APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-SIS-RP-15-13
Approved June 28, 2013
Infrastructure Security Working Group

Equipment and Technology for Public Transit

Abstract: This document proposes recommended practices for security equipment and technology at transit passenger facilities to enhance the security of people, operations, assets and infrastructure.

Keywords: assessment, balanced security, considerations, equipment, technology, security program

Summary: This *Recommended Practice* provides equipment and technology strategies and background information. It offers an overview and description of the applicability of the equipment and technology pillar. This *Recommended Practice* discusses several elements of equipment and technology, as well as other security standards and best practices used by transit agencies to enhance their security program(s).

Scope and purpose: This *Recommended Practice* is the part of the "Security Program Considerations" series of infrastructure security *Recommended Practices* and white paper documents prepared for used by the transit industry. Other infrastructure security specific program topics developed for this series address the four pillars of security—physical security, operations, planning, and equipment and technology—that will also be provided to the transit industry for consideration and use.

Participants

The American Public Transportation Association greatly appreciates the contributions of **Bill Pitard**, who provided the primary effort in the drafting of this *Recommended Practice*.

At the time this standard was completed, the working group included the following members:

Sean Ryan, MNR, *Chair*
Randy Clarke, MBTA, *Vice Chair*

Gabriela Amezcua, *CTA*
Brad Baker, *MBTA*
Jevon D'Souza, *TSA*
Rick Gerhart, *FTA*
David Hahn, *APTA*
Eric Hartman, *OCTA*
Mark Mahaffey, *VTA*
Chris McKay, *TSA*
Bill Pitard, *STV Inc.*
John Plante, *CTA*
Charles Rappleyea, *CATS*
Harry Saporta, *TriMet*
Allen Smith, *SPAWAR*
Brian Taylor, *Halifax*
Eric Ebert, STV Inc.

Contents

Equipment and Technology for Public Transit

1. Introduction

Public transit operates in inherently open environments. It provides ease of access and gathers volumes of people in confined spaces to provide passengers with efficient and convenient transportation through regions and their communities. These unique attributes make public transportation vulnerable to adversarial targeting and threats. For these reasons, a sound understanding of the elements of the physical security pillar is necessary to assist agencies to implement approaches to effectively manage the risks of their environments.

While transit security programs may implement or operate using different types of strategies, measures or solutions, a "Security 101" philosophy or a basic level of appropriate strategies should be understood to reduce risk and enhance the posture of all transit properties. The "Security Program Considerations" series of infrastructure security *Recommended Practices* prepared for transit passenger facilities provides such information (see **Table 1**).

TABLE 1
APTA Security Standards Program Documents

APTA Number	Recommended Practice Title
APTA SS-SEM-RP-004-09	"General Guidance on Transit Incident Drills and Exercises"
APTA SS-SRM-RP-001-09	"Security and Emergency Preparedness Plan (SEPP)"
APTA SS-SIS-RP-001-10	"Security Lighting for Transit Passenger Facilities"
APTA SS-SIS-RP-002-10	"Security Lighting for Nonrevenue Transit Passenger Facilities"
APTA SS-SIS-RP-003-10	"Fencing Systems to Control Access to Transit Facilities"
APTA SS-SIS-RP-004-10	"Chain Link, Mesh, or Woven Metal Fencing Systems to Control Access to Transit Facilities"
APTA SS-SIS-RP-005-10	"Gates to Control Access to Transit Facilities"
APTA SS-SIS-RP-006-10	"Ornamental Fencing Systems to Control Access to Transit Facilities"
APTA SS-SIS-RP-007-10	"Crime Prevention Through Environmental Design for Transit Facilities"
APTA SS-SIS-RP-008-10	"Bus Stops Design and Placement Security Considerations"
APTA IT-CCTV-RP-001-11	"Closed Circuit Television System (CCTV)"
APTA SS-SIS-RP-009-12	"Anti-Vehicle Barriers for Public Transit"

2. Equipment and technology pillar overview

The equipment and technology pillar incorporates some or all elements of any one or several pillars together into a system that provides a uniform approach to applying a security solution. However, equipment and technologies described in this *Recommended Practice* may also be used as standalone systems. When effectively applied, these elements provide an agency with resources to mitigate risk and to operate a balanced and effective security program.

Adversaries may target people, operations, assets and infrastructure in the transit environment. To reduce the risk from these threats, the effective implementation of equipment and technology should be considered.

Examples of similarly structured *Recommended Practice* documents that describe a broad scope of infrastructure security and derivative topics are described in **Table 1**. Other Security Standards Program documents are also listed as resources herein to aid the development of a balanced security program and should be used where applicable by accessing APTA's Security Standards and Recommended Practices page at http://www.apta.com/resources/standards/Pages/Security-Standards.aspx

2.1 Stakeholder considerations

Transit agencies should understand and buy in to transit equipment and technology to enhance the security posture of the environments where they must operate. To the extent possible, the application of any or all of the topics of this *Recommended Practice* should be considered to assist agencies to meet their security program requirements and to enhance their safe operations.

2.2 Benefits

An agency's security program that includes equipment and technology provides its people, operations, assets and infrastructure the following benefits:

- Fosters transit domain awareness (TDA)
- Creates pride of ownership by transit users and employees
- Ensures transit agencies of a capability to deter, detect, delay, respond to and mitigate, where appropriate, in response to security events or incidents
- Enhances the safety and security experience of its ridership within the transit environment

3. Security risk assessment

Transit agencies should complete a systemwide security risk assessment to determine exposure to their systems' people, assets, operations and infrastructure. A risk-based approach that factors threat, vulnerability and consequence should be used to assess transit systems. The findings should be used to select security measures that mitigate risk to and enhance the protection of people, assets, operations and infrastructure. For more information regarding various Security Risk Assessment methodologies, see the following:

- National Infrastructure Protection Plan (U.S. Department of Homeland Security [DHS])
- FEMA 452 – Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks (Federal Emergency Management Agency [FEMA])
- A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (American Association of State Highway and Transportation Officials [AASHTO])
- Public Transportation System Security and Emergency Preparedness Planning Guide (Federal Transit Administration [FTA])
- Security Vulnerability Assessment Methodology for Petroleum and Petrochemical Industries, (National Petrochemical & Refiners Association [NPRA])
- Risk Analysis and Security Countermeasure Selection. T.L. Norman, 2010. CRC Press, Boca Raton, FL.
- Code of Practice on Conducting Security Risk Assessments of Rail and Transit Operations (Government of Canada, Transport Canada, 2010)
- Security Risk Assessment for Transport Operators (Government of Australia, Department of Transport, State of Victoria, 2012)

4. Security equipment and technology

The equipment and technology pillar delineates security-specific information and functions. For instance, the application of equipment and technology capabilities to deter, detect, delay and respond to security incidents or events, thereby offering a level of protection to people, operations, assets and infrastructure.

4.1 Types of equipment and technology

4.1.1 Transit domain awareness

A key component of an active, layer-protected and balanced security program, TDA is the effective understanding of activities within or associated with the transit domain that could impact the security, safety, economy or environment of an agency. TDA is supported by other agency physical security, plans, operations and equipment and technology, some of which are described below.

4.1.2 Electronic security systems

An electronic security system (ESS) (see **Figure 1**) provides early warning of an internal or external intruder by combining the functions or deterrence with detection, delay and response, coupled with people, procedures and equipment to meet the agency's security system objectives. ESS consists of hardware and software operated by trained personnel. An ideal system, for example, would include an access control system (ACS), an intrusion detection system (IDS) and a video surveillance system (VSS) integrated as a single physical protection system. To attain balanced protection, an agency should designate protection zones throughout its property and, by applying the basic principles of security (deter, detect, delay and respond), integrate layers of protection through deployment of ESS to mitigate risk. An ESS checklist is provided in Appendix B for agency users to understand and identify important elements of an ESS.

> **NOTE:** VSS is formerly known as CCTV.

4.1.3 Access Control System

An ACS manages access to specifically designated areas of facilities. The basic ACS sequence shows the user presenting the access medium (credential) for authentication; the central processing unit (CPU) compares the credential with the ACS enrollment database, the credential is validated and authorizes access, and then the CPU unlocks the controlled door permitting entry to the authorized user (**Figure 2**). Authorized people may be employees, contractors or visitors.

At a minimum, components of an ACS should include an enrollment station (camera, CPU with database), credentials (key card/badge), card readers (swipe, proximity or code/identity), electric locks and the capability to record authorized, unauthorized and attempted access control events.

4.1.3.1 Credentials

ACS credentials are based on one or more of the following principles:

- **What you have.** An ACS credential (key card/badge).
- **What you know.** A personal identification number (PIN).
- **Who you are.** A personal attribute (e.g., fingerprint, other biometrics)

FIGURE 1
Basic Electronic Security System (ESS) Overview

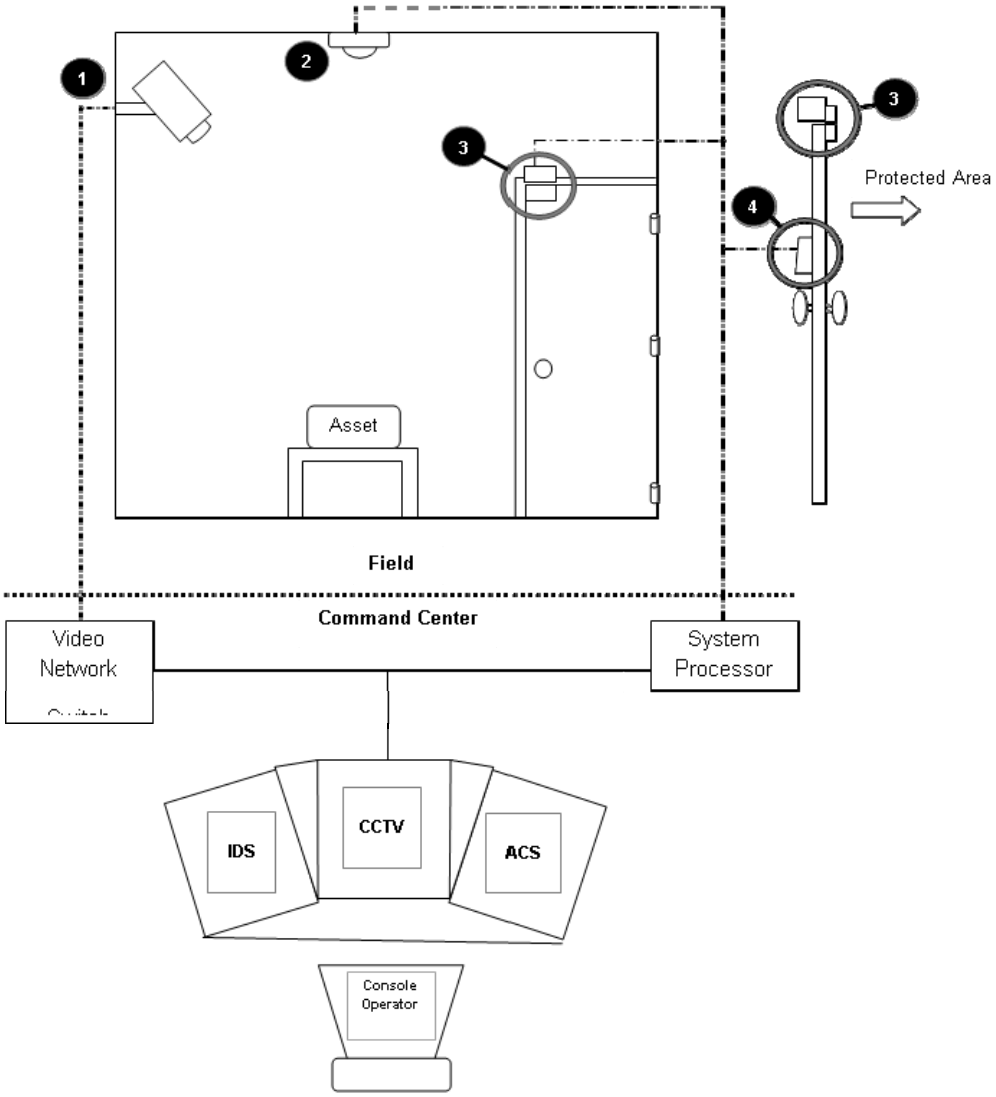
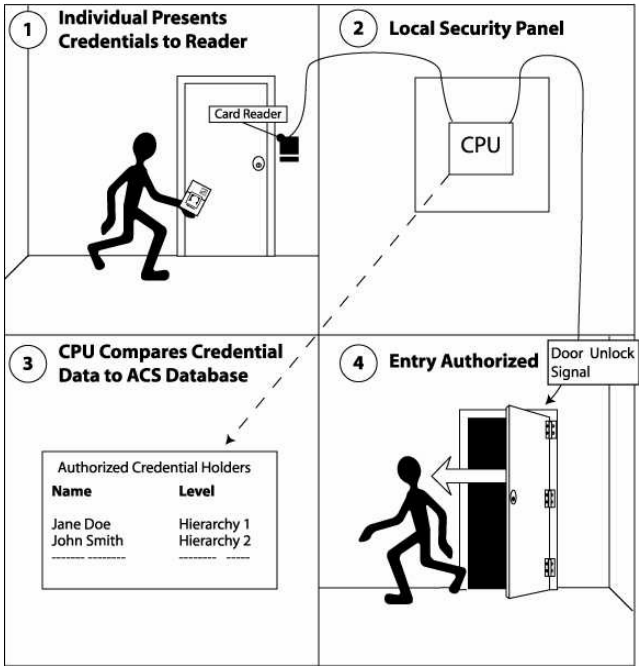


FIGURE 2
Basic Access Control System (ACS) Sequence



All ACS credentials must be controlled and designed to prevent counterfeit. The access medium and a current picture of the user should be combined into the same credential. The user's picture should include a view from the shoulders to the top of the head, be colored and be heat laminated into the credential. The user's name, organization and an expiration date should be printed in a viewable font on the front of the credential and be visible from at least 4 ft away. Include "Return if Found" information (e.g., address and contact) on the access medium to enhance its recovery if lost. An ACS medium should also be integrated with VSS and IDS to monitor time and attendance, providing authorized users access to authorized areas without activating an alarm. Similar applications may be applied to vehicle gates or fencing, doors and other access openings.

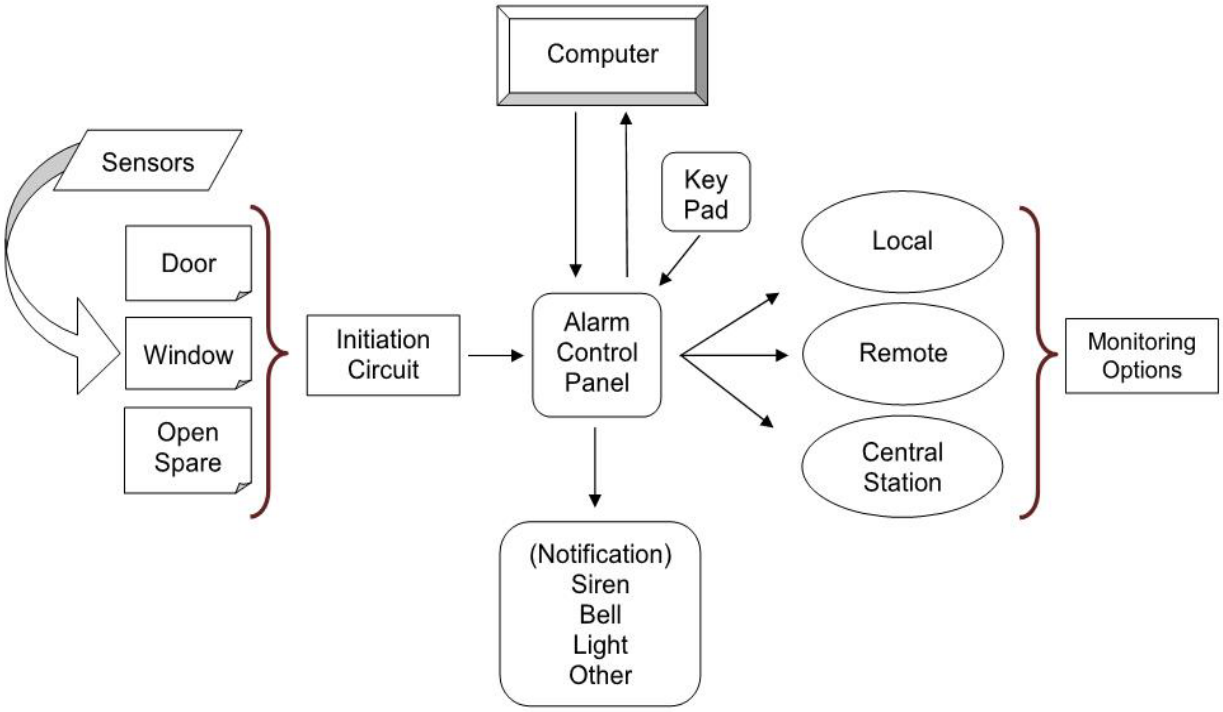
4.1.4 Intrusion Detection System

An IDS (**Figure 3**) combines detection sensors (e.g., door, window, etc.) with a computer, an alarm control panel, and a power source to detect unauthorized entry into a protected area and to provide notification (e.g., alarm, siren) that a breach has occurred. IDS may also be integrated with the appropriate ACS and VSS interfaces to detect one or more types of intrusion into protected areas. The nomenclatures of interior and exterior sensors, respectively, are described in **Table 2** and **Table 4** (Appendix A). A description of IDS components and functions follows:

4.1.4.1 Sensors

Sensors are devices that are used to detect and monitor events or activities in protected areas under various conditions. They detect changes that occur to the specific operating conditions for the area they protect (door, window, etc.) There are numerous detection sensors available that offer monitoring and detection capabilities. Sensors have interior and exterior applications and can be active or passive, covert or visible, volumetric or line sensing.

FIGURE 3
Basic IDS Sequence



Specifically:

- Active sensors transmit a signal and detect a change in the signal; passive sensors only receive energy to generate a signal.
- Passive sensors simply detect energy emitted in the proximity of the sensor; they do not produce a signal from the transmitter.
- Covert sensors are hidden from view, whereas visible sensors are openly displayed and may act as visual deterrents to an adversary.
- Where volumetric sensor are capable of detecting motion in designated detection zones, larger areas rooms, closets and other interior spaces or areas, line sensors detect intrusion in specific areas of the designated detection zone.

Detection sensor application should be designed, specified and tailored to detect intrusion by surveying the environment, weather, seismic, natural hazards, wildlife and other conditions of the areas where the device(s) will be installed. The challenges associated with interior and exterior sensors, respectively, are described in **Table 3** and **Table 5** (Appendix A).

4.1.4.2 Initiation circuit

Any event or action that results in an alarm device initiating an alarm status, such as a pull station, a volumetric sensor, a door switch, etc.

4.1.4.3 Computer

The computer is the central hub of an IDS. It provides monitoring, display, acknowledgement and control capabilities of the protected zone alarm sensor points.

4.1.4.4 Alarm control panel

An alarm control panel is the system's main component. It operates either in a standalone or in a networked mode. It is designed to accept input from various detection sensors and to monitor their circuitry for abnormal operation. Generally, control panels have connections for power supplies, batteries, bell outputs, programmable outputs, communication buses and a fixed number of input zones for connecting the detection devices. The battery backup for the IDS system is typically located in the alarm control panel.

4.1.4.5 Keypad

The keypad enables commands to be entered into the alarm control panel (user codes, silencing alarms, arming and disarming zones, etc.). It also provides system status, such as violated devices or zones, trouble signals, etc. Keypads may use a sound, such as a bell, chime or buzzer, to provide notice of a change in the state of the system. Keypads should be placed in areas that are readily accessible by the user, typically at the primary entrance to an area. Most systems allow multiple-unit keypad installation at multiple entrances or where they can be monitored by response personnel.

4.1.4.6 Notification

Notifications are preset options designed to indicate an alarm status in a protected zone by way of an audible or visual device. Notification of an alarm status may include, but is not limited to, siren, lights, bells and other devices.

4.1.4.7 Monitoring

ESS systems are most effective when monitored by exception in real time. This means that alarm monitoring system settings should be programmed to cause an alarm annunciation when an undesirable act takes place. Rapid response to activities or events in real time can provide a return on investment for a transit organization by addressing alarms as they occur. The typical types of alarm status monitoring follow:

- **Local alarms** are simple alarms. Typically they are installed on the exterior of the structure and are used for low-value assets. By using this method, alarms initiate an audible and/or visible signal, typically at the facility or building where the IDS are installed. Local alarm annunciation relies on security or police patrols, passersby or building occupants returning to the structure to acknowledge the alarm status.
- **Remote monitoring of systems** consists of alarm activations being monitored, transmitted to and annunciated at a local (contracted) security company or local police dispatch center that also records the alarm annunciation. A contracted service or a formal agreement with local police may be required to ensure monitoring and response.
- **Central-station monitoring** includes proprietary devices and circuits that are automatically signaled to, recorded at, maintained by and supervised from an agency's owned central location with operators who monitor the system continuously. This type of monitoring is typically performed by contractors and/or in-house agency staff.

4.1.5 Video surveillance system

The CCTV *Recommended Practice* (http://www.apta.com/resources/standards/Pages/IT-Standards.aspx) provides guidance on CCTV systems for transit facilities. See **Table 1** for a list of APTA *Recommended Practices*. VSS works with other technologies to provide verification of system events.

4.1.6 Emergency call stations

Emergency call stations (ECS) provide ridership with a direct link from a point within the transit environment to a security operator. ECS are designed for installation at a variety of areas and to withstand the physical environment and operational conditions encountered.

ECS operate from various power sources, such as 120 AC or 12 V DC service or solar power. ECS may also be scheduled to operate during specific days, hours or times via a controller or timer. Specific means of communication may also vary based on availability within a planned service area or areas. For example, ECS can be designed to communicate via landline phone service, cellular tower service, two-way radio, Voice Over Internet Protocol (VoIP), WiFi-VoIP (wireless), or over a 900 MHz bandwidth. At a minimum, the following functional capabilities should be considered in the design of an ECS:

- Backup power and communication sources to ensure continuous ECS operation and connectivity during utility and service outages
- Call-back (aka ring-back) function to reconnect and communicate with the caller's site in the event of a disconnected or dropped call

Additionally, various options may be available when considering requirements for an ECS. They may include cameras, audio siren, auto dial, continuously open microphones, synchronization with other ECS cameras to capture different angles and images of the area, signs designating the location of ECS devices, etc. If a CCTV option is designed into the ECS, then cameras should be installed to synchronize their fields of view to the area of the activated ECS site to verify the caller, the nature of the call, the site, activities in the area of the caller, etc. An agency should always consider the indigenous languages spoken and other means of communications used in the communities they serve to ensure that the services and instructions of an ECS are well understood and that their locations are clearly identified.

Adequate due diligence should precede any proposed procurement and installation of security equipment and technology by an agency. For example, an agency should first complete a security risk assessment to determine if a requirement exists for the equipment and technology to be installed at their properties (see **Table 1** and Section 3). Then, a site survey should be completed to identify other requirements at the site, such as the Americans with Disabilities Act, OSHA requirements, local codes or ordinances, enablers (ridership volumes and pedestrian circulation) or challenges, utility service, installation location(s), etc. Finally, operation testing of functions should be performed before acceptance of the equipment and technology and its commissioning into service.

ECS policies and procedures should be prepared, exercised and implemented to validate an accurate, timely and effective response.

5. Training considerations

ESS system operators should attend manufacturers' basic and refresher training for the systems they operate.

6. Maintenance considerations

Follow each ESS manufacturer's recommended annual, quarterly and/or periodic maintenance schedule to maintain each system's optimum functionality. Also, the transit agency's bid review process may include contacting identified customers to ascertain performance and other service data about the bidder's product. When advertising for bids from manufacturers, specifications should include a requirement that the bid response include a list of customers that have purchased/installed the bidder's product.

Appendix A: Tables

TABLE 2
Interior Sensor Nomenclature

Boundary Penetration Sensors				
Electromechanical (contacts)	P	C/V	L	• Magnetic reed switch • Balanced magnetic switch • Hall effect switch • Break wire grid and screens
Infrared	P/A	V	L	• Infrared light sources for transmitters • Photo detectors for receivers
Vibration	P	C/V	L	• Glass breakage (frequencies above 20 kHz) • Fiber op cable (can be set to detect vibration)
Capacitance	P	C	L	• Most common proximity type
Fiber optic cable	P	C/V	L	• Proximity sensor or vibration • Continuity sensor; senses damage or breakage • Microbend sensor; senses movement and pressure
Interior Motion Sensors				
Microwave	A	V	V	• Typically monostatic configuration • Senses Doppler frequency changes • Optimum detection: away or toward
Ultrasonic	A	V	V	• Monostatic (Acoustic frequency 19–40 kHz) • Bi-static combined with Doppler
Sonic	A/P	V	V	• Sonic (microphone sound change sensing)
Infrasonic	P	V	V	• Volume change sensing
Passive infrared (PIR)	P	V	V	• Thermopile and pyroelectric detector • Senses background thermal energy changes • Optimum detection; pass across detection patterns
Dual technology motion sensors	P/A	V	V	• Microwave combined with PIR
Video motion detection	A	V/C	L	• Detects changes in grayscale • Analog or digital formats
Proximity Sensors				
Capacitance	A/P	C/V	L	• Senses approaching person(s) or touch • Fiber optic cable sensor
Pressure	P	C	L	• Wireless sensors • Pressure mats

P: Passive *A: Active* *C: Covert* *V: Visible* *L: Line*

TABLE 3
Interior Sensor Challenges

Type	Wind	Temp	RH	Small Animals/ Wildlife	Electrical Interfere Lightning	Power	Radio Frequency	Seismic
Boundary Penetration Sensors								
Active glass break	L	VL	VL	VL	L	L	L	L
Continuity	VL	VL	VL	VL	VL	VL	VL	VL
Simple magnetic switch	VL	VL	VL	VL	L	L	L	L
Balanced magnetic switch	VL	VL	VL	VL	L	L	L	LM
Passive ultrasonic	M	L	L	MH	L	L	L	L
Vibration	LM	L	L	L	L	L	L	H
Fiber-optic	LM	L	VL	VL	VL	VL	VL	LM
Volumetric Sensors								
Active sonic	M	L	L	L	L	L	L	L
Microwave	L	L	L	M	M	M	M	L
PIR	L	H	L	M	M	M	M	L
Ultrasonic	L	L	M	M	M	M	M	L
Video motion	L	L	L	M	M	M	M	L
Proximity Sensors								
Capacitance	L	L	M	M	M	L	L	LM
Pressure	L	L	L	L	L	L	L	L
Fiber optic	L	L	L	M	VL	VL	VL	M

VL: Very low *L: Low* *M: Medium* *H: High*

TABLE 4
Exterior Sensors Nomenclature

Type	Passive (P) or Active (A)	Covert (C) or Visible (V)	Line of Sight (LOS) or Terrain Following (TF)	Volumetric (VOL) or Line (L)
Buried Line				
Seismic pressure	P	C	TF	L
Magnetic field	P	C	TF	VOL
Ported coaxial cable	A	C	TF	VOL
Fiber optic cable	P	C	TF	L
Fencing Associated				
Fence disturbance	P	V	TF	L
Sensor fence (taut wire)	P	V	TF	L
Electric fence	A	V	TF	VOL
Free-Standing				
Active infrared	A	V	LOS	L
Passive infrared	P	V	LOS	VOL
Bi-static microwave	A	V	LOS	VOL
Dual technology	A/P	V	LOS	VOL
Video motion detection	P	C	LOS	VOL

TABLE 5

Exterior Sensor Challenges

Sensor Type	Wind	Rain	Standing Water/Runoff	Snow	Fog	Small Animals	Large Animals	Small Birds	Large Birds	Lightning	Overhead Power Lines	Buried Power Lines
Fence mounted	H	M	L	L	VL	L	M	L	L	L	VL	VL
Taut wire	VL	VL	VL	VL	VL	VL	L	VL	VL	VL	VL	VL
Electric field	M	LH	VL	M	VL	M	VH	L	M	M	L	VL
Capacitance	M	M	VL	M	VL	M	VH	L	M	M	L	VL
Ported cable	VL	M	H	L	VL	VL	M	VL	VL	M	VL	L
Seismic/pressure	M	L	L	L	VL	L	VH	VL	VL	L	L	M
Seismic/magnetic	M	L	L	L	VL	L	VH	VL	VL	H	M	H
Microwave	L	L	MH	LM	L	MH	VH	VL	M	LM	L	VL
Infrared (IR)	L	L	L	M	M	M	VH	L	M	L	VL	VL
Video motion	M	L	L	L	MH	L	VH	VL	M	L	L	VL

VL: Very low *L: Low* *M: Medium* *H: High* *VH: Very high*

Appendix B: ESS Checklist

☐	1. What are the primary goals/objectives for this project?
☐	2. What is the purpose of the system or systems?
☐	3. Will the system be standalone or integrated with other systems? ☐ IDS ☐ ACS ☐ VSS (check all applicable systems)
☐	4. Will the systems be used on a daily basis? Describe how.
☐	5. Has a site survey been completed?
☐	6. Were specific area needs addressed and reviewed, such as property, safety, liability, security, efficiency, lighting and other?
☐	7. Have the number(s) of different structures to be included with the system(s) been identified?
☐	8. Have the distances between structures been measured?
☐	9. Were the method of transmission for data, video and power identified and located at the site?
☐	10. Does video or data need to be recorded?
☐	11. Has periodic maintenance of the system been identified?
☐	12. Has the person responsible for the system after installation been identified?
☐	13. Do the system's operators/administrators require system training?

References

American Association of State Highway and Transportation Officials (AASHTO), "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection." http://highwaytransport.transportation.org/Documents/NCHRP_B.pdf

American Public Transportation Association (APTA) *Recommended Practices*:
APTA IT-CCTV-RP-001-11: "Closed Circuit Television System (CCTV)"
APTA SS-SIS-RP-001-10: "Security Lighting for Revenue Transit Facilities"
APTA SS-SIS-RP-002-10: "Security Lighting for Nonrevenue Transit Facilities"
APTA SS-SIS-RP-003-10: "Fencing Systems to Control Access"
APTA SS-SIS-RP-004-10: "Chain Link, Mesh or Woven Fencing Systems to Control Access"
APTA SS-SIS-RP-005-10: "Gates to Control Access"
APTA SS-SIS-RP-006-10: "Ornamental Fencing Systems to Control Access"
APTA SS-SIS-RP-007-10: "Crime Prevention Through Environmental Design for Transit Facilities"
APTA SS-SEM-RP-004-09: "General Guidance on Transit Incident Drills and Exercises"
APTA SS-SRM-RP-001-09: "Security and Emergency Preparedness Plan (SEPP)"

APTA Security Emergency Management series. http://www.apta.com/resources/standards/Pages/Security-Standards.aspx. ASIS International, "International Glossary of Security Terms." www.asisonline.org/library/glossary/index.xml

Department of Homeland Security (DHS), National Terrorism Advisory System. www.dhs.gov/files/programs/ntas.shtm

DHS, National Infrastructure Protection Plan. www.dhs.gov/nipp

Federal Emergency Management Agency (FEMA), FEMA 452 - Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks.www.fema.gov/plan/prevent/rms/rmsp452.shtm

Federal Transit Administration (FTA), "An Introduction to All-Hazards Preparedness for Transit Agencies," (2010). http://www.fta.dot.gov/documents/SMPM_Instruction_Manual.pdf

FTA, "Public Transportation System Security and Emergency Preparedness Planning Guide" (2003). http://transit-safety.volpe.dot.gov/publications/security/PlanningGuide.pdf

National Petrochemical & Refiners Association (NPRA), "Security Vulnerability Assessment Methodology for Petroleum and Petrochemical Industries, 2nd Ed." www.npra.org/docs/publications/newsletters/sva_2nd_edition.pdf

National Transit Institute (NTI), "Terrorist Activity Recognition and Reaction." www.ntionline.com/courses/courseinfo.php?id=128

Norman, Thomas L., CPP, PSP, CSC, *Integrated Security System Design: Concepts, Design, and Implementation* (Butterworth-Heinemann, Burlington, MA, 2007).

Norman, Thomas L., CPP, PSP, CSC, *Risk Analysis and Security Countermeasure Selection,* (CRC Press, Boca Raton, FL, 2010).

Transportation Security Administration (TSA)/FTA, "Security and Emergency Management Action Items for Transit Agencies." www.tsa.gov/assets/pdf/mass_transit_action_items.pdf Rail PAX

Definitions

all-hazards preparedness: An integrated planning and capability building for safety, security and emergency management to optimize and continuously improve the use of resources and the management of risks from hazards, threats, vulnerabilities and adverse events or incidents for transit agencies.

access control: An aspect of security that often uses hardware systems and specialized procedures to manage and monitor movement into, out of or within a specific protected area. Access to various areas may be limited by need to know, place, time or a combination of all.

clear zone: An area that is clear of visual obstructions and landscape material that could conceal a threat or perpetrators, e.g., the space immediately adjacent to and around an inhabited building without obstructions large enough to conceal explosives 6 in. or greater in height.

crime prevention through environmental design (CPTED): A crime-prevention philosophy based on the theory that proper design and effective use of the built environment can lead to a reduction in the fear of and incidence of crime, as well as an improvement in the quality of life.

deter: Making a target inaccessible or difficult to defeat through the use of small hand tools (hammer, drills, electric power tools, etc.) or by using a specific tactic to bypass a security system.

detect: The act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter (such as scaling a fence, opening a locked window, or entering an area without authorization).

delay: To impede penetration into a protected area.

entry control: The control of people, vehicles and materials through entrances and exits of a protected area; equipment or technology that channels, restricts or controls entry to an area, space or location.

evacuation: Organized, phased and supervised dispersal of people from dangerous or potentially dangerous areas.

first responders: Local police, fire and emergency medical personnel who first arrive at the scene of an incident and take action to save lives, protect property and meet basic human needs.

forced entry: Entry to a denied area achieved through force to create an opening in fencing, walls, doors, etc., or to overpower guards.

layers of protection: Using concentric circles extending out from an area to be protected as demarcation points for different security strategies.

notification: Capability to provide real-time information to all building or asset occupants or personnel in the immediate vicinity of the building or asset during emergency situations.

public access area: An area of a facility where public access is not restricted or prohibited.

response: Employees, guards or law enforcement representatives who deploy to investigate a detection event or to interdict an intruder or trespasser.

restricted area: An established area requiring a higher degree of security to protect sensitive and/or high-value assets kept therein.

standoff distance: The distance between an asset or building or a portion thereof (target) and the potential location of an explosive device (threat).

target: An object, background or reflector at which something (i.e., a threat) is aimed.

target hardening: Using physical barriers or changes in a location to reduce the opportunity for crime and to make the completion of a crime more difficult.

threat: Any indication, circumstance or event with the potential to cause loss of or damage to an asset.

transit domain awareness (TDA): The awareness and understanding of activities within or associated with the transit domain that could impact the security, safety, economy or environment of an agency. It is a key component of an active, layer-protected and balanced security program that is supported by other agency plans and activities.

Abbreviations and acronyms

AASHTO	American Association of State Highway and Transportation Officials
AC	alternating current
APTA	American Public Transportation Association
ACS	access control system
CCTV	closed-circuit television
CPTED	crime prevention through environmental design
CPU	central processing unit
DC	direct current
DHS	Department of Homeland Security
ECS	emergency call stations
ESS	electronic security system
FEMA	Federal Emergency Management Agency
FTA	Federal Transit Administration
IDS	intrusion detection system
kHz	kilohertz
MHz	megahertz
NPRA	National Petrochemical & Refiners Association
NTAS	National Terrorism Advisory System
NTI	National Transit Institute
PIR	passive infrared
TDA	transit domain awareness
TSA	Transportation Security Administration
V	volt
VSS	video surveillance system

