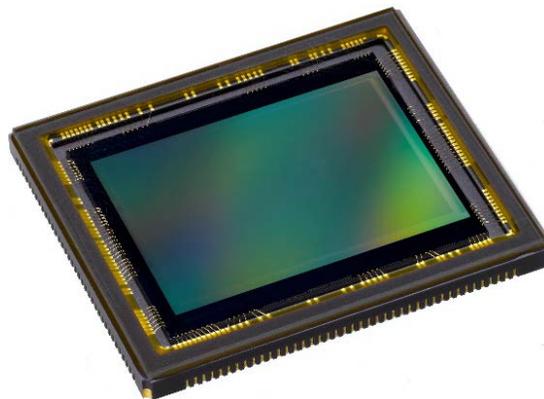
Lowlight and wide-gamut light performance is quite possibly the most important feature of a surveillance camera in complex exterior environments. Without quality lighting performance, the high-resolution camera will be less effective.

Lowlight Performance

Airports are active environments at all hours of the day. Winter brings extended hours of darkness, and some international terminals may even see increased passenger loads in overnight hours. Artificial lighting can provide the safety of a well-lit area, but this is not always coordinated with security surveillance needs, and certain types of artificial light can actually hinder image quality. Ultimately, it is important to use cameras that can provide the highest quality images in the lowest light possible.

Though camera resolution has increased, the physical size of the CMOS⁴ image sensors has not (Figure A-12). The increase in resolution is made possible by fitting more individual photosensitive diodes into the same physical area. This consistent reduction in the size of diodes means they are subject to increasingly less incident light. The old adage is that lowlight performance gets worse as resolution increases, but camera manufacturers have developed various methods to sidestep this issue and bring quality lowlight performance to high-resolution cameras.

Figure A-12. CMOS Sensor



Source: Canon

Day/night cameras are designed for exterior applications where lighting levels can vary significantly. During the day, lighting is sufficient, but after dusk, lighting levels can drop drastically. To account for these varying lighting conditions, certain manufacturers have packaged imagers and filters into a single camera so that the camera automatically adjusts when lighting deteriorates. During lowlight situations, the camera physically moves an IR filter into the light path and uses near-infrared light to provide a usable monochrome image. The obvious drawback is the loss of color, as shown in the bottom left image in Figure A-13.

⁴ CMOS: Complementary Metal-Oxide-Semiconductor

Figure A-13. Lowlight Examples



Source: Bosch

On-camera or dedicated IR artificial lighting is another way to deal with lowlight situations. In these cases, the camera is capable of controlling on-camera or off-camera dedicated IR lights. As with day/night cameras, an IR filter is brought in so the camera is still only producing a monochrome image. The benefit is that the scene can be illuminated more effectively, and the camera can produce more usable images. The upper right image in Figure A-13 is an example.

Finally, manufacturers have proprietary solutions that combine special CMOS chip technology with on-camera software enhancement to produce quality color images in situations that the human eye would consider almost completely dark. The bottom right image in Figure 41 is an example. Though these solutions are unique to each individual manufacturer, they work with all current industry standards and are largely independent of any compatibility issues with VMS software. Additionally, most of the top manufacturers offer similar solutions under various names, such as Bosch Starlight and Axis Lightfinder. Some manufacturers claim extreme wide dynamic ranges (discussed further below). Ultimately, a camera's ability to resolve usable color images below 1 lux should be the target requirement (see Table A-1).

Table A-1. Lux Condition Equivalents

LUX RATING CHART

	Condition	Light Level (LUX)	Foot Candles (FC)
Day Time	Sunlight	107,527	10,000
	Daylight	10,752.70	1,000
	Overcast Day	1,075.30	100
	Very Dark Day	107.53	10
	Twilight	10.75	1
Night Time	Deep Twilight	1.08	0.1
	Full Moon	0.108	0.01
	Quarter Moon	0.0108	0.001
	Starlight	0.0011	0.0001
	Overcast Night	0.0001	0.00001

Of the three options noted above (i.e., day/night cameras, on-camera or dedicated IR artificial lighting, or CMOS chip technology with on-camera software enhancement), common recommendations for airports include the third solution, which can best be described as enhanced lowlight color performance. The expected situation at most airports is that artificial light will likely provide environments with shadows in the 1 to 10 lux range. Quality cameras with superior lowlight color performance as well as wide dynamic range, as described below, are best equipped to provide security staff with usable, actionable images.

Wide Dynamic Range (WDR)

Wide gamut lighting scenes are another challenging situation cameras often face. Cameras typically have a much smaller window of dynamic range than the human eye. On a sunny day, we may see a covered taxi stand as a shaded area, while a camera only sees darkness as the camera is trying to correctly expose the sunlit areas. Most imagers are not capable of correctly exposing two areas that differ beyond 12 to 15 stops of light. This situation is faced daily in almost all exterior frontage areas, and is problematic during all hours of the day.

Interior cameras face a similar issue. The majority of a scene may be well lit, but sun through a window or door may be overexposing certain areas or causing the camera to underexpose other more important parts. Likewise, car headlights and cameras viewing entry areas can create challenging conditions as shown in Figure A-14.

Figure A-14. Non-WDR versus WDR View

Source: Viper Solutions

Manufacturers have developed ways to maximize the usable video that can be obtained from cameras faced with such challenging lighting situations. These cameras are typically said to have WDR, and while there are different methods to achieve it, and some are better than others.

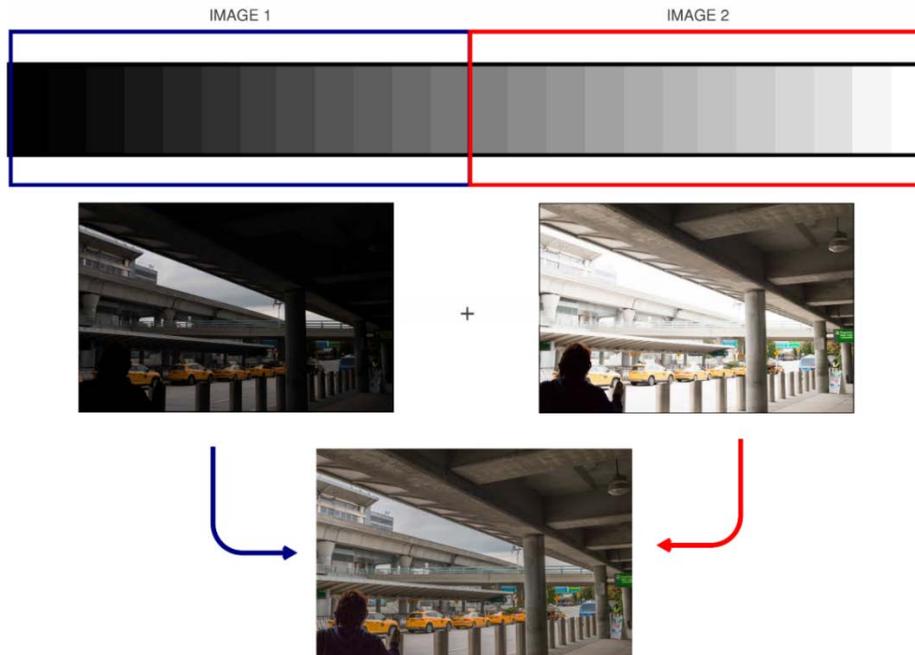
Contrast Enhancement

Contrast enhancement is considered the least effective means of WDR. With this method, the camera adjusts the contrast of the scene in an effort to expand its dynamic range. However, the image is still limited to its original dynamic range, as the camera simply tries to compress the dynamic range of the scene into that of the camera.

Multi-Image Stacking

With multi-image stacking, the camera shoots two almost simultaneous images: one set to the low end of the spectrum and one to the high end. The camera processor takes both images, stacks them, and creates a single image using the best exposure to create a single high-dynamic range image that is transmitted as the single captured frame (see Figure A-15). This is considered a superior method to contrast enhancement and is often called True WDR.

Figure A-15. Multi-Image Stacking WDR



Combination of Both

The recent availability of a third option combines both of the above methods along with advanced algorithms and chip technology. Most industry-leading manufacturers have their own version of this technology, including Axis’ “Forensic Capture” and Panasonic’s “Super-WDR.” The technology can produce remarkable results.

A.3.4 Fixed vs. Pan-Tilt-Zoom

While the advent of modern megapixel fixed cameras has brought forth the idea of eliminating relatively expensive PTZ cameras in favor of high-resolution cameras with forensic zoom capabilities, the reality is that each technology has pluses and minuses. A high megapixel camera can provide surveillance of an entire area, allowing for forensic investigation within the camera FOV. It is also possible to zoom and pan within the image, creating a virtual PTZ within live or recorded video.

However, when a security alarm occurs, the megapixel cameras may not offer the ability to view a specific portal or area further from the camera with sufficient resolution to assess the nature of the alarm. In contrast, the PTZ camera provides flexibility and coverage capacity, with the ability to assess alarms, view specific locations, and allow for following specific people in real time. For forensic purposes, however, the PTZ will almost invariably be pointed in the wrong direction or will not provide the view or resolution necessary.

The application for most video coverage is forensic in nature and suited to the never-blinking fixed camera views. PTZ cameras are recommended as supplemental to fixed camera coverage. In active situations, PTZs will allow for more investigative review of live situations and can also supplement as repositionable fixed camera views when not actively being repositioned by an operator.

A.3.5 Network Utilization and Storage

Camera resolution, compression algorithms, and frame rate are the primary parameters affecting network utilization and storage requirements. Resolution is largely a function of the required image

quality coupled with frame rate, and compression algorithms can be used to reduce the overall impact on the network and storage requirements. Frame rate impacts the ability of cameras to capture certain aspects of motion and can be adjusted on a camera-by-camera basis to best fit the various objectives of each camera.

Frame Rate

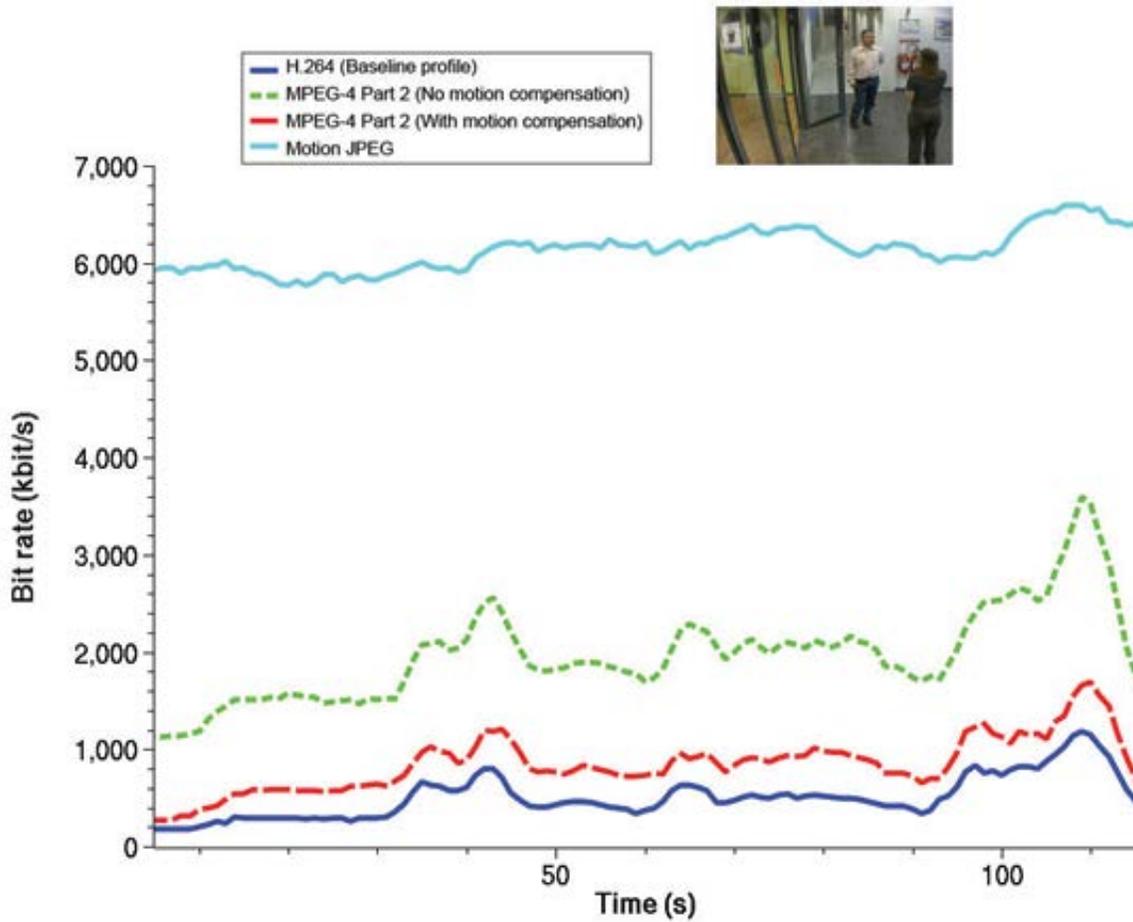
In addition to the pixels per feet/meter, another important metric for camera video is fps. A more subjective measure, fps is related to the type of activities being viewed. The NTSC standard for full motion video in the United States is 30 fps. The fps for traditional analog cameras was related to the power frequency; the analog cameras were interlaced units, meaning that they would capture every other line of the video, every other cycle. So, a full frame would be captured every two cycles of the 60 Hertz power cycle for US utility power, creating the 30 full fps. While this has been the traditional industry metric for what is considered full motion video, the human eye tends to perceive anything above 12 fps as motion. Movies have standardized on 24 fps, and while higher frame rates are being trialed, most people cannot differentiate between standardized and higher rates.

In the CCTV industry, 30 fps is typically only used in specific applications that involve sleight of hand or objects moving at speed. For example, casinos typically use 30 fps to detect misdealing or other gambling sleights of hand. Cameras placed on interstates for tolling purposes may capture video at or above 30 fps based on the vehicle speeds and the need to capture a license plate view. In airport environments, it is much more common to record at 15 fps on a routine basis while motion is present, and only raise the fps when an alarm occurs within the camera FOV. It is also common to reduce the fps during periods of inactivity, with the fps being reduced to 7.5 or even to 1 when no motion is detected in the camera FOV. Most airports will continue to record at least 1 fps for all cameras even when no activity is present, since the ability to prove that no activity occurred is often as important as proving that something did occur. The frame rate for cameras can be set on a camera-by-camera basis so there is flexibility to meet a variety of needs.

Bandwidth, Compression, and Storage

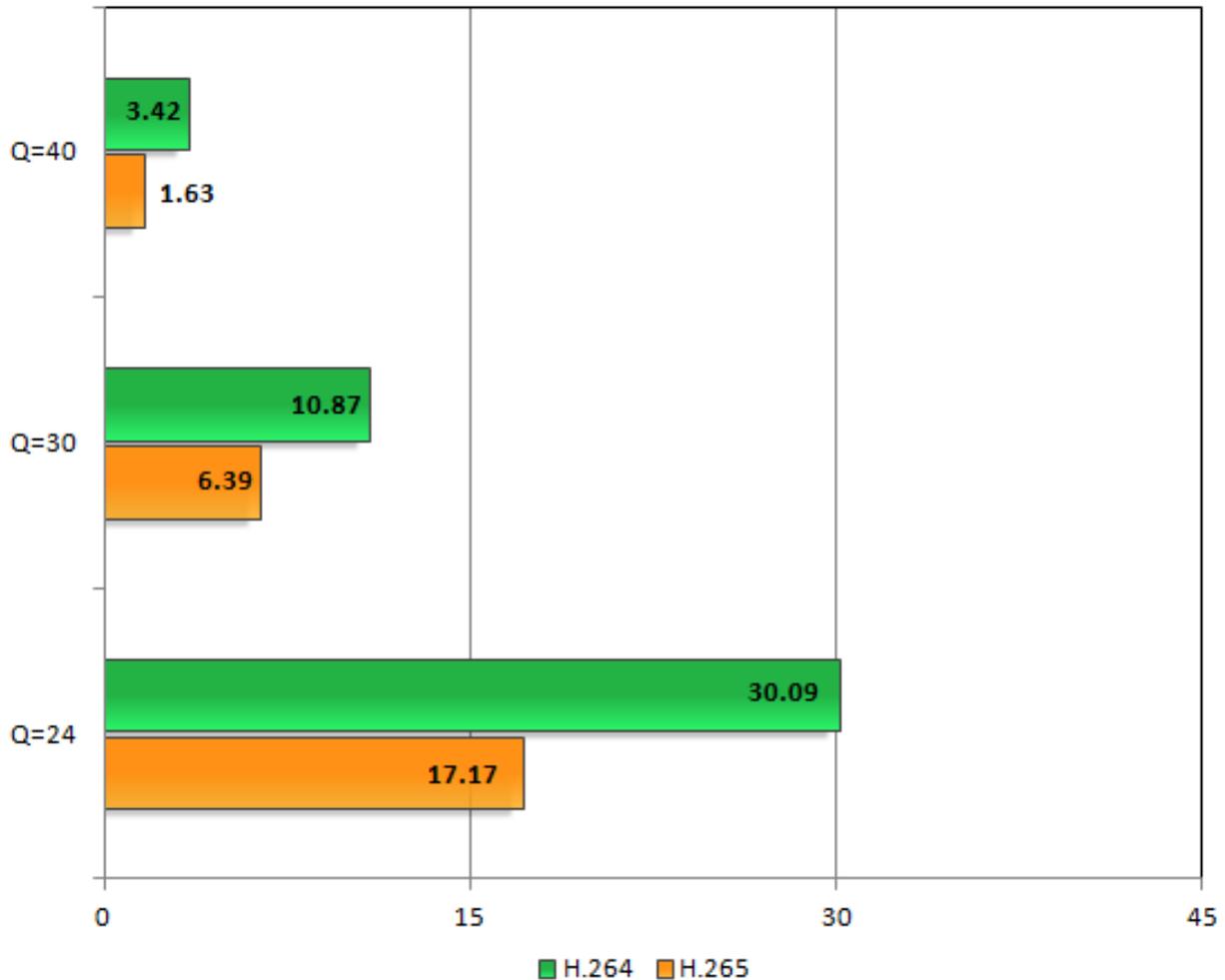
H.264 video compression has become widely available in the marketplace and is now considered the industry's standard form of compression. Compared with the older MPEG-4 compression, H.264 offers a significant savings in bandwidth and storage as shown in Figure A-16.

Figure A-16. Motion JPEG, MPEG-4, and H.264 Bit Rate Comparison



The latest video compression released is H.265, and the expected decrease in bandwidth and storage is 40 to 50 percent compared to H.264 as shown in Figure A-17 below. As camera resolution continues to increase, the ability to further compress the video is critical. However, it is important to note that the bandwidth reduction cannot occur unless a camera is either replaced or upgraded. This means that the installed cameras are likely to remain at H.264 until such time as the cameras are replaced. As the recording size is related to the compression used on a camera, it may be worthwhile to evaluate the storage costs versus camera costs to determine if a scheduled replacement makes sense to save storage space.

Figure A-17. H.264 versus H.265 Storage Comparison (in MB)



A.3.6 Camera Ease-of-Maintenance and Resiliency

A system that only achieves project objectives temporarily before system fatigue takes over is not acceptable. Beyond the noted security objectives, providing for a maintainable and durable solution is imperative to meeting the overall system objectives sustainably. Key aspects of a durable and maintainable solution include:

Camera Locations: The best defense against camera vandalism is to locate the cameras out of the reach. This needs to be weighed against maintenance and FOV concerns, but mounting heights should be chosen to remove the temptation to vandalize.

Vandal Resistance: Since it may not always be possible to locate cameras out of harm's way, any camera within reach of pedestrians should be vandal resistant. Vandal-resistant cameras are widely available in the marketplace and not significantly more costly than standard versions. Wherever possible, all cameras and supporting infrastructure should be locked and located out of sight.

Temperature Ratings: Many cameras and supporting equipment will be subjected to temperature extremes. Both cold and hot weather performance needs to be considered, but overheating due to direct sunlight on equipment and enclosures is likely to be the most detrimental to system performance. Preference should be given to equipment with operating temperatures in the -10 to +125-degrees Fahrenheit range. For extremely cold-weather situations, heaters may be necessary in special situations.

Weather Ratings: Any cameras located outside will need to be capable of sustaining wet weather and direct water spray that may be necessary for routine maintenance.

Maintenance Considerations: Choice of locations for equipment, including cameras and supporting infrastructure, should be based on simplifying maintenance access in addition to the primary need of supporting specific FOVs. Cameras that are located in hard-to-reach areas that can only be accessed via special equipment or extensive roadway shutdowns will likely not be as well maintained and will eventually negatively impact the quality of the overall system.

Network and Power Redundancy: Redundancy for both network and electrical connectivity should be considered, but it should be noted that redundancy can come at a cost that greatly exceeds the benefit. This is especially true when considering exterior installations. Weather changes can turn backup battery systems into maintenance headaches, and long-life/weather resistant uninterruptible power supplies or generator power can be expensive.

A.3.7 Minimum Camera Specifications

Following is a list of minimal camera specifications. Specific camera requirements will vary from area to area. This list simply details camera functions that will be important to providing quality images for any PIDS.

- **IP-Based Cameras:** All cameras should utilize standard Ethernet to communicate to the VMS. Likewise, all cameras should be native IP.
- **Power over Ethernet (PoE):** Where possible, all cameras should be powered by PoE. Outdoor units may require separate power supplies due to their increased power load. Mid-span PoE devices could be used to provide PoE power if PoE switches are not available.
- **Megapixel Resolutions – Fixed Cameras:** The required resolution will vary depending on the location of each camera. 4CIF (704x576), also considered standard definition, is approximately equivalent to legacy analog resolution. Though this cost-effective option is still useful, it is recommended that 3MP or higher resolution cameras should be considered the minimum acceptable resolution for a PIDS.
- **Megapixel Resolutions – PTZ Cameras:** Until recently, PTZ cameras have been limited to 4CIF resolution. At the time of this report, 4CIF versions still dominate the industry, but 3MP and higher versions are widely available. HD/Megapixel PTZ cameras should be considered the minimum requirement, with 4CIF-resolution versions to be used in specific locations.
- **30 Frames per Second (fps):** Cameras should be capable of transmitting 30 fps at their highest resolution. Lower rates may be acceptable for high-resolution cameras, but should never go below 15 fps.
- **Video Streams:** The cameras should be capable of transmitting at least three streams with unicast and multicast capabilities. The streams should be capable of being adjusted for encoding type, frame rate, and quality separately from each other.
- **Video Encoding:** H.264 should be the standard encoding method for at least one of the streams, at full resolution and images per second.
- **Video Analytics:** At a minimum, cameras should be internally capable of motion and camera tamper analytics. Depending on the final system design, higher-level analytics could be camera or server based.
- **WDR:** Many cameras will be required to resolve images that have widely varying lighting conditions, such as the main entrance. In these areas, highly capable WDR cameras can reduce

incoming light levels for selected areas of the image, thereby allowing darker areas to be correctly resolved.

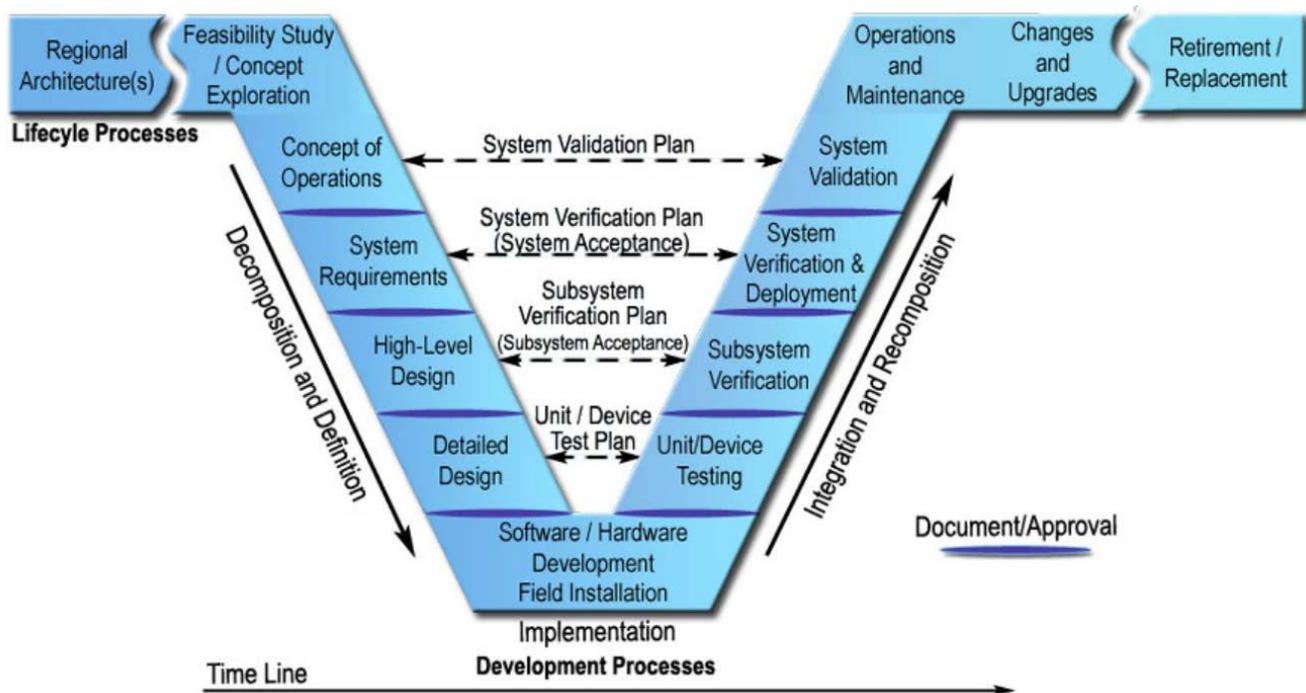
- **Lowlight Performance:** Many cameras will be required to operate in lowlight situations. Exterior cameras are an obvious example, but nearly all interior cameras will also be faced with lowlight situations throughout a given day. Low ambient light levels are a major factor in poor quality images, so cameras with proven lowlight performance are imperative.
- **Environmental Housing:** Exterior cameras should be enclosed in environmental housings that maintain an IP66 rating at minimum. Housings should have heaters and blowers.
- **Vandal Resistant:** External cameras located within reach of people should be enclosed in vandal-resistant housings. Cameras mounted under the covered walkways where ceilings are within reach are an example of where these should be used. Vandal-resistant housing may be used sparingly on interior cameras as well.

APPENDIX B: SYSTEMS ENGINEERING METHODOLOGY AND SUPPLEMENTAL INFORMATION

The practice of systems engineering reduces the risk inherent in complex projects and increases the probability that the final system will meet user needs by clearly and measurably defining the system before implementing the solution. The process starts by asking the team to define the problem they are trying to solve rather than by describing the solution.

The systems engineering model identifies the discrete system life cycle steps, such as problem definition, concept of operations (ConOps), design, implementation, maintenance, and others. The model, known as the “V,” is shown in Figure B-1.

Figure B-1. Methodology for Systems Engineering



Source: National ITS Architecture Team 2007

Concept of Operations

Melding physical security measures with technology systems, processes, policies and procedures, and personnel through a ConOps improves the efficacy of the security program while reducing risk. Moreover, engaging stakeholders in the planning and design process, including the FAA, TSA, and other concerned agencies; airport tenants; and law enforcement, emergency management agencies, and airport operations and maintenance personnel, yields a more accepted security approach and improves operational success (TransSecure, Inc. 2017). Table B-1 provides basic elements of a ConOps for individual security initiatives. Using this process for all security initiatives supports consistency in building competencies among end users, and provides a methodology to identify issues to be mitigated prior to implementation.

Table B-1. Basic Elements of a ConOps for Security Initiatives

Element Number	Element Description
1	Security Mission Statement – Provides guidance necessary to establish and mature the security program and elements within the program to link strategy, objectives, and tactics
2	Security Engagement/Cooperation Plan – Provides a formalized committee structure to link relevant airport stakeholders into the security planning, implementation, and management process (See Section 3.1.1.3, Project Stakeholders)
3	Operational Measures – Provides functional elements to: <ul style="list-style-type: none"> • Promote intrusion deterrence, detection, assessment, and response • Support the implementation of perimeter security initiatives • Link perimeter security initiatives to access control • Define video surveillance protocols including use of video analytics • Identify security needs for vehicle queuing operations • Identify parameters for recognition and management of suspicious behavior • Assess and mitigate territorial reinforcement needs • Define operational procedures for gates, doors, bollards, fencing, lighting, and other perimeter protective design features and systems • Define information/data collection, storage, and retention policies • Ensure emergency generators supporting perimeter security needs are fueled and functional • Ensure signage is properly maintained
4	Communications – Facilitate tactical interoperable communications among relevant airport stakeholders to support perimeter security alarm assessment and response
5	Staffing – As perimeter security initiatives are contemplated, assess the impact on labor to ensure that staffing levels and training are appropriate for the chosen perimeter security initiative
6	Perimeter Security Supportive Technologies – Address selection, use, and deployment of video surveillance, intrusion detection, access control, call for assistance, voice communications, mass notification/emergency communications systems, and other technologies to meet perimeter security objectives
7	Protective Design Elements – Identify existing and theoretical physical design elements to support perimeter security and their impact/interface regarding personnel, processes, and technology, including necessary training and exercise programs to support effective, competent use of protective design elements
8	Central Control Center/Emergency Operations Center Functions – Ensure that central control center/ emergency operations center functions are readily available and that coordination protocols among all stakeholders are established to support timely and accurate communication, resourcing, and procedural implementation
9	Emergency Response Plan – Ensure that emergency response plans are written in accordance with NIMS/ICS and other relevant standards and synchronize response procedures with perimeter security initiatives
10	Crisis Communication Planning – Ensure that communications procedures for the media and general public address perimeter security intrusions that may require alternative operations or expedited closure of the airport, and ensure that coordination procedures address airport participation in a joint information center with other relevant stakeholders
11	Training and Exercises – Ensure that training and exercises are performed with respect to changes in perimeter security procedures and technology

Element Number	Element Description
12	Change Management – The ConOps should identify a process for resolving and documenting updates and changes in technology, physical security, procedures, and staffing to ensure that perimeter security is maintained throughout all possible changes. Change management should also address modifications to perimeter security when threat and vulnerability assessment indicates a change in threat posture.

The ConOps recommendations are based in part on DHS protocols provided in the National Infrastructure Protection Program and the Transportation Systems Sector Specific Plan (SSP). The SSP is the strategic plan for the transportation sector, fulfilling the requirements of Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, and the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended by the 9/11 Commission Act) for the National Strategy for Transportation Security. The SSP consists of a base plan and six modal annexes (aviation, maritime, mass transit and passenger rail, highway infrastructure and motor carrier, freight rail, and pipeline) and consolidates strategic planning and infrastructure protection requirements.

The SSP describes collaboratively developed strategies to reduce risks to critical transportation infrastructure from the broad range of known and unknown terrorism threats. Other SSP-derived best practices and initiatives that support perimeter security and overall airport security are provided below.

All-Hazards Risk Assessment

Airports should work with industry subject matter experts and DHS to identify and implement an all-hazards risk assessment model that includes terrorism and man-made, technological, and cyber threats, as well as natural hazards. Periodic use of a nationally recognized all-hazards risk methodology allows airports to update the risk profile and to apply results to modify the overall security program.

Scheduled Review of Security Best Practices

In conjunction with periodic (biennial/triennial) risk assessments, airports should conduct a comprehensive review of best practices in security planning and program management, revise and implement security and preparedness plans and procedures, and use best practices to guide executive decision-making and preparation of integrated plans, budgets, and programs to support all-hazards risk mitigation.

Scheduled Review of Security Policies and Procedures

In conjunction with periodic (biennial/triennial) risk assessments, airports should conduct a comprehensive review of facility security policies and procedures from an operational standpoint and modify or adjust them to existing conditions. During reviews, airports should focus on identifying gaps and preparing new security policies and procedures that reflect both internal and external needs and are consistent in style, depth, and content based on existing threats.

Develop the Basis of Design

The basis of design, with regard to systems engineering, includes a narrative covering the technical expectations and operational requirements of the system. If properly implemented, the basis of design will address and subsequently codify the functional requirements identified in the project's ConOps. The basis of design should remain technical in nature and not focus on personnel-related practices such as staffing, policies, and procedures. The intent of the basis of design is to provide a foundation on which an appropriate testing and commissioning process for the perimeter intrusion detection system can be built.