



RAPID TRANSIT SYSTEM EXTENSIONS
COMPENDIUM OF DESIGN CRITERIA

VOLUME I
SYSTEMWIDE DESIGN CRITERIA

CHAPTER 8
SYSTEM SECURITY DESIGN CRITERIA

INTERIM RELEASE
REV 1

OCTOBER 30, 2008

PROGRAM MANAGEMENT CONSULTANT

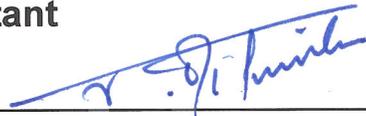
– Intentionally Left Blank –

VOLUME I – SYSTEMWIDE

CHAPTER 8 – SYSTEM SECURITY DESIGN CRITERIA

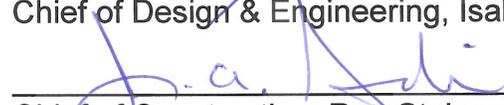
REVISION 1

Program Management Consultant

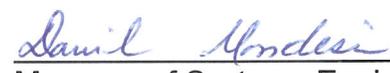
Submitted  Date 4/16/2009
Project Manager, Soji Tinubu

**Miami-Dade Transit
Engineering Review Board Members**

Approval  Date 4-16-09
Chief of Design & Engineering, Isabel Padrón

FOR  Date 4/16/09
Chief of Construction, Ron Steiner

 Date 4-16-09
Chief of Safety, Eric Muntan

 Date 4/16/09
Manager of Systems Engineering, Daniel Mondesir

Director Approval

Approval  Date 4/20/09
Deputy Director, Albert A. Hernandez

Approval  Date 06/01/09
MDT Director, Harpal Kapoor

– Intentionally Left Blank –

DOCUMENT REVISION RECORD

ISSUE NO.	DATE	REVISION DESCRIPTIONS
0	9-26-07	Interim Release
1	10-30-08	Revisions to conform with MIC-EH design

ISSUE NO.	SECTIONS CHANGED
1	No changes made to this chapter in this revision.

– Intentionally Left Blank –



VOLUME I – SYSTEMWIDE CRITERIA
 CHAPTER 8 - SYSTEM SECURITY CRITERIA
 REVISION 1

Table of Contents	Page No.
8.1 SYSTEMWIDE SECURITY DESIGN CRITERIA.....	1
8.1.1 GENERAL	1
8.1.2 SECURITY STRATEGY	3
8.1.2.1 LEVEL OF PROTECTION.....	4
8.1.2.2 IDENTIFY AND SELECT COUNTERMEASURES.....	4
8.1.2.3 EVALUATE COUNTERMEASURES.....	5
8.1.2.3.1 Performance Characteristics	5
8.1.2.3.2 Proven Track Record in a Transit Environment	5
8.1.2.3.3 Future Agency Needs	6
8.1.2.3.4 Families of Technologies	6
8.1.2.4 ACCESS MANAGEMENT	7
8.1.2.4.1 Access Management Guidelines	7
8.1.2.4.2 Access Management Parameters.....	7
8.1.2.4.3 Challenges in the Transit Environment.....	8
8.1.2.4.4 Access Management as Part of a Comprehensive Security Plan	10
8.1.2.4.5 Access Management Concepts.....	10
8.1.2.4.5.1 Crime Prevention Through Environmental Design (CPTED)	10
8.1.2.4.5.2 Access Control	11
8.1.2.4.5.3 Intrusion Detection and Surveillance	11
8.1.2.4.5.4 Layered Security.....	12
8.1.2.4.5.5 Systems Integration.....	13
8.1.2.4.6 Tools/Techniques	14
8.1.2.4.6.1 Policies and Procedures.....	15
8.1.2.4.6.2 Perimeter Protection and Barriers	15
8.1.2.4.6.3 Entry-Point Screening.....	17
8.1.2.4.6.4 Credentials and Credentialing	18
8.1.2.4.6.4.1 Credentials.....	18
8.1.2.4.6.4.2 Credentialing.....	19
8.1.2.4.6.5 Surveillance Systems	20
8.1.2.4.6.6 Intrusion Detection.....	22
8.1.2.4.6.7 Security Personnel	22
8.1.2.4.6.8 Communication and Information Processing Systems	23
8.1.2.5 LIGHTING	24
8.1.2.5.1 Security Lighting.....	24
8.1.2.5.1.1 Perimeter Lighting	27
8.1.2.5.1.2 Entry, Guardhouse, and Parking Lot Lighting.....	27
8.1.2.5.1.2.1 Entry/Guardhouse.....	27
8.1.2.5.1.2.2 Parking Lot Areas	28

8.1.2.5.1.2.3	Emergency Power and Backup Power	29
8.1.2.5.1.3	Types of Lighting	29
8.1.2.5.1.3.1	Continuous Lighting	30
8.1.2.5.1.3.2	Standby Lighting	30
8.1.2.5.1.3.3	Moveable Lighting.....	31
8.1.2.5.1.3.4	Emergency Lighting	31
8.1.2.5.2	Vehicle Access Control and Parking.....	32
8.1.2.5.2.1	Vehicle Inspection	33
8.1.2.5.2.2	Facility Parking/Traffic Control.....	33
8.1.2.5.2.3	Adjacent Parking	35
8.1.2.5.2.4	Parking Registration / Vehicular Identification Systems.....	35
8.1.2.5.2.5	Towing of Unauthorized Vehicles	35
8.1.2.5.2.6	Vehicle Access Points	35
8.1.2.5.2.7	High-Speed Vehicle Approaches.....	36
8.1.2.5.2.8	Drive-Up / Drop Off Locations	37
8.1.2.5.3	Vehicle Barriers	37
8.1.2.5.3.1	Barrier Use	38
8.1.2.5.3.2	Applications in a Transit Environment	38
8.1.2.5.3.2.1	Vehicle Speed.....	40
8.1.2.5.3.2.2	Vehicle Stops.....	41
8.1.2.5.3.2.3	Vehicle Restriction	41
8.1.2.5.3.2.4	Traffic Direction.....	41
8.1.2.5.3.2.5	Revenue Collection.....	41
8.1.2.5.3.2.6	Theft Deterrence.....	41
8.1.2.5.3.3	Barrier Types.....	41
8.1.2.5.3.4	Barrier Selection and Implementation.....	42
8.1.2.5.4	Critical and Restricted Area Access.....	42
8.1.2.5.4.1	Critical Operating Areas	42
8.1.2.5.4.2	Hazardous Areas and Security Areas.....	44
8.1.2.5.5	Windows	44
8.1.2.5.5.1	Construction	45
8.1.2.5.5.2	Steel Bars and Grills.....	45
8.1.2.5.5.3	Glass Brick	46
8.1.2.5.5.4	Glass and Steel Framework	46
8.1.2.5.5.5	Security Glazing	46
8.1.2.5.6	Sewers and Storm Drains.....	47
8.1.2.5.7	Rooftop Access Points.....	47
8.1.2.5.8	Air Intakes.....	48
8.1.3	SPECIFIC SECURITY CRITERIA	49
8.1.3.1	TRANSIT SYSTEM SECURITY LEVELS.....	49
8.1.3.2	ACCESS CONTROLS.....	54
8.1.3.2.1	Locking Devices	54
8.1.3.2.2	Control of Locks and Keys.....	55

8.1.3.2.3	Key Control Official	55
8.1.3.2.4	Records Requirements	55
8.1.3.2.5	Issue and Control Procedures	56
8.1.3.2.6	Lost and Unaccounted-for Keys and Electronic Access Cards	57
8.1.3.2.7	Locksets	57
8.1.3.2.8	Doors	57
8.1.3.2.8.1	Accessible Steel Grates and Doors	57
8.1.3.2.9	Door Hinges.....	58
8.1.3.2.10	Door Jambs.....	58
8.1.3.2.11	Fencing	58
8.1.3.2.11.1	Perimeter Fences	58
8.1.3.2.11.2	Clear Zones	60
8.1.3.2.11.3	Fence Fabric.....	61
8.1.3.2.11.4	Posts and Hardware	63
8.1.3.2.11.5	Openings	63
8.1.3.2.11.6	Gates.....	64
8.1.3.2.11.6.1	Perimeter Gates.....	64
8.1.3.2.11.6.2	Unattended/Inactive Gates.....	65
8.1.3.2.11.7	Wall/Roof Openings.....	65
8.1.3.2.11.7.1	Extending Interior Wall Construction to Ceiling or Roof Deck	66
8.1.3.2.11.7.2	Reinforced Wall.....	67
8.1.3.2.11.7.3	Intrusion-Detection Sensors.....	67
8.1.3.2.11.8	Miscellaneous Openings	67
8.1.3.2.11.9	Miscellaneous Fire Escapes.....	67
8.1.3.2.11.10	Miscellaneous Manholes	68
8.1.3.2.11.11	CCTV Cameras and Other Security Systems.....	69
8.1.3.3	LEVEL 1 SECURITY HARDWARE DEVICES	71
8.1.3.3.1	Locking Devices	71
8.1.3.3.1.1	Locksets	71
8.1.3.3.1.2	Doors.....	72
8.1.3.4	KEY CONTROL	72
8.2	SYSTEM PROCEDURES SECURITY CRITERIA.....	75
8.3	SYSTEM ELEMENT SECURITY DESIGN.....	83
8.3.1	STATION FACILITIES.....	83
8.3.1.1	GENERAL	83
8.3.1.2	STATION PERIMETER.....	83
8.3.1.3	ANCILLARY SPACES.....	84
8.3.1.4	VISIBILITY	84
8.3.1.5	CONCESSIONS.....	85
8.3.1.6	RESTROOMS	85
8.3.1.7	STATION PROTECTION	85
8.3.1.8	LIGHTING	86

8.3.1.9	LOCKERS	86
8.3.1.10	PARKING FACILITIES SECURITY	86
8.3.1.11	TRACTION POWER EQUIPMENT	89
8.3.2	GUIDEWAY FACILITIES.....	91
8.3.2.1	BARRIERS.....	91
8.3.2.2	EMERGENCY ACCESS	91
8.3.2.3	INTRUSION DETECTION.....	91
8.3.3	TRAIN CONTROL SECURITY	92
8.3.3.1	THE CENTRAL CONTROL FACILITY	92
8.3.3.2	SITE ANALYSIS.....	93
8.3.4	COMMUNICATION SECURITY	93
8.3.4.1	GENERAL	93
8.3.4.2	STATION COMMUNICATION.....	95
8.3.4.3	INTRUSION ALARMS.....	96
8.3.4.4	MONITORING.....	97
8.3.4.5	ELECTRONIC SURVEILLANCE (CCTV).....	98
8.3.5	PASSENGER VEHICLES	99
8.3.6	ADMINISTRATION FACILITY.....	99
8.3.7	MAINTENANCE FACILITIES SECURITY	101
8.3.8	LANDSCAPING	102
8.3.9	FARE COLLECTION.....	103
8.3.10	TRACKWORK.....	103
8.3.11	FIRE AND ACCESS CONTROL AND INTRUSION DETECTION MANAGEMENT.....	104
8.3.12	STATION ATTENDANT’S BOOTH.....	105
8.4	OTHER REFERENCE MATERIALS	107
	APPENDIX A: ACRONYMS	109
	APPENDIX B: DEFINITIONS	111
	APPENDIX C: SAMPLE THREAT AND VULNERABILITY ANALYSIS REPORT.....	117

8.1 SYSTEMWIDE SECURITY DESIGN CRITERIA

8.1.1 GENERAL

- A. These criteria describe the System Security design requirements for Miami Dade Transit (MDT) projects. This document should be used concurrently with Chapter 7 Systems Safety and Chapter 9 Fire/Life Safety Criteria.
- B. Optimum protection shall be provided to patrons, patron's property and employees from crime and harassment and to the transit property from loss, damage and vandalism. This begins with a consideration of MDT's overall security purpose; to maximize within the constraints of schedule, budget and operational effectiveness, the level of protection against potential harm afforded to passengers, employees, incidental occupants, contractors, responders, and other individuals who utilize the transportation system or are in the surrounding neighborhoods. This includes normative as well as emergency conditions.
- C. Public confidence in the protection of patrons and their property shall be engendered. Goals of the System Security Criteria include:
- Ensure that security and emergency preparedness are emphasized in all phases of the project, especially in the conceptual through final design stages.
 - Promote analysis tools and methodologies to encourage secure system operation through identification, evaluation and resolution of threats and vulnerabilities, and the ongoing assessment of agency capabilities readiness.
 - Provide a high quality transit system that, where practical, meets or exceeds industry guidelines as well as satisfies all Federal, State

- and local security and safety mandates.
- Increase and strengthen community involvement and participation in the security and safety of the system in the planning, construction and operations phases of the project.
- D. Intruders into critical, sensitive or controlled areas of the transit system shall be deterred or detected. The level of security should include countermeasures that will:
- Determine the appropriate levels of protection
 - Establish functional requirements
 - Analyze the necessary balance between cost, effectiveness, and efficiency while providing high quality service then identify and select countermeasures
- E. Fast and easy access for emergency services organizations to the transit system shall be provided. Develop an integrated approach to systems security and safety. This assures coordinated, team based efforts to identify, report, and eliminate security threats commencing in the design phase and beyond for MDT projects. Information will be shared, solicited and incorporated into designs as appropriate from internal as well as external contacts. These shall include the Fire Department, Police Department, Emergency Medical Services, Department of Homeland Security (DHS) and other safety and security based organizations.
- F. There shall be strict law enforcement and assistance in the vigorous prosecution of offenses on the transit system. Utilize design based efforts to develop an inventory of resources available for the MDT systems to contribute to the community during security and safety

related emergencies and natural disasters. Coordinate designs and communications with local responders, Federal Emergency Management Administration (FEMA), the Department of Homeland Security (DHS), National Guard and selected branches of the armed services.

G. All transit system structures shall be designed and constructed to protect against burglary, theft and sabotage. Vandal resistant design and/or material shall be used on the exterior of all structures and in all areas accessible to the public. The level of protection required for each asset should be matched with the level of threat. Factors to consider include:

- The importance of the asset
- The most likely method of attack
- The type of perpetrator
- The probability of attack
- The severity of the consequences

8.1.2 SECURITY STRATEGY

A security strategy lays out the actions that are necessary to move toward an integrated transit security system. An effective strategy is comprehensive and dynamic, with the flexibility to respond to any type or level of security threat. Accordingly, developing a security strategy is a process that involves initial assessment, planning, implementation, and constant evaluation.

It may include a combination of actions that counter possible threats and vulnerabilities, polices and procedures, access management measures, communications systems and technologies, and systems integration practices.

8.1.2.1 LEVEL OF PROTECTION

After assessing the problem, the level of protection for each asset should be determined matching the level of protection with the level of threat. Factors to take into account include the importance of the asset, the likely method of attack, the type of perpetrator of potential attacks, the probability of attack, and the severity of the consequences. Figure 8-1 is a simplified diagram depicting the degree of countermeasures as they correspond to various levels of threat.

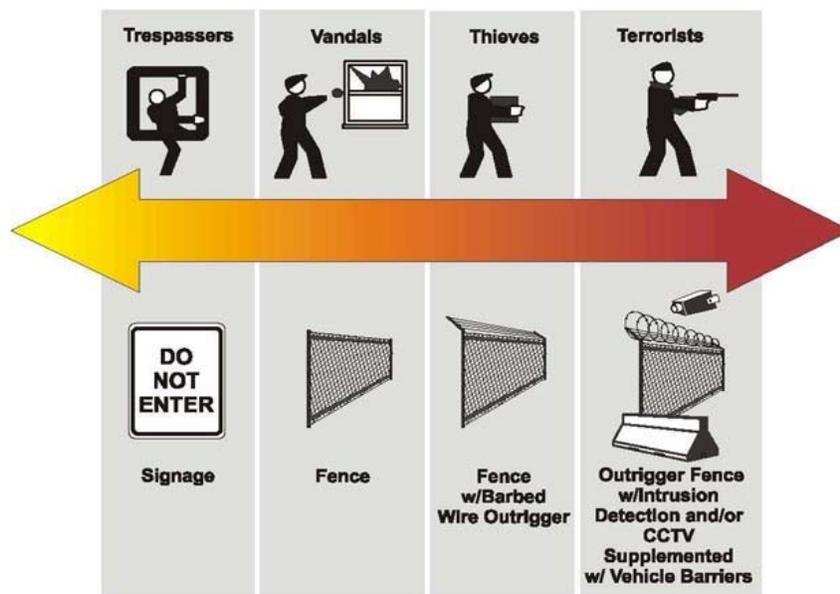


Figure 8-1: Corresponding Threats to Level of Protection

8.1.2.2 IDENTIFY AND SELECT COUNTERMEASURES

Security countermeasures can be technological or procedural and operational, and cover a wide range of sophistication, cost and level of integration. Consider measures that are feasible, that address the identified problems, and that work within the existing framework. Many countermeasures exist, and a complete feasibility assessment of a range of alternatives can generate solutions that best fit identified needs. Measures

such as staff training, appropriate facility design and well-planned procedures may prove more effective and economical in some circumstances than high tech admission control systems. It is likely that different parts of a single agency might rely on a combination of countermeasures to address multiple and conflicting requirements.

8.1.2.3 EVALUATE COUNTERMEASURES

Consider the following factors when selecting and evaluating countermeasures: performance characteristics, proven track record in a transit environment, future MDT needs, family of technologies, and cost efficiencies.

8.1.2.3.1 Performance Characteristics

Security systems need to have a high degree of reliability. MDT should consider evaluating established performance, such as probability of detection, false alarm rates, and vulnerability to defeat. MDT may also consider evaluating the potential for the technology to introduce new vulnerabilities into the system. Potential vulnerabilities may be inherent in a system, or be the result of poor installation or incorrect use. In either case the risk introduced by such vulnerabilities should be known, accepted and addressed where feasible, with other measures.

8.1.2.3.2 Proven Track Record in a Transit Environment

Security countermeasures should have a documented record of success, if possible within in a transit environment. Transit environments have unique operating characteristics and may place unusual requirements on security equipment, including:

- Environmental characteristics, such as a physically dirty

environment, vibrations, electromagnetic interference (EMI), or weather exposure

- Assets distributed over wide area
- Open or public system
- Operational constraints (such as throughput requirements)
- MDT should consider factoring in the experiences of peer agencies and other security users when selecting equipment.

8.1.2.3.3 Future Agency Needs

The countermeasures selected should meet MDT's current requirements and be consistent with the long-range goals of MDT's comprehensive security plan and strategy. Selecting security solutions should consider needs for future requirements, such as the potential for expansion, scalability, integration and upgrading. Technology factors to consider include:

- Ability to put multiple security functions on the same hardware platform
- Non-proprietary/off-the-shelf (OTS) software/equipment
- Support for data collection and storage
- Automated problem recognition
- Advanced software options for the operation of integrated controls and displays
- Ability to create single security user profiles used/enforced by multiple security applications

8.1.2.3.4 Families of Technologies

Specific countermeasures may involve a wide array of available options, which may have variations designed for different purposes or locations.

Technology differences should be analyzed to determine which variation best

meets its particular needs.

8.1.2.4 ACCESS MANAGEMENT

Access management is a set of policies, plans, procedures, personnel, and physical components that provide control and awareness of assets and activities in and around facilities and restricted areas.

8.1.2.4.1 Access Management Guidelines

This section presents sample guidelines for various access management security measures. The guidelines are not exhaustive; they are an outline of general approaches to access management and are a useful resource, but MDT must identify its particular security needs and determine which access management measures are appropriate. Also consider the differences in threat levels and/or particular circumstances among various geographic areas or facilities. Some guidelines are more appropriate for non-public transit facilities - administrative offices, maintenance yards, and operations control centers; others could be effectively implemented in stations, parking lots and garages, and other facilities open to and used by the public. Access management decisions will be made on a case-by-case basis to meet the needs and available resources of MDT.

8.1.2.4.2 Access Management Parameters

Access management controls who should be permitted access to facilities and restricted areas; where they can access (e.g., garage or rail yard facilities, vehicles, utility areas within stations or terminals); and when they can access these areas (e.g., certain days of the week or shifts). In addition to controlling passage in and out of facilities or areas, determining who belongs and who does not, access management includes the ability to observe and track movement in and out of controlled areas. MDT will grant

access for various combinations of persons and assets, depending on the needs and restrictions established by MDT.

Basic principles of access management include:

- Limiting the number of access points
- Identifying and dedicating secure areas
- Providing transition areas between secure and non-secure areas
- Minimizing interference with the movement of passengers and system operations
- Not interfering with fire protection and life safety systems
- Conforming to Americans with Disabilities Act (ADA) requirements
- Layering of security systems
- Using protective measures addressing all threat phases-
deterrence, detection, defense, mitigation, response and recovery
- Providing an audit trail and/or transaction reporting capability

In developing an access management plan, consideration should be given to identifying assets and areas that should be controlled. Decisions have to be made regarding who will be given access to those assets and areas. Also decide how different access management tools-such as intrusion detection and surveillance-can work together as a part of an integrated security system.

8.1.2.4.3 Challenges in the Transit Environment

Transit systems must accommodate thousands of customers daily, 24 hours a day/seven days a week in some facilities. Customers using transit systems may pass near restricted areas such as tunnels, control rooms, utility rooms, power supplies, or hazardous-material storage areas. This presents a unique challenge for transit agencies; implementing access control systems that

provide easy access to public areas of facilities, at the same time as limiting access to non-public areas to authorized personnel.

Transit agencies are constantly faced with the challenge of managing risks to diverse assets throughout the system. Access management strategies and systems for transit environments must work in a wide variety of settings and be effective in protecting diverse asset types (see Figure 8-2.).

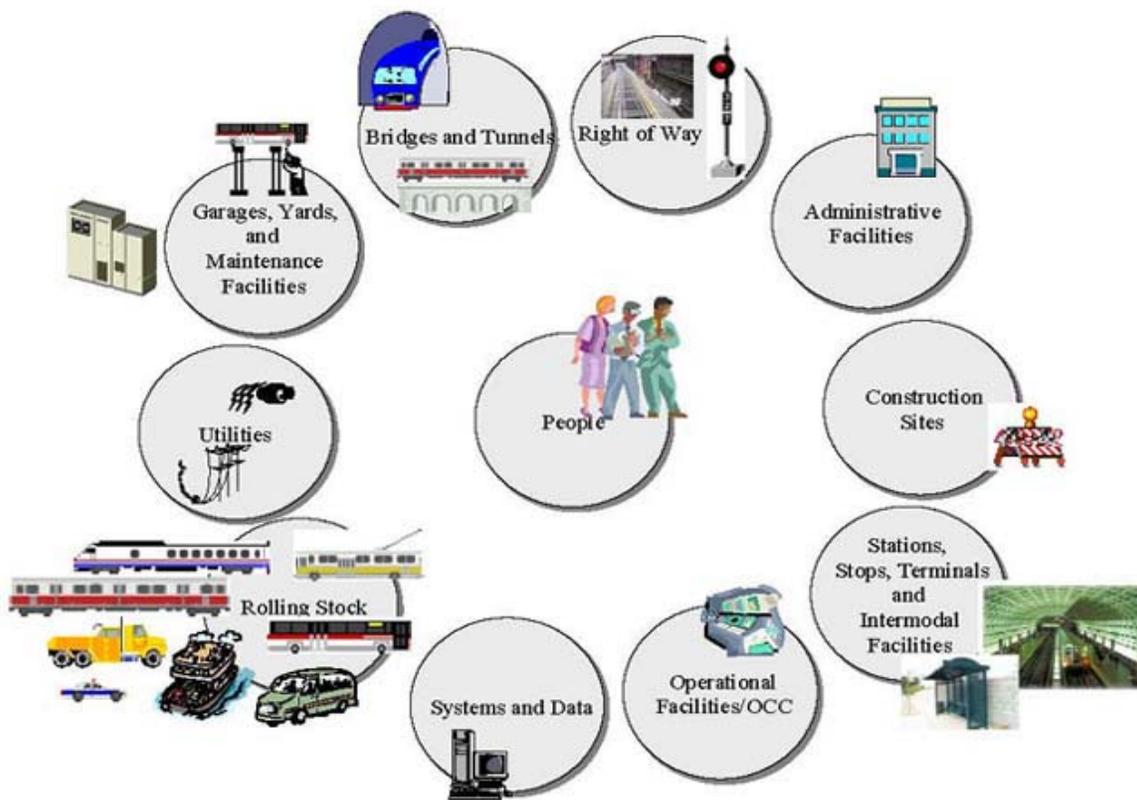


Figure 8-2: Transit System Assets

Each asset has its own level of risk-attractiveness as a target, vulnerabilities, accessibility, and criticality to the system. However, MDT should consider prioritizing risks through threat and vulnerability assessments and select sets of countermeasures that provide the best overall risk reduction for the system as a whole. Since funding for security efforts is limited, MDT must strive to

ensure that protective security measures for each asset are equal to the threats and vulnerabilities of that particular asset and the potential consequences of an attack.

8.1.2.4.4 Access Management as Part of a Comprehensive Security Plan

A transit agency's access management efforts are part of a larger, comprehensive security plan that reflects an accurate assessment of critical assets and potential threats and vulnerabilities, and establishes a methodology for addressing them. The goal is to protect the agency's assets. In addition, because many access management tools have multiple security roles, access management efforts can be tightly woven into an overall security strategy.

MDT should consider preparing and implementing access management strategies that are consistent with their comprehensive security plan. The Threat and Vulnerability Assessment (TVA) can be used to help determine which access management strategies to implement.

8.1.2.4.5 Access Management Concepts

An effective access management strategy draws on several broad security concepts: CPTED, access control, intrusion detection/surveillance, layered security, and systems integration.

8.1.2.4.5.1 Crime Prevention Through Environmental Design (CPTED)

CPTED is a method of situational crime prevention that is based on the premise that the proper design and effective use of the built environment can lead to a reduction in crime and an improvement in the quality of life.

CPTED principles related to access management, such as natural

surveillance, are considered a logical first step in improving security. Natural surveillance is a design strategy intended to facilitate observation of activities taking place on a site. Designing for natural surveillance involves providing ample opportunity for legitimate users, engaged in their normal activities, to observe the spaces around them.

To reduce the need for guards and technology, MDT will consider a CPTED strategy that takes advantage of as many architectural elements as possible, such as appropriate building layout and pedestrian flow, lighting, landscaping, and surveillance. Architectural design strategies are discussed in more detail in the Security-Oriented Design Considerations for Transit Infrastructure section of the *FTA Transit Security Handbook*.

8.1.2.4.5.2 Access Control

Access control is the ability to determine who can or cannot enter specific fields, areas or access particular assets or information. It is the fundamental principle of access management, and an important aspect of an effective security system.

Access control relies on a combination of physical elements (barriers, portals, credentials) and policies (asset classification, credentialing) to operate properly.

8.1.2.4.5.3 Intrusion Detection and Surveillance

Intrusion detection is the ability to know when someone has entered a secured area, and may include the ability to determine the identity of that person. This tracking of movement includes both authorized and unauthorized activity, and therefore can serve as both a staff management and a security tool.

Surveillance is the ability to monitor a specified area. This may occur through an on-site staff member or via remote technologies, such as closed-circuit television (CCTV). Surveillance systems vary in terms of detecting and recording capabilities.

8.1.2.4.5.4 Layered Security

The concept of layered security allows multiple opportunities for thwarting or disrupting terrorist activities and is a key aspect of an effective access management strategy.

Some antiterrorist measures are active defense measures. Highly visible security forces and security countermeasures could convince terrorists they will be unable to carry out their "attack sequence" of Target, Surveille, Plan, Rehearse, Execute, Escape, and may reduce the likelihood of an attack. Use of these high-visibility measures may cause terrorists to change their methods or switch to a more lightly defended target, requiring agencies to frequently reassess total target vulnerability.

Counter-surveillance is also a fundamental part of layered security. The conduct of extensive target reconnaissance is a common procedure for most terrorist groups. Mitigation of these attacks involves detection of the intentions of the terrorist-recognizing and reporting pre-incident indicators of a pending attack. Employees and security forces must be aware that surveillance is possible, understand the need to counter it, and be able to detect and report it. For example, when entry point personnel are equipped with cameras they become a more effective countermeasure, and are able to photograph persons or vehicles suspected of surveilling a location.

Security measures implemented at several different levels ("layers") throughout a facility help provide redundancy. The concept of layered protection recommends placing the most critical or most vulnerable assets in the center of concentric levels of increasingly stringent security measures (refer to Figure 8-3). For example, a transit facility's operations control room should not be placed right next to the building's reception area. Instead, where feasible, it should be located deeper within the building so that, to reach the control room, an intruder would have to penetrate numerous rings of protection, such as a fence at the property line, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door to the control room.

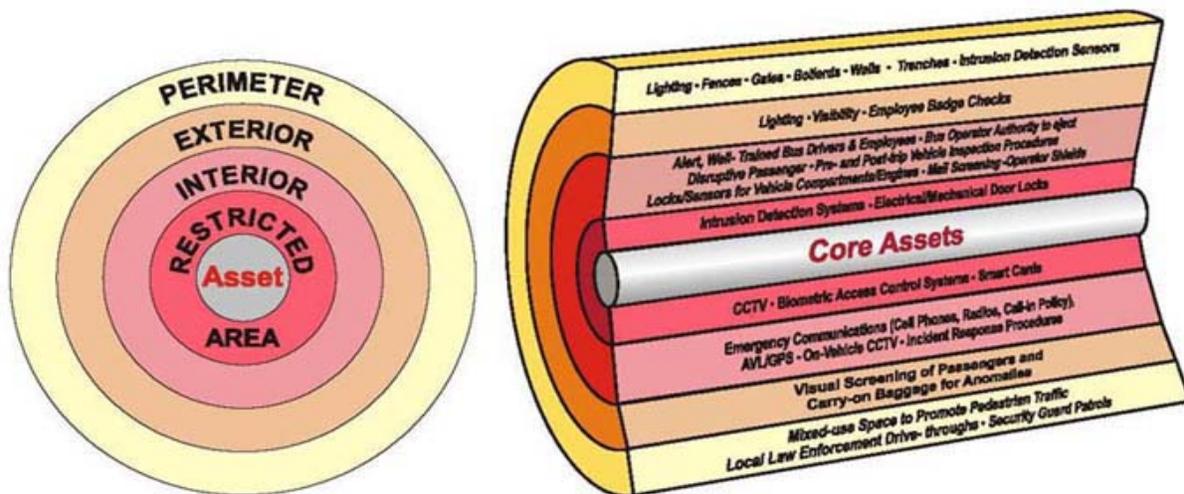


Figure 8-3: Layers of Security

8.1.2.4.5.5 Systems Integration

Integrated access management systems will permit MDT to monitor, detect, and respond to events more effectively. Systems integration streamlines management functions and improves the ability to secure assets by moving

access management beyond the use of isolated security technologies to a setup in which the systems share information and act in concert.

Figure 8-4 shows potential integration opportunities for access management components. Integrated access management systems for such functions as intrusion detection, surveillance, access control, and credentialing can monitor individuals' movements within restricted areas, and through points of entry and exit.

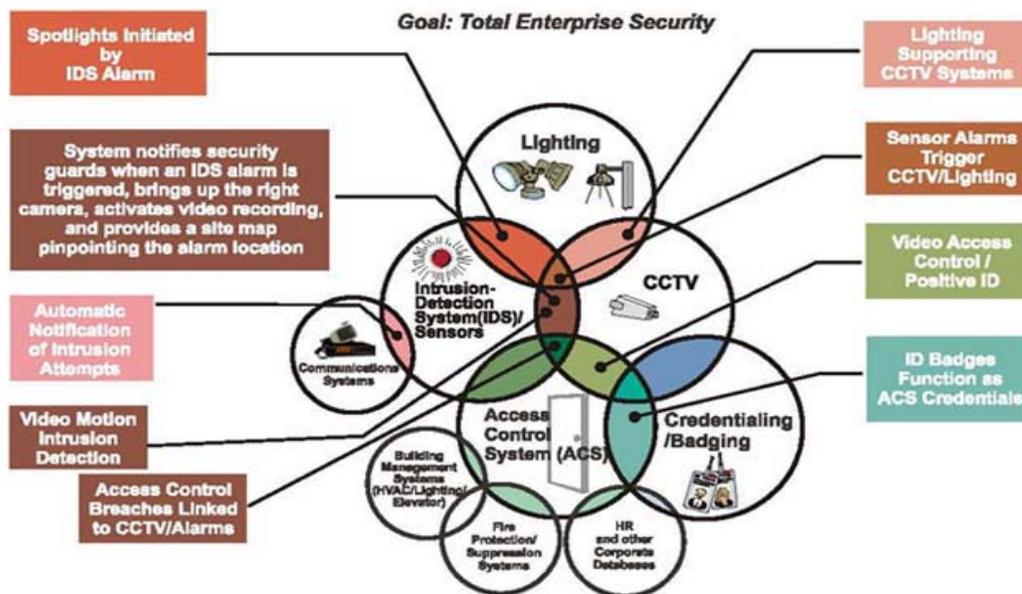


FIGURE 8-4: Access Management Component Integration

8.1.2.4.6 Tools/Techniques

Tools and techniques to consider in managing access include:

- Policies and procedures
- Perimeter protection and physical barriers
- Entry-point screening
- Credentials and credentialing
- Surveillance systems

- Intrusion-detection systems (IDS)
- Security personnel
- Communications and information processing systems
- Lighting

When used effectively, these tools and techniques create an adaptable network of security measures, with a high degree of interaction among subsystems, and the ability to evolve over time in response to changing security requirements and technologies.

8.1.2.4.6.1 Policies and Procedures

A crucial aspect of access management and of security systems in general, is the need for an effective set of administrative policies and procedures establishing the various system elements and security functions. The policies establish the relationship between groups of users and sets of assets, and permit or deny different users' access to certain assets.

MDT's up-to-date access management plan lists the functional requirements for access management systems, as well as standard operating procedures that address contingencies for security issues that may arise. Security personnel must have clear, effective procedures to perform their duties well.

8.1.2.4.6.2 Perimeter Protection and Barriers

Barriers can be used to define property boundaries and to enclose secured areas. Physical barriers include any objects that prevent access into a restricted area or through an entry portal, including fences, doors, turnstiles, gates, and walls.

There are two categories of physical barriers:

- *Access-control barriers* are those used at entry points to selectively allow people to pass through. The most common admission-control barriers are swing doors, revolving doors, turnstiles, and portals. These may be operated mechanically or electronically in conjunction with electromagnetic door locks, keypads, or other entry-point screening mechanisms.
- *Perimeter-control barriers* establish a secure boundary around an area, and limit access to and from that area to admission-control points. They can be constructed from a variety of materials, and may be designed to prevent some types of movement while permitting others (such as bollards that block motor vehicles while enabling pedestrians to pass through). Barriers can be placed to direct passenger flow and deter access to isolated or hidden locations.

A common and effective type of physical barrier for perimeter control is chain-link fencing with barbed wire. It is flexible and easy to erect around any size and shape of structure and along rights-of-way and bridges and is also relatively inexpensive to install. Agencies should consider inspecting fence lines regularly for integrity and repairing any damage promptly. Fences and other simple barriers, such as walls, can be enhanced with intrusion-detection or CCTV systems, to improve their effectiveness at preventing unauthorized access.

Shrubbery and landscaping decisions along a perimeter should be located to minimize their impact on maintaining visibility for surveillance purposes. Building walls, floors, and roofs may form part of the barrier and should be designed to provide security equivalent to that of the security barrier.

8.1.2.4.6.3 Entry-Point Screening

A critical part of the access control function is entry-point screening; a method for enforcing selective admission at entrances and other access points. Entry-point screening typically involves secure/non-public areas within a transit system, and can entail verification of identity, a physical search of belongings or a vehicle, x-ray search of bags and packages, weapons detection of both belongings and people, explosives detection, or chemical/biological agent screening. Although high ridership volume, limited space, and the limited throughput of current metal detection screening technologies would not allow mass screening of all passengers in transit stations without severely impacting service, consider screening at key high-security facilities/areas, or selectively screen for high-risk individuals, locations, and events.

Entry control, i.e., allowing or denying entry, may have more immediate relevance and success in non-public facilities and areas, such as operations centers, maintenance facilities, and special equipment rooms in stations, when combined with an automated access-control device. Entry-point screening is particularly beneficial with temporary or occasional workers and visitors.

Consider utilization of variable levels of entry control:

- A security guard controls entry; ID cards or other means of identification may be checked.
- An agency-provided special ID card/badge to work with automatic readers (based on what you HAVE).
- A code, such as a personal identification number (PIN), for entering on a keypad (based on what you KNOW)
- A biometric device for feature recognition, such as fingerprint identification (based on who you ARE).

Each approach offers different level of security, has different labor requirements and uses different technologies (see Figure 8-5).

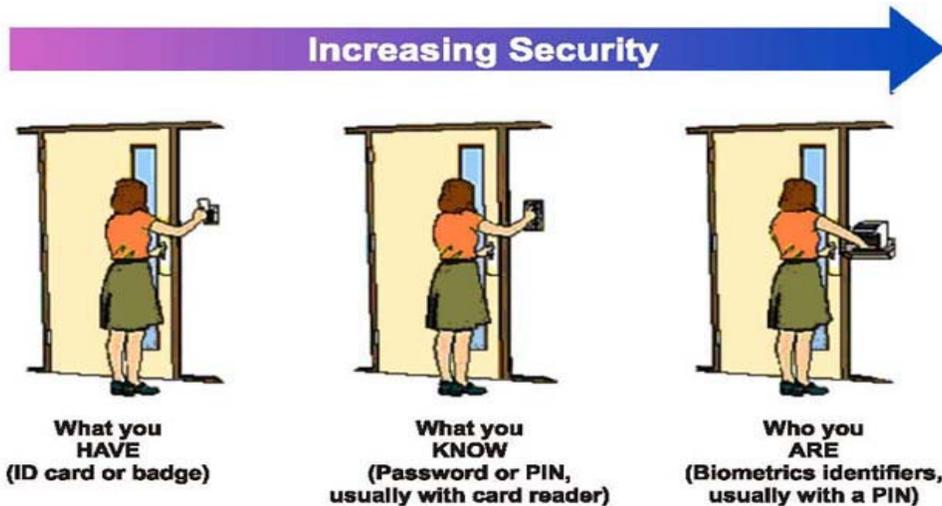


FIGURE 8–5: Entry Control Techniques

8.1.2.4.6.4 Credentials and Credentialing

Credentials and credentialing are key components for access control systems.

8.1.2.4.6.4.1 Credentials

Credentials are physical objects used to gain admission at entrances or other access points, such as identification cards, badges, card keys or physical attributes. A credential signifies that an individual's qualifications have been assessed and validated. Whether the credential is a simple badge with a picture presented for sight identification or a "smart" card that can be used to gain physical access to secure areas or to gain virtual access to computer networks, it is the key to the access control system. A credential can work on several levels. Security workers may visually inspect credentials using graphics, colors, pictures, and text to help identify personnel and their access

to restricted areas. The credential may electronically identify the holder to the security system, which checks a data base to ensure the credential holder has the required clearance. There may also be additional personal information about the cardholder on the credential or in a central database, including biometric data or a Personal Identification Number (PIN) that must be entered at a reader. Examples of biometric technologies are fingerprint, iris scan, retinal scan, hand geometry, face scan, voiceprint, and signature.

8.1.2.4.6.4.2 Credentialing

Credentialing is the issue and management of credentials, as well as the procedures used to make decisions about granting credentials to particular individuals. Credentialing typically includes the process of reviewing individuals' qualifications, to assess whether they should be granted access to buildings, facilities, secured areas, or computer networks. Consider assigning a security classification to each part of the system, and identifying the types of users accessing each part. Also consider performing some form of background check before the credentials are issued, ranging from viewing a photo ID, to performing a criminal wants and warrants check, or even an intense background check with interviews. The more important the areas to which an individual will have access, the more stringent and periodic the background check may have to be. Figure 8-6 illustrates the credentialing process for access control.

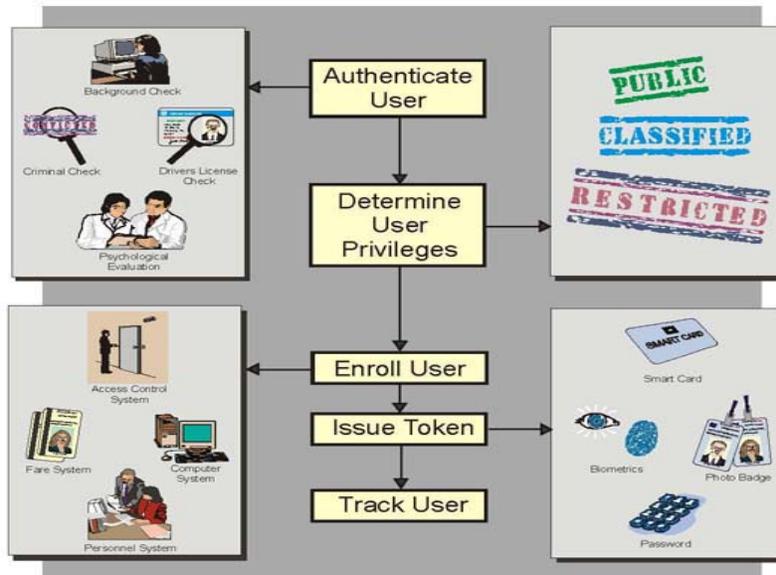


FIGURE 8–6: CREDENTIALING AND ACCESS CONTROL

Credentialing is an important access management tool. In the transit environment, its use is limited to individuals employed or contracted (including concessionaires) by MDT, and to some visitors at administrative facilities. Permanent employees, temporary employees, visitors requiring escort, and visitors not requiring escort are examples of users for whom different types of credentials may be needed.

8.1.2.4.6.5 Surveillance Systems

Deploying remote CCTV surveillance systems expands the areas in and around transit facilities monitored by security personnel. CCTV surveillance systems may include fixed cameras and pan/tilt/zoom cameras that security personnel can remotely control, and often include video-recording systems. In addition, the visible presence of surveillance cameras in an area can serve as a deterrent to potential intruders who believe they are being observed.

Agencies should be aware of the labor intensity of watching banks of monitors, be cautious about relying on CCTV beyond their ability to monitor

activities, and should consider the use of event triggered surveillance. For example, pairing remote-surveillance with intrusion-detection systems results in event-triggered surveillance, which may be particularly useful for vulnerable areas that might not otherwise require constant observation, such as tunnel portals or power substations.

When combined with a videotape or digital recording system, a surveillance system can provide vital information about security events. Responders can use the video information to apprehend intruders or to communicate descriptions of intruders to law enforcement agencies. In addition, the video record can potentially be used as evidence in a trial, provide investigators with information about the causes of events, and discourage future occurrences. Videotape evidence can improve the likelihood that an alleged criminal is convicted in a court of law. Agencies must follow local and state requirements for the auditing, handling, storage, and retention of such materials. Some jurisdictions require that it be possible to trace any recorded images to a specific date, time, recording device and recording medium and operator. New rules being introduced relating to the submission of CCTV video recordings as evidence state that it must be proven that a videotape has been completely erased before being reused. Failure to comply with data protection requirements may affect the police's ability to use CCTV images to investigate a crime and may hamper the prosecution of offenders.

It is important to note with the installation of a surveillance system, particularly one including CCTV technology, the agency may have to consider developing a privacy policy to manage the use of any images or sounds recorded by the system.

8.1.2.4.6.6 Intrusion Detection

An Intrusion Detection System (IDS) is a combination of integrated electronic components, including sensors, control units, transmission lines, and monitoring units, that detect one or more types of intrusion into an area protected by the IDS. An IDS includes both interior and exterior systems, and may also include electronic entry control devices and CCTV for alarm assessment.

IDSs can be useful throughout transit system operations, allowing security personnel to monitor the movements of authorized people in restricted-access areas and to alert security personnel of potential breaches by unauthorized persons. At perimeters IDSs provide improved security-response time. Pairing intrusion-detection systems with remote surveillance technology enables event-triggered surveillance.

There are numerous types of interior and exterior sensors that agencies can deploy to signal security personnel when an intruder crosses a threshold, opens a door, or breaks a window. These include area sensors, barrier sensors, point sensors, and volumetric sensors. Intrusion sensors may be buried in the ground or mounted to a fence, wall, ceiling, floor, door, or window. Sensing technologies include magnetic or mechanical switches, pressure sensors, infrared sensors, acoustic sensors, and video cameras.

8.1.2.4.6.7 Security Personnel

Since the September 11, 2001 attacks, roles of security forces have been shifting from prior focus on crime-prevention and safety to also ensuring the security of the transit system and riders against terrorist attacks.

Security personnel are responsible for carrying out access management policies and procedures and for overseeing and operating the access control

systems used. Functions performed by security personnel can include:

- Identification checks - visually inspecting badges, credentials, or other forms of identification. Entry-point screening - visually inspecting bags and parcels, vehicles, operating metal detectors and x-ray machines, etc.
- Monitoring security systems - monitoring surveillance cameras, digital video, intrusion detection, and other security systems.
- Patrols - patrolling on foot or in a vehicle to ensure that doors are locked and fences and gates are secured. Patrols visually inspect buildings and grounds and can provide a human presence to deter intruders. A patrol can also include a K-9 component to provide additional deterrence and detection.
- Response - responding to alarms or unauthorized entry.
- Communications - contacting law enforcement and emergency response personnel.

8.1.2.4.6.8 Communication and Information Processing Systems

Communication systems are vital because they ensure that information about incidents can be sent to appropriate persons. These systems enable person-to-person communications and can link various access management subsystems into a networked security system.

Communications links can be established using any number of modes or combinations of modes, including telephone, cell phone, fax, e-mail, Web site, radio, intercom, wired, wireless, fiber optic, PDA or pager to transmit voice, data, and/or video. On-site security personnel can use communications systems to summon police or other appropriate emergency response organizations when necessary. Reliability, redundancy, and security of communications links are important to the overall success of a security

system.

Information processing systems are also an integral part of many security systems. Consisting of a combination of hardware and software, including computers, data bases, and workstations, they are used by security personnel to coordinate activities, record incident data, provide audit trails, and generate reports. Information systems make possible central control and maintenance of user access, authorization, and authentication. They are also used within systems for signal processing and monitoring, and for managing many control systems.

8.1.2.5 LIGHTING

Lighting increases visibility in and around transit facilities, and makes it more difficult for intruders to enter a facility undetected. It is beneficial in almost all environments, especially those that receive little natural light or are used at night. Agencies should consider lighting when installing and updating other access management subsystems, particularly those that utilize surveillance and intrusion detection. In accordance with CPTED principles, lighting can also be used to create greater levels of comfort for passengers and staff present in transit facilities.

8.1.2.5.1 Security Lighting

Security lighting is that portion of the lighting system which increases visibility around perimeters, buildings, storage tanks, and storage areas, loading docks, as well as in buildings, hallways, and parking lots. It is a security management tool that is applicable in almost all environments within a transit system, and should be considered when installing and updating other access management sub-systems, particularly those focusing on surveillance.

Security lighting allows the security force to visually monitor the lighted areas,

making it difficult for someone to enter the facility undetected, and facilitating the apprehension of offenders. Determining which system is appropriate for a given application depends on the identified risk control requirements of the facility.

At a minimum, all access points, the perimeter, restricted areas, and designated parking areas should be illuminated from sunset to sunrise or during periods of low visibility. Also refer to Volume II Chapter 4 and Table 4-3 for additional information. In some circumstances, lighting may not be required, but these circumstances must be addressed in the facility security plan. The plan must show that the absence of lighting will not adversely impact risk and should include the alternative measures being used. Undesirable shadowing will exist, and the total elimination of shadowing is not practical in all areas. Consider the environment where stations and other infrastructure are located, so as to make lighting appropriate to the area. More residential environments may be less receptive to bright, consistent lighting. Consider methods of making lighting safe, attractive and neighborhood-friendly, such as high-level, indirect lighting, multiple low-level lights, or some combination of both.

These guidelines should be considered when installing security lighting:

- Facilities should be illuminated to an acceptable industry standard, such as the Illuminating Engineering Society of North America (IESNA) or other recognized industry standard. Also comply with Volume II Chapter 4 and local codes.
- To provide better visibility, updated lighting technology should be used. For CCTV compatibility, consider metal halide lighting.
- Lighting should be directed downward and should produce high contrast with few shadows.

- Illumination is recommended whenever possible, but equivalent measures such as motion detectors or intrusion alarms may be used to monitor areas at facilities where perimeter illumination is unpractical.
- In some circumstances, it may be preferable to use lighting systems only in response to an alarm or during specific operations.
- Portable floodlights may be used to supplement the primary system.
- When used, portable floodlights should have sufficient flexibility to permit examination of the barrier under observation and adjacent unlighted areas.
- Controls, switches, and distribution panels for lighting should be located in restricted areas (such as the Station Attendant Booth), weatherproofed, protected to prevent unauthorized access or tampering, readily accessible to security personnel, and inaccessible from outside the perimeter.
- Wiring for security lighting should be in tamper-resistant conduits, preferably underground; if above ground, wiring should be high enough to reduce the possibility of tampering.
- Critical facilities should provide a secondary supply line(s) separated from the primary power line(s). The facility should have the ability to automatically and rapidly switch to the secondary power line(s) during primary power failures.
- Power supplies for security lighting should be adequately protected.
- Standby/emergency lighting should be tested per industry and code standards, for example:
 - Monthly for a duration of 30 seconds to confirm system operation, and
 - Annually to confirm the minimum duration of emergency

lighting is compliant with codes and requirements of MDT and the AHJ.

- Inoperative lights and lamps should be repaired/replaced promptly.
- Materials and equipment in storage areas should not mask security lighting.

These lighting guidelines should be considered for perimeter lighting and for entry, guardhouse, and parking lot lighting.

8.1.2.5.1.1 Perimeter Lighting

Where perimeter lighting is required, the lighting units for a perimeter fence should be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area both inside and outside the fence.

Perimeter lighting should be continuous and on both sides of the perimeter fence and should be sufficient to support CCTV and other surveillance equipment where required.

The cone of illumination from lighting units should be directed downward and outward from the structure or area being protected. Cones of illumination should overlap to provide coverage in the event of bulb burnout.

The lighting should be arranged so as to create minimal shadows and minimal glare in the eyes of security guards.

8.1.2.5.1.2 Entry, Guardhouse, and Parking Lot Lighting

8.1.2.5.1.2.1 Entry/Guardhouse

Vehicle and pedestrian entrances to the facility should be illuminated.

Lighting at manned entrances must be adequate to identify persons, examine credentials, inspect vehicles entering or departing the facility premises through designated control points (vehicle interiors should be clearly lighted), and prevent anyone from slipping unobserved into or out of the premises.

Entry lighting should be sufficient to allow for personnel identification during times of darkness and extreme environmental conditions.

Lighting intensity at entrances should be planned to ensure that arriving drivers can readily recognize the premises and see where to drive their vehicle.

Lighting should not be placed to cause blinding of the driver.

Semi-active and unmanned entrances should have the same degree of continuous lighting as the remainder of the perimeter, except that additional, standby lighting should be available to provide the same illumination required for manned entrances when the entrance becomes active.

Gate houses at entrance points should have a reduced level of interior illumination to enable the security guards to see better, increase their night vision adaptability, and avoid illuminating them as a target.

8.1.2.5.1.2.2 Parking Lot Areas

In addition to the security hazard of providing hiding places, unlit parking areas are vulnerable to thieves and can pose a risk of physical attack to employees and patrons.

Parking areas should be provided with uniform illumination sufficient to allow

for personnel identification by CCTV during times of darkness and extreme environmental conditions. Also see Volume II, Table 4-3.

8.1.2.5.1.2.3 Emergency Power and Backup Power

The emergency lighting at the Parking lot and facility entries should be connected to the emergency power system to ensure they remain operational during periods when commercial power is interrupted.

Emergency power shall be supplied for a minimum of at least 90 minutes. Emergency power requirements are dictated by codes, the AHJ and MDT practices, policies and procedures. Emergency power duration may be longer if required by these entities.

Emergency power shall be supplied to emergency circuits by separate panels dedicated to emergency circuits and identified for that specific purpose.

Backup power shall be provided which will power both emergency and non-emergency circuits in the event of interruption of commercial power. Backup power can be supplied by a combination of a UPS with batteries and a LPG fueled generator. Sizing of the UPS, generator and LPG tank will be dictated by the electrical loads and duration requirements. See also; Volume II Stations, Chapter 4, Electrical Design Criteria.

8.1.2.5.1.3 Types of Lighting

There are four general types of security lighting systems: continuous, standby, moveable, and emergency. Determining which system is appropriate for a given application depends on the identified risk control requirements of the facility.

8.1.2.5.1.3.1 Continuous Lighting

Continuous lighting is the most commonly used form of security lighting systems, consisting of a series of fixed luminaries arranged to illuminate a given area on a continuous basis with overlapping cones of light during the hours of darkness. There are two primary types of continuous lighting:

- *Glare Projection.* This lighting is useful when the desired effect is the glare of lights directed toward the exterior of the facility and into the eyes of a potential intruder. The lighting at gate entrance locations is an example. A vehicle approaching the gate during the hours of darkness is fully illuminated, but the guard station remains in the shadow of the light pattern.
- *Controlled Lighting.* This lighting is used most often at locations where it is necessary to limit the width of the lighted strip outside the perimeter fence because of nearby residential areas, public thoroughfares, or other activity centers. With controlled lighting, the width of the illuminated strip can be controlled and arranged as required. For instance, one possible configuration might be a wide band of illumination inside the fence and a narrower band on the exterior of the fence. The physical design of the luminaries allows the light source to be directed to achieve these results. The angle of the luminaries is primarily downward with some angle adjustment to attain the desired width. Fully shielded lighting (fixtures that emit no light above the horizontal direction) can also alleviate neighbor objections.

8.1.2.5.1.3.2 Standby Lighting

The arrangement of this lighting system is similar to continuous lighting and meets the same security lighting specifications, but is used only in certain

circumstances. When a possible intruder is detected, the security system or guard force can activate the standby lighting system for extra illumination. It can also be deployed at unattended/attended gates for extra lighting. Standby lighting differs from the continuous lighting in that only security personnel or the security system software have control over the system.

8.1.2.5.1.3.3 Moveable Lighting

This lighting system consists of manually operated movable light sources and luminaries such as searchlights, which can be lighted during hours of darkness to cover specific areas as needed. Moveable lights are normally used to supplement continuous or standby systems.

8.1.2.5.1.3.4 Emergency Lighting

This lighting system may duplicate the other three systems in whole or in part. Its use is normally limited to periods of main power failure or other emergencies.

While security lighting should be connected to the backup power system when possible, it is a firm requirement that the emergency lighting portion of the security lighting be connected to a power source, specifically identified as “Emergency Power” that fulfills all emergency lighting power requirements. No non-emergency loads may be connected to the panels or circuits identified for emergency power.

See Section 8.1.2.5.1.2.3 - Emergency Power for duration requirements.

Table 8-7 lists the standard luminance in foot-candles that may be used for several security lighting targets. Unless otherwise directed by MDT’s Office of Safety and Security for site specific security areas, the designer shall

provide lighting in accordance with Volume II, Stations Design Criteria.

Lighting Target	Illuminance	
	Lux	Foot-candles
LARGE OPEN AREAS (Standard System)		
Average minimum illuminance	2	0.2
Absolute minimum illuminance	0.5	0.05
LARGE OPEN AREAS (Glare System)		
Average minimum illuminance	2	0.2
Absolute minimum illuminance	0.5	0.05
SURVEILLANCE OF CONFINED (low ceiling / interior) AREAS		
Average minimum illuminance	5	0.5
Absolute minimum illuminance	1	0.1
SURVEILLANCE OF VEHICLE OR PEDESTRIAN ENTRANCES		
Average minimum illuminance	10	1
Absolute minimum illuminance	2.5	0.25
CCTV SURVEILLANCE	Varies with individual systems (Consult CCTV manufacturer)	

Figure 8-7: ILLUMINANCE SPECIFICATION

8.1.2.5.2 Vehicle Access Control and Parking

Vehicle controls can most appropriately be applied at those transit facilities that are not typically open to the public—such as administrative offices, maintenance facilities, operation control centers—as a way to deter unauthorized or illegal access. Some of the methods listed here may also be applied around suburban transit stations or other public facilities with significant available parking and a steady flow of pick-up/drop-off traffic.

MDT should follow these vehicle control and parking guidelines for vehicle inspection, facility parking/traffic control, adjacent parking, parking

registration/vehicle ID, unauthorized vehicles, vehicle access points, high-speed vehicle approaches, drive-up/drop-off locations, and electronic vehicle access control.

8.1.2.5.2.1 Vehicle Inspection

Vehicle inspections ensure that incendiary devices, explosives, or other items that pose a threat to security are not present.

Inspections must be limited and no more intrusive than necessary to protect against the danger of sabotage or similar acts of destruction or violence, based on the existing threat level. The inspection should, however, be reasonably effective.

Inspection techniques include, but are not limited to, magnetometers, physical examinations of the person or objects visually or through the use of trained animals, electronic devices, x-radiography or a combination of these methods. Use of trained animals may be limited due to availability and safety in systems where a third rail is present.

If evidence of criminal activity or contraband is discovered during security inspections, it should be treated as a criminal act and the appropriate procedures for such an act should be followed.

All vehicles entering or leaving the facility should be subject to search by security personnel. Signs should be posted to advise persons of this requirement.

8.1.2.5.2.2 Facility Parking/Traffic Control

Where required, access to non-public parking should be limited to transit

agency vehicles, personnel, contractors, and authorized visitors. This can be accomplished by use of a trained guard force, parking lot barriers such as barrier arms, or at a minimum, designation and identification of authorized parking spaces.

Visitor parking should be clearly marked and should be as close as possible to the visitor reception area of the facility. Parking should not be permitted close to or against perimeter barriers. Handicapped parking may be allowed within the established buffer zone if the vehicle and operator are identified to the staff responsible for parking control.

Whenever possible, parking areas for all transit and staff vehicles should be located inside the perimeter of protected areas.

Where possible, parking areas for general vehicles should be located outside a facility's buffer zone. Parking should not be allowed within 100 feet (30.5 meters) of the building exterior, when possible. Parking areas may be fenced and should be well lighted in accordance with the existing illuminance specification. Americans with Disabilities Act (ADA) parking will be considered separately.

Parking within the facility should be restricted only to those areas indicated in a facility physical security plan. Parking lot activity should be monitored either visually or by CCTV. Also see Volume VII Section 7.06.2. Parking regulations should be strictly enforced. Vehicle entry and exit routes should be clearly marked. A facility should have formal procedures for controlling vehicle access and parking.

8.1.2.5.2.3 Adjacent Parking

Where possible and where prudent, areas adjacent to transit facilities may be controlled to reduce the potential for vehicle-based threats against transit agency facilities and employees.

8.1.2.5.2.4 Parking Registration / Vehicular Identification Systems

Facilities implementing a vehicular identification system should establish procedures for identifying vehicles in accordance with established credentialing procedures.

A visual vehicle identification sticker/badge system can be used independently or to supplement the electronic entry control system.

8.1.2.5.2.5 Towing of Unauthorized Vehicles

Procedures for towing unauthorized vehicles at facilities should be established. Reasonable and prudent steps should be made to locate and identify the operator of unidentified vehicles.

If the operator cannot be located within a reasonable time and the vehicle cannot be verified as harmless to the facility, the vehicle should be removed by the safest, most expeditious, and prudent means. Local towing companies may be utilized for this service.

Where required, signage should be posted in all parking areas warning of the risk of towing unauthorized vehicles.

8.1.2.5.2.6 Vehicle Access Points

The first line of defense in limiting opportunities for aggressors to get vehicles close to buildings is at vehicle access points at the controlled perimeter, in

parking areas, and at drive-up/drop-off points.

Restrict the number of access points to the minimum necessary for operational or life safety purposes. This will limit the number of points at which access may have to be controlled with barriers and/or personnel in increased threat environments or if the threat increases in the future.

8.1.2.5.2.7 High-Speed Vehicle Approaches

Traffic calming can be used on inbound and outbound roadways to control vehicle speed and slow incoming vehicles before they reach the facility gate/active barrier so that security personnel have adequate time to respond to unauthorized activities (see Figure 8-8).

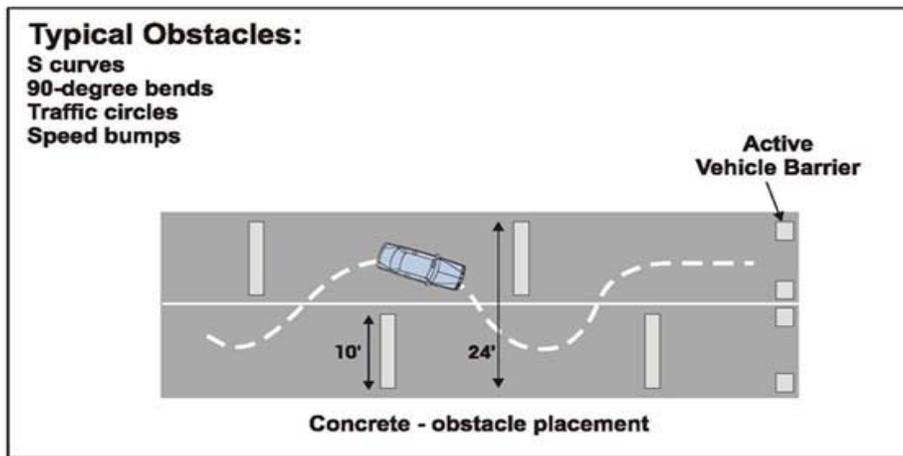


FIGURE 8-8: SPEED REDUCTION APPROACH

Appropriate traffic calming measures include:

- Road alignment (circle, serpentine)
- Swing gates
- Speed humps or speed tables
- Passive vehicle barriers (bollards, jersey barriers, etc.)

Since the energy of a moving vehicle increases with the square of its velocity, minimizing a vehicle's speed allows vehicle barriers to be lighter and less expensive. To facilitate reductions in vehicle speeds, ensure there are no unobstructed vehicle approaches perpendicular to inhabited buildings at the required parking and roadway standoff distances.

8.1.2.5.2.8 Drive-Up / Drop Off Locations

Where possible, locate drive-up/drop-off points away from large unprotected glazed areas of buildings to minimize the potential for hazardous flying glass fragments in the event of an explosion.

For example, locate the lane at an outside corner of the building or away from the main entrance. Coordinate the drive-up/drop-off point with the building geometry to minimize the possibility that explosive blast forces could be increased due to being trapped or otherwise concentrated.

8.1.2.5.3 Vehicle Barriers

The possibilities for preventing unauthorized vehicle access to non-public facilities consist of human intervention, in which members of a security force are posted to prohibit passage, or physical barrier placement in which a mechanical system is placed to prevent unauthorized vehicle passage. Vehicle barriers should be considered when necessary to control identified risks (e.g., car or truck intrusions). To reduce the risk to facilities and people, vehicle barriers may be constructed/installed in conjunction with perimeter barriers in front of stations, in personnel access areas, and along avenues of vehicle access.

Note that many perimeter barriers in use today can be forcefully penetrated

by common road vehicles: a car or light truck can easily crash through most fences and gates with minimal delay or damage to the vehicle. When necessary to control identified risks, reinforced or heavy-duty barriers should be used.

8.1.2.5.3.1 Barrier Use

Uses of vehicle barriers include: safety, theft deterrence, asset protection, pedestrian vs. vehicle traffic separation/delineation; pedestrian control; vehicle control; and traffic control. Barriers protect facilities, critical infrastructure, and people from both errant and terrorist vehicle attacks. It is important to note there are often conflicts between limiting access for unauthorized vehicles and allowing access to authorized vehicles.

8.1.2.5.3.2 Applications in a Transit Environment

Vehicle barriers are most appropriate for protecting those transit facilities that are not typically open to the public; administrative offices, maintenance facilities, operation control centers, etc.; as a way to deter unauthorized or illegal automobile access. In addition, some of the methods listed here may be applied around suburban transit stations or other public facilities, to isolate structures from pick-up and drop-off lanes. As shown in Figure 8-9, vehicle barriers can be effective countermeasures at various locations within the transit environment, including construction sites, entrance/road closures, building/work site, pedestrian walkways, parking lots/garages, or in any emergency.

USAGE	LOCATION				
	Entrances, Exits, Perimeters of Administrative / Control Facilities	Entrances / Exits to Parking Garages, Parking Lots	Entrances to Stations / Terminals	Entrances to Storage / Maintenance Facilities / Yards	Construction Sites
Create Standoff Distance	x	x	x	x	
Protect Assets / Pedestrians	x	x	x	x	
Slow Vehicles (speed control)		x		x	
Stop Vehicles		x	x	x	
Restrict Vehicle Entry		x	x	x	x
Direct Traffic	x	x	x	x	x
Revenue Collection		x			
Theft Deterrent		x		x	

FIGURE 8-9: VEHICLE BARRIER USAGE

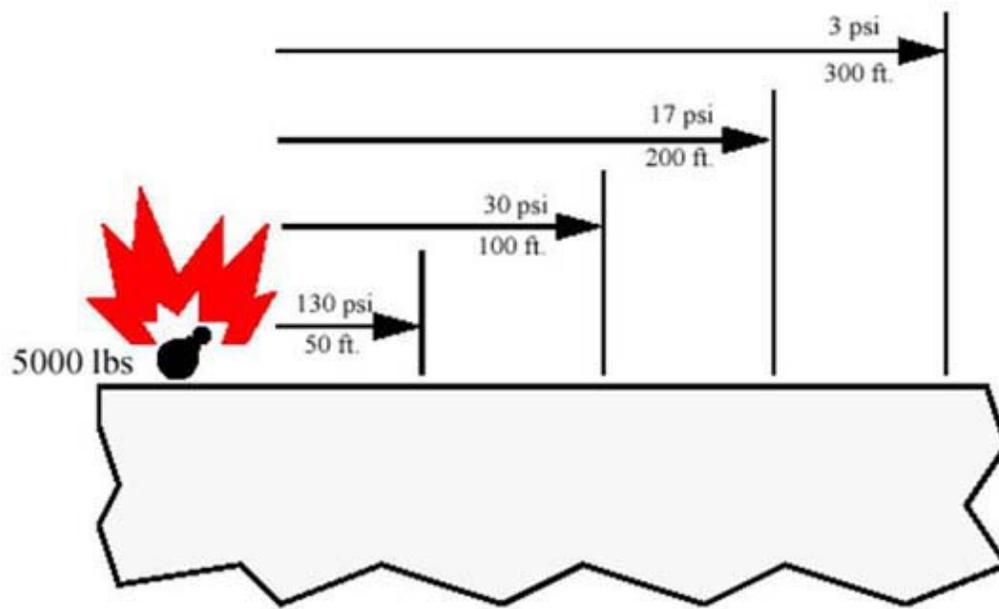
Standoff Distance

Barriers can be used to create a standoff distance providing a measurable blast-effect mitigation zone (a buffer zone between a potential bomb and the asset/facility). The intent is to keep unauthorized vehicles a sufficient distance away from the facility/asset, so the nearest distance at which a vehicle-based bomb can be detonated limits the amount of damage from an explosion.

Barriers can be placed to establish a standoff distance at a particular location or around the entire perimeter of a facility. Determine the minimum standoff distance necessary to provide a reasonable blast-effect mitigation zone that provides a survivable structure. This should be based on the results of a structural analysis.

There are several sources that provide guidance as to the proper setbacks for a variety of structure types. The Department of Defense Security Engineering

Manual and the TSWG Terrorist Bomb Threat Standoff Card are two examples. Figure 8-10 shows blast overpressures at various distances for a 5,000 lb TNT equivalent blast.



Source: LLNL, undated

Figure 8-10. Blast Overpressures as a Function of Distance (For a Bomb Equivalent to 5,000 Pounds of TNT)

Asset Protection

Barriers can protect assets from intentional or unintentional ramming by vehicles. For example, bollards can be used around fueling stations, around guardhouse entrances to protect guards and entrance equipment, or at station entrances to protect pedestrians.

8.1.2.5.3.2.1 Vehicle Speed

Barriers can limit vehicle speeds on facility approaches using speed controls.

8.1.2.5.3.2.2 Vehicle Stops

Barriers can stop unauthorized vehicles from proceeding through vehicle checkpoints/entryways.

8.1.2.5.3.2.3 Vehicle Restriction

Barriers can be used to restrict vehicle entry, limiting access to agency vehicles only.

8.1.2.5.3.2.4 Traffic Direction

Barriers can channel traffic at an approach or within a facility.

8.1.2.5.3.2.5 Revenue Collection

Barriers can enforce revenue collection at parking lots and garages.

8.1.2.5.3.2.6 Theft Deterrence

Barriers can deter theft at parking lots and garages.

8.1.2.5.3.3 Barrier Types

Barriers are grouped into two general categories:

- Natural barriers include water, vegetation, and terrain. A natural barrier may exist "naturally," or be placed by individuals.
- Fabricated/structural barriers include bollards, guardrails, fences, and walls.

Properly designed and installed barriers are effective in controlling both pedestrian and vehicular movement inside of a facility, or within a facility's perimeter. "Vehicle Barrier Types," for a list of all barrier types and a description of their effectiveness and use.

8.1.2.5.3.4 Barrier Selection and Implementation

Vehicle barrier functions range from those used to provide positional control of vehicles to those used to create a physical barrier designed to resist the head-on attack of a ramming vehicle. A much more resistant barrier would obviously be required for the latter use.

8.1.2.5.4 Critical and Restricted Area Access

Restricted areas are those portions of a facility with access limited to authorized persons, typically because the areas are identified as essential to the security of the operations, control, or safety of a facility. Examples include, but are not limited to, communications or control centers, mechanical/utility areas, hazardous material handling and storage areas, and CCTV display rooms. As an alternative, an entire facility may be designated as a restricted area.

Mechanical areas may exist at one or more locations within a building. These areas house centralized mechanical systems (heating, ventilation, and air conditioning, elevator, water, etc.), including filters, air handling units, and exhaust systems. Such equipment is susceptible to tampering and could be used in a chemical, biological, or radiological attack. Access to mechanical areas should be strictly controlled by keyed locks, keycards, or similar security measures. Additional controls for access to keys, keycards, and key codes should be strictly maintained.

8.1.2.5.4.1 Critical Operating Areas

To control unauthorized access to critical operating areas, establish restricted areas and consider implementing appropriate measures such as:

- MDT should designate in writing which areas of the facility are considered restricted.

- All restricted areas should have a clearly marked perimeter barrier. Erect fences or other barriers to delineate a perimeter where natural barriers do not form a boundary.
- Block entry through windows to restricted areas (e.g., install bars on windows).
- All restricted areas should not allow access from the ceiling (i.e., drop ceilings).
- All restricted areas should be clearly defined and marked indicating that an area has restricted access. Markings indicating restricted areas should be posted and clearly visible to all personnel. Restricted areas should have a personnel identification and control system with all entrances/exits guarded, controlled, or secured with alarms.
- Limit the number of access points.
- Only those personnel whose duties require access to information or equipment should be allowed within restricted areas.
- Persons whose duties do not require access should be required to remain under constant escort while in restricted areas.
- Security personnel should perform routine patrols of restricted areas, especially if no employees are present or the threat level is high.
- At heightened threat levels, procedures should be in place for personnel to guard or patrol restricted areas.
- Walls separating work areas on a raised floor (e.g., in computer rooms) where the level of security is different on either side of the partition should extend and completely shut off the area between the raised floor and the permanent floor.

8.1.2.5.4.2 Hazardous Areas and Security Areas

When a potentially hazardous area is also a security area, follow these guidelines:

- Provide a minimum number of entrances for security areas that satisfy the requirements of the National Fire Protection Association NFPA 101 Life Safety Code and provide some exits for emergency use only.
- Equip entrances to and exits from security areas with doors, gates, rails, or other movable barriers to direct and control the movement of workers or vehicles through designated portals.
- Install panic hardware on emergency exit doors in security area perimeters that is only operable from the inside and equipped with at least a loud local alarm, and install door locks and latches that comply with NFPA 101.
- Equip all non-monitored exits from protected areas, material access areas, or vital areas with intrusion alarms.
- Implement security controls that do not prevent rapid evacuation of personnel.

8.1.2.5.5 Windows

Window openings can be used to access transit agency facilities and/or remove transit agency property and documents from a facility. Any part of a window that is 18 feet (5 meters) or less above ground, or 18 feet (5 meters) or less from a potential access point, such as an adjoining building or tree, is considered vulnerable to inappropriate or illegal access.

When planning security safeguards for windows, include the impact of window placement on security, in accordance with Crime Prevention Through Environmental Design (CPTED) principles, since facility occupants can

observe who is approaching the facility and outsiders can observe crimes being committed inside. Fire and safety concerns should also be included.

8.1.2.5.5.1 Construction

Windows should be of sturdy construction and properly set into substantial frames. The window frame must be securely fastened to the building so that it cannot be pried loose and the entire window removed.

If a window can be opened, it should be secured on the inside. The mechanism used to secure the window may be a bolt, a slide bar, or crossbar. Key-operated locking devices for windows should be coordinated with and approved by the appropriate fire and safety officials before installation. Outside hinges on a window should be of the security type or be welded, flanged, or otherwise modified to make unauthorized removal difficult.

Windows next to doors should be protected so that aggressors cannot unlock the doors through them.

8.1.2.5.5.2 Steel Bars and Grills

Window glass can be broken or cut to enable an intruder to reach inside and release the lock. When necessary to provide the required degree of safeguarding, bars or steel grills may be used to protect vulnerable window openings. Prior coordination with fire and safety officials is necessary before placing bars or any other type of obstruction across window openings that might impede evacuation efforts.

Bars and grills should be installed on the inside of the window opening, wherever possible, to ensure maximum protection.

Bars should be at least 0.5 inches (1.25 cm) in diameter if they are round and at least 1 inch (2.5 cm) wide by 0.25 inches (0.63 cm) thick if they are of the flat type.

Grills should be constructed of Number 9-gauge security mesh, with individual mesh square dimensions not to exceed 2 inches (5 cm) on a side.

Bars and grills must be securely fastened to the window frame so that they cannot be pried loose.

8.1.2.5.5.3 Glass Brick

Glass bricks may be used as a substitute for conventional windows, provided their use meets ventilation requirements and conforms to fire and safety regulations.

8.1.2.5.5.4 Glass and Steel Framework

Small glass squares set in steel framework cannot be considered as secure construction. An intruder can break a pane of glass and reach through the opening to access the locking mechanism. The metal portion is normally not intended to provide protection against forced entry and is vulnerable to breaking or cutting by a potential intruder.

8.1.2.5.5.5 Security Glazing

The design and installation of protective window glazing measures should be under the direction of a facility engineer. Windows on first and second floors or windows facing a roadway should be considered candidates for glazing.

Laminated and heat treated glass should be used for new construction and security film for retrofit applications. When security film is used, care should

be taken in developing appropriate specifications. Not all film on the market is true security film that will enhance survivability under blast loads. Security film with a minimum thickness of 7 mm should be used.

8.1.2.5.6 Sewers and Storm Drains

Accessible opening to sewers and storm drains should be secured if the areas of the openings associated with them are larger than 96 square inches (619.4 sq cm) and more than 6 inches (15.2 cm) in any one dimension.

8.1.2.5.7 Rooftop Access Points

Rooftop structures can present readily available points of access to a potential intruder. Infrequently used access points, such as openings in elevator penthouses, rooftop hatchways, and trap doors should be addressed in a building's security plan. Rooftop access points may require security safeguards.

Rooftop access points should be secured with approved high security padlocks, locks, and/or security bars. Where necessary, these openings should be alarmed to prevent unauthorized entry attempts.

Skylights and similar structures should be protected with steel bars or mesh installed on the interior of the opening to make it more difficult to remove.

Roofs also provide access to HVAC units and restroom exhausts. Roof areas with HVAC equipment should be treated like mechanical areas. Fencing or other barriers should restrict access from adjacent roofs.

Access to roofs should be strictly controlled through keyed locks, key cards, or similar measures.

8.1.2.5.8 Air Intakes

Ground-level air intakes to HVAC systems provide an opportunity for aggressors to easily introduce contaminants that could be drawn into the building. The security of outdoor air intakes is essential to protecting the indoor environment from an external attack.

A recent Centers for Disease Control (CDC) document identifies actions to enhance occupant protection from an airborne chemical, biological, or radiological (CBR) attack. (Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health. *"Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks."* May 2002).

Locate all air intakes at least 10 feet (3 meters) above the ground.

Relocate accessible air intakes to a publicly inaccessible location (a secure roof or high sidewall).

If relocation of outdoor air intakes is not feasible, construct intake extensions to place the intake beyond the reach of individuals (an extension height of 12 feet (3.7 meters) is suggested). Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes.

Entrance to the intake should be covered with a sloped (45° minimum) metal mesh to reduce the threat of objects being tossed into the intake.

If intakes cannot be made physically inaccessible, a security zone should be

established around outdoor air intakes.

8.1.3 SPECIFIC SECURITY CRITERIA

To accomplish the general criteria, the following specific criteria are established:

All Critical Elements and Element Subsystems will be reviewed by the Designer to identify those which are susceptible to security risks and problems. Each will then be assigned a security level in accordance with the following subsections.

8.1.3.1 TRANSIT SYSTEM SECURITY LEVELS

There shall be four security levels of the transit system:

- A. Level 1: Critical security areas shall be restricted and controlled to allow access to those areas only to authorized transit employees with relevant disciplines. Typically these areas are identified as essential to the security of the operations, control, or safety of a facility. Examples include, but are not limited to, communications or control centers, mechanical/utility areas, hazardous material handling and storage areas, and CCTV display rooms. As an alternative, an entire facility may be designated as a restricted area.

Mechanical areas may exist at one or more locations within a building. These areas house centralized mechanical systems (heating, ventilation, and air conditioning, elevator, water, etc.), including filters, air handling units, and exhaust systems. Such equipment is susceptible to tampering and could be used in a chemical, biological, or radiological attack. Access to mechanical areas should be strictly controlled by keyed locks, keycards, or similar security measures. Additional controls for access to

keys, keycards, and key codes should be strictly maintained. Invitees may have access to the area in the company of an authorized transit employee only.

To control unauthorized access to critical operating areas, MDT will establish restricted areas and consider implementing appropriate measures such as:

- MDT will designate in writing which areas of the facility are considered restricted.
- All restricted areas should have a clearly marked perimeter barrier. Erect fences or other barriers to delineate a perimeter where natural barriers do not form a boundary.
- Block entry through windows to restricted areas (e.g., install bars on windows).
- All restricted areas should not allow access from the ceiling (i.e., drop ceilings).
- All restricted areas should be clearly defined and marked indicating that an area has restricted access. Markings indicating restricted areas should be posted and clearly visible to all personnel. Restricted areas should have a personnel identification and control system with all entrances/exits guarded, controlled, or secured with alarms.
- Limit the number of access points.
- Only those personnel whose duties require access to information or equipment should be allowed within restricted areas.
- Persons whose duties do not require access should be required to remain under constant escort while in restricted areas.
- Security personnel should perform routine patrols of restricted

areas, especially if no employees are present or the threat level is high.

- At heightened threat levels, procedures should be in place for personnel to guard or patrol restricted areas.
- Walls separating work areas on a raised floor (e.g., in computer rooms) where the level of security is different on either side of the partition should extend and completely shut off the area between the raised floor and the permanent floor.

- B. Level 2: Sensitive security areas shall be controlled to allow only authorized transit employee's access to those areas. Invitees may have access to the area in the company of an authorized transit employee only.

All persons entering and/or leaving non-public/secure facilities/areas within the transit system should possess and show a valid identification card or document to gain access. All passengers in vehicles must have valid identification. Identification must be presented to security personnel upon request. Security personnel or competent authority should verify that identification documents and applicable licenses or credentials match the person presenting them. In the event that an individual seeking access to the facility does not have an identification card that meets the requirements, only prescribed alternative means of identification should be accepted.

As the threat level dictates, the facility should develop a verification process to ensure that all persons requiring access to the facility have valid business at the facility. Vendors, contractors, truck drivers, and visitors should be scheduled in advance to the maximum extent

possible. If their arrival is not prearranged, entry should be prohibited until their need to enter is verified and vehicle inspected.

Valid identification cards or documents must be tamper resistant and at a minimum include the holder's name and a recent photograph of the holder. Any of the following may constitute a valid form of identification:

- Employer-issued employee identification cards
- Identification card issued by a government agency
- State issued drivers license (note that some states do not require photos)
- Labor organization identity card
- Passport

Guards should check vehicle drivers and passengers for proper identification, and check the vehicle for suspected bombs and suspicious packages. Persons arriving by motorcycle should be required to remove helmets to assist in identification. Guards should admit only authorized vehicles. Guards should detain visitors whose arrival is not expected at the entrance until cleared by authorized personnel.

A record should be kept of non-transit agency vehicles permitted access to secure premises. Security personnel should randomly verify the identity and identification of persons encountered during roving patrols.

The facility should have a process to account for all persons within the facility at any given time. Visitor identification should be displayed at all times and should be visually distinct from employee identification (orange is used by some agencies). Visitor ID should include an expiration date. Return of visitor IDs should be controlled and reconciled

daily. Place visitor-accessible locations in buildings away from sensitive or critical areas, areas where high-risk or mission-critical personnel are located, or other areas with large population densities of personnel.

C. Level 3: Moderate security areas shall be controlled to allow transit employees and controlled visitors to those areas. During nonworking hours, those areas shall be protected by the security requirements of the facility in which they are located. Security procedures for pick-ups and deliveries can include:

- Delivery orders should be verified prior to being allowed access to restricted areas. Shipping documents for deliveries should be checked for accuracy and items being delivered should be adequately described on documentation, including piece count if applicable.
- Pick-up and delivery appointments should be from known vendors only.
- Deliveries should be accepted only in designated areas.
- All packages entering or leaving the facility should be subject to search by security personnel. Signs should be posted at each access point to advise of this requirement.
- Facilities with a loading dock should have procedures in place to ensure that deliveries are supervised and not left unattended.
- Facilities employing a guard force should have guard force personnel notify facility management that a vehicle is en route to the loading dock.
- Where required, entry into the facility loading dock should be controlled and observed by CCTV. All personnel who may receive or make shipments should be aware of the procedures employed by the facility to ensure the security of the loading

dock area and all shipping and receiving procedures. Package inspection/screening requirements should also be reviewed.

- D. Level 4: Minimum security areas shall be those to which the public will have access during operating hours. During nonoperating hours, those areas will be protected by the security requirements for the individual facility.

8.1.3.2 ACCESS CONTROLS

Access control to non-public/secure areas of the MDT Transit System is essential. The most common access control barriers are swing doors, revolving doors, slam gates, turnstiles, and portals. These may be operated mechanically or electronically in conjunction with electromagnetic door locks, keyboard and memorized codes, encoded cards and card readers, video comparators (with or without guard assistance) and biometric identifiers. Automated access control systems can sometimes reduce the number of security staff by replacing them at entrance points.

Level 2 areas shall be controlled by the following security hardware requirements:

8.1.3.2.1 Locking Devices

Access to sensitive security area portals and equipment shall be controlled by pick, vandal and shear resistant locking mechanisms, key or combination activated. Also see Volume VII Section 7.05.11.

There shall be a Master Keying System prepared for all keys to locking devices on the transit system. Each system element or element subsystem shall be keyed differently from other elements/subsystems, but all like

element/subsystems shall be keyed alike. Wherever practical, a superior level key shall also activate the lock on a relevant subordinate level door, such as, the key to the Train Control and Communications room door shall also activate the ancillary area door, but the key to the ancillary area door shall not activate the lock to the Train Control and Communications room door.

8.1.3.2.2 Control of Locks and Keys

For effective control, accurate records should be maintained and dated, and semi-annual physical inspections and inventories should be made. Keys should be stamped "DO NOT DUPLICATE" prior to being issued.

8.1.3.2.3 Key Control Official

A key control official should be appointed in writing for every facility having control over its own locking system.

This official is responsible for the supply of locks and their storage, the handling of keys, records management, investigation of lost keys, ensuring hand receipts are signed for all keys issued and turned in, and the overall supervision of the key program at the facility.

8.1.3.2.4 Records Requirements

The key control official should maintain a permanent, secured record of the following:

- Locks by number
- The location of each lock
- The combination (if applicable)
- Date of last combination change or core change
- Keys by number
- Location of each key (un-issued key storage or hand receipts)

- Type of key combination of each key
- A record of all keys not accounted for
- Record, by name, of people to whom each key was issued.

8.1.3.2.5 Issue and Control Procedures

Issuance of keys should be kept to a minimum and take place under constant key control supervision. The following requirements apply:

- Keys, coded cards, and push-button combinations should be accessible only to those persons whose official duties require access to them.
- Combinations to push-button locks should be changed following the discharge, suspension, or reassignment of any person having knowledge of the combinations and at such other times as deemed appropriate. Combination changes should be done at least every six months.
- Keys that are not issued should be stored in a locked container that has been approved by the security manager.
- Access lists for persons authorized to draw keys should be maintained in the key storage container.
- Key containers should be checked periodically and all keys accounted for by documented semi-annual inventories.
- Keys must be retrieved from personnel transferred, discharged, suspended, or retiring and the employee's security codes should immediately be removed from electronic access systems. At times, it may be worthwhile to consider additional measures, such as changing locks, when a disgruntled employee leaves.
- Periodic re-keying of locks to secure areas should be considered to address normal key attrition problems.
- Key control systems should be inspected regularly and

malfunctioning equipment repaired or replaced.

8.1.3.2.6 Lost and Unaccounted-for Keys and Electronic Access Cards

When the results of the key inventories and inspections reveal that there are lost keys or access cards, the key control custodian should:

- Report the loss of unaccounted-for keys/access cards to the security manager, together with a list of the areas to which the keys provide access. Codes for lost access cards will be removed from the facility access control system.
- In coordination with the security manager and the facility manager, determine the extent to which locks should be recoded, changed, or otherwise modified to prevent compromise of existing safeguards.

8.1.3.2.7 Locksets

Locksets shall be heavy duty mortise type with corrosion resistant parts and finish, and shall contain a dead locking latch with a minimum of a 3/4 inch latch throw and stops in face.

8.1.3.2.8 Doors

Doors shall be constructed of hollow core metal, solid wood or solid core metal grill. Also see Volume II Section 1.09.7 for door fire rating.

8.1.3.2.8.1 Accessible Steel Grates and Doors

Grates and doors on ground level are other potential access points into a facility. These types of openings often serve as service entrances or exterior elevator entrances, or they may simply provide light and air to the basement level of the building. The mounting frame must be properly secured. The grates or doors can be welded into place, or they can be secured with a steel

chain and high security padlock.

8.1.3.2.9 Door Hinges

Hinges on doors which open outward shall be provided with nonremovable pins or security studs. Coordinate with hinge requirement in Volume II Section 1.09.7.

8.1.3.2.10 Door Jambs

Door jambs shall be fabricated from heavy gauge metal, treated to be corrosion resistant, with reinforcements at the strike and hinges.

8.1.3.2.11 Fencing

The top of the barrier shall be at least eight feet high with respect to the surrounding terrain, with three strands of barbed wire not more than six inches between strands of not less than 12-1/2 gauge wire with 14 gauge, four point barbs, pointing outward to prevent scaling. The bottom of the fencing shall be flush with the ground and the fabric of the fencing shall be at least nine gauge. There shall be a clear zone on the outside of the fencing devoid of trees or other objects which would conceal a person attempting to scale the fence.

8.1.3.2.11.1 Perimeter Fences

Perimeter fences define the physical limits of a facility or controlled area; provide a physical and psychological deterrent to unauthorized entry; channel and control the flow of personnel and vehicles through designated portals; facilitate effective utilization of the security force; provide control capability for persons and vehicles through designated entrances; and enhance detection and apprehension of intruders. Fencing can be used as a barrier in various locations:

- Perimeters of property parking lots and structures
- Bus yards, maintenance depots, etc.
- Vital facilities (power, fuel, etc.)
- Along track/right-of-way
- Pedestrian bridges

Fencing can range from high-security grill type fencing to common, low cost chain-link fencing. If the security threat is lower or if aesthetics are a high priority, ornamental fencing can also be used if it is properly designed to deter scaling. Typical fence requirements include:

- Perimeter fences and other barriers should be located and constructed to prevent the introduction of persons, dangerous substances or devices, and should be of sufficient height and durability to deter unauthorized passage.
- Areas adjacent to fences and barriers should be cleared of vegetation, objects and debris that could be used to breach them, or hide intruders.
- Boxes or other materials should not be allowed to be stored/stacked against or in close proximity to perimeter barriers.
- The fence line needs to be inspected regularly for integrity and any damage needs to be repaired promptly.
- Whenever locations permit, fencing should be located not less than 50 feet (15.2 meters) or more than 200 feet (61 meters) from the asset being protected.
- Any opening with an area of 96 square inches (619 sq cm) or greater, and located less than 18 feet (5.5 meters) above ground level outside the perimeter or less than 14 feet (4.3 meters) from controlled structures outside the perimeter barrier, should be provided with security equivalent to that of the perimeter.

- If a body of water forms any part of the perimeter barrier additional security measures should be provided.
- A fence that is at least 4 feet (1.25 meters) high can be used as a barrier to guide pedestrian movements.

Although low-level risks may be controlled with a perimeter fence, fences alone will not stop a determined intruder or a moving vehicle attack, and will resist impact only if reinforcements are added. To control identified risks, agencies should enhance the effectiveness of fencing with lighting, CCTV, fence sensors to detect climbers or cutting actions, and/or augmented by security force personnel. A fence that is not protected with intrusion-detection equipment may be vulnerable to attack and unauthorized access if it is not under constant surveillance by security personnel.

8.1.3.2.11.2 Clear Zones

Clear zones for security fences should meet the following requirements:

- Fences should be constructed so that an unobstructed area or "clear zone" is maintained on both sides of the barrier to make it more difficult for a potential intruder to be concealed from observation.
- Whenever practical, exterior and interior clear zones should be 20 feet (6 meters) or more. The clear zone should be free of any object or feature that would offer concealment, such as a physical structure or parking area, or which could facilitate unauthorized access such as an overhanging tree limb.
- When a clear zone is not practical, other compensatory measures may be necessary to control access to secured areas. Appropriate supplemental protective measures include increasing the height of portions of the fence, providing increased lighting, CCTV

surveillance cameras monitored from a remote location, installation of intrusion-detection sensors and security patrols.

8.1.3.2.11.3 Fence Fabric

The most common type of physical barrier for perimeter control is chain-link fencing, often installed with barbed-wire outriggers. It is flexible, relatively inexpensive, and easy to install around any size and shape of structure/security zone. These guidelines focus on chain-link fencing, but agencies should look at alternatives, such as expanded metal fencing in areas of greater risk, e.g., where vandalism is high.

Fencing fabric should meet the following requirements designed to increase fence performance:

- Fences, including gate structures, should be number 9-gauge or heavier chain-link fabric. Fabric should be aluminum or zinc-coated steel wire chain link with mesh openings not larger than 2 inches (5.08 cm) on a side.
- Fence fabric should be attached to the exterior side of line posts using not less than 9-gauge steel ties.
- Fence height should be a minimum of 8 feet (2.4 meters) to deter unauthorized passage. This includes a fabric height of 7 feet (2.1 meters) plus a barbed-wire/razor wire outrigger extension of 1 foot (0.304 meters).
- The distance between the bottom of the fence fabric and firm packed ground should not exceed 2 inches (5.08 cm).
- When the fencing is being installed on soft ground, the fabric should reach below the surface sufficiently to compensate for shifting soil. To prevent individuals or objects from going under the fence, a cement apron not less than 6 inches (15.2 cm) thick can

be installed under the fence. The fence fabric can also be extended below the bottom rail and set in the concrete. Exposed surface of concrete footings should be crowned to shed water.

- Pipe framing can be installed on the fabric where it touches the ground, or 2-foot (0.6 meter) long U-shaped stakes can be used to fasten the fabric to the ground. Fence fabric should be attached to terminal posts with stretcher bars that engage each fabric link. The stretcher bars should be held to the fence post with clamps in such a way as to hold the fabric taut.
- If exterior intrusion-detection systems are to be mounted, the maintaining of constant fabric tension (minimum horizontal tension of 1,000 pounds) will greatly reduce sensor vibration.
- A tension wire should be stretched from end to end of each section of fence and fastened to the fence fabric within the topmost 12 inches (30.5 cm). Taut reinforcing wires, a minimum of 9-gauge, should be installed and interwoven with or affixed with 12-gauge fabric ties spaced 12 inches (30.5 cm) apart along the top and bottom of the fence fabric.
- Salvage should be twisted and barbed at top and bottom.
- Metal fencing should be electrically grounded.
- If a masonry wall is used as the perimeter barrier, it should be at least 7 feet (2.1 meters) in height with a top guard of barbed wire or at least 8 feet high with broken glass set on edge and cemented to top surface.
- If building walls, floors, or roofs form a part of the perimeter barrier, all doors, windows, and openings on the perimeter side should be properly secured.

8.1.3.2.11.4 Posts and Hardware

All fence posts, supports, and hardware for security fences should meet the following requirements:

- All fastening and hinge hardware should be secured against attempts at unauthorized removal by peening or spot welding to allow proper operation of the components but deter disassembly of fence sections or removal of gates.
- The bolts securing the clamps to the posts should be peened or otherwise modified in a manner to deter attempts at unauthorized removal.
- All posts and structural supports should be located on the interior of the fence. Posts should be spaced not more than 10 feet (3 meters) apart and should be embedded in bell-shaped concrete footings to a depth of 3 feet (0.61 meters) to prevent shifting or sagging.

8.1.3.2.11.5 Openings

Agencies should consider the following requirements for maintaining the fence's integrity when traversing culverts, troughs, ditches, or other openings:

- Openings should terminate well within the secure area defined by the perimeter security fence barriers.
- If perimeter security fence barriers must traverse culverts, troughs, ditches, or other openings 96 square inches (619.4 sq cm) or greater in area and larger than 6 feet (1.8 meters) in any one dimension, the opening should be protected by an extension of the fence construction. This extension may consist of iron grills or other barrier structures designed to prevent unauthorized access.
- Bars and grills should be installed in such a way that they do not impede required drainage. Hinged security grills used with an approved high security hasp, shackle, and padlock, which can be

opened when necessary, are often a workable solution to securing drainage structures.

8.1.3.2.11.6 Gates

8.1.3.2.11.6.1 Perimeter Gates

The number of perimeter gates designated for active use should be kept to the absolute minimum required for operations. Sufficient entrances to accommodate the peak flow of both pedestrian and vehicular traffic, as well as adequate lighting at egress and ingress points should be considered.

Gates should be of such material and installation as to provide protection equivalent to the perimeter barriers of which they are a part.

The space between the bottom edge of the gate and the pavement or firm ground should not exceed 2 inches (5.08 cm).

All entry gates should be locked and secured or guarded at all times or should have an effective entry detection alert system.

Gates over 6 feet (1.83 meters) in height should have locks at the top and bottom to ensure that the gate cannot be pried open a sufficient distance to allow unauthorized entry.

Vehicular gates should be set well back from the public highway or access road in order that temporary delays caused by identification control checks at the gate will not cause undue traffic congestion.

Sufficient space is provided at the gate to allow for spot checks, inspections, searches, and temporary parking of vehicles without impeding traffic flow.

At least one vehicle gate that is at least 14 feet (4.3 meters) wide for each enclosure should be provided to permit entry of emergency vehicles.

For facilities employing a security force, a security guard house can be provided at the site perimeter for permanent manned gates.

Fenced facilities employing electronic card access systems should consider configuring the main employee entrance gate with an automated entry control system with CCTV for visual assessment capability.

8.1.3.2.11.6.2 Unattended/Inactive Gates

Consider the following requirements for unattended/inactive gates:

- Unmanned gates should be securely locked at all times.
- Security lighting should be provided to deter attempts at tampering during the hours of darkness.
- Perimeter intrusion-detection system (PIDS) and CCTV protective measures are appropriate when necessary to meet identified risk control requirements during those periods when the gate is not under the direct visual observation and control of a security officer.

8.1.3.2.11.7 Wall/Roof Openings

Wall structures and masonry barriers present potential vulnerabilities for restricting access at a facility, particularly where light construction or improper securing of structural elements would enable an intruder to gain access. A common example is a shared wall between adjacent rooms, one of which is a restricted area.

When a vulnerable wall separating controlled space from an adjacent non-

controlled space is identified, countermeasures to reduce risk to an acceptable level are needed. The objective is to secure the wall with a level of physical security to match the value of the assets being protected and the threats.

Transit system building structures or rooms which have windows with louvers, air ducts, air vents or other openings in roofs or exterior walls, where such openings exceed eight inches in the least dimension, shall be provided with a formidable barrier securely fastened, and when installed outside, the fasteners shall be nonremovable with common tools. Exterior doors with louvers shall not be used if there is any alternative. If there is no alternative, the louvered area shall be protected as above.

Designers should follow these wall safeguard guidelines relating to interior wall extension, reinforced wall, and intrusion-detection sensors.

8.1.3.2.11.7.1 Extending Interior Wall Construction to Ceiling or Roof Deck

This is often possible when the vulnerability is caused by a wall that does not extend entirely from floor to ceiling, providing the potential for illicit access over the top of the wall.

Possible solutions include extending the wall to the ceiling or constructing an expanded metal barrier to close the intervening space between the top of the existing wall and the ceiling.

When the primary concern is merely to detect unauthorized access attempts, lightweight construction such as plasterboard can be used. When lightweight materials are used, consider installation of an intrusion-detection sensor in the ceiling space to detect attempts at forced entry.

8.1.3.2.11.7.2 Reinforced Wall

Covering the entire wall with 9-gauge expanded metal may be appropriate to control identified risks.

8.1.3.2.11.7.3 Intrusion-Detection Sensors

If the primary concern is that entry may be possible by forcible means without detection, as might be the case in a storage room or similar area, the use of intrusion-detection sensors can be an effective solution.

Vibration detectors placed on a wall surface is one way of sensing attempts at forcible entry through a wall.

8.1.3.2.11.8 Miscellaneous Openings

Preventing inappropriate access to a facility requires physically securing storage, roof, and mechanical areas, as well as outdoor air intakes of the building's HVAC system. Miscellaneous openings include fire escapes, utility manholes, sewer manholes, storm drainage manholes, catch basins, culverts, drains, steel grates and doors, rooftop access points, tunnels, and sidewalk elevators.

Agencies should follow these guidelines relating to fire escapes, manholes, accessible steel grates and doors, sewers and storm drains, rooftop access points and air intakes.

8.1.3.2.11.9 Miscellaneous Fire Escapes

Exterior fire escapes usually do not provide access directly into a building. If a fire escape is not properly designed it can provide a potential intruder with easy access to the roof or to openings high above ground level. Physical

security safeguards must be coordinated with appropriate fire and safety officials to ensure they do not interfere with emergency systems, procedures, or equipment. In some instances, it may not be possible to reduce completely the physical security hazard posed by a fire escape or similar safety feature. In these cases, alternative security measures are necessary to control identified risks, such as CCTV, IDS, and guard patrols.

Windows or other openings leading off fire escapes should meet both security standards and life safety code requirements if they provide potential access points for an intruder. Measures taken to secure windows must be coordinated with the appropriate fire and safety officials to ensure that they do not impede safety processes.

To promote security, the fire escape should not extend all the way to the ground. If the fire escape must reach all the way to the ground for safety reasons, alternative security safeguards that meet life safety requirements may be needed.

Coordination with fire and safety officials is necessary in relation to any security measures directly affecting the fire and safety systems and procedures.

8.1.3.2.11.10 Miscellaneous Manholes

Manholes can provide entrances into buildings for service purposes, or provide access to utility tunnels containing pipes for heat, gas, water, telephone transmission conduits, cables, and other utilities.

Manhole covers must be adequately secured if they provide access to a building or to any communications or utility lines servicing that building or

operation.

A case hardened chain and high security padlock can be used to secure a manhole cover; the use of a heavy-duty hinged-steel dead bar secured with a high security padlock and heavy-duty hasp is an alternative method.

8.1.3.2.11.11 CCTV Cameras and Other Security Systems

CCTV cameras, where used, shall contain burn in resistant image conversion tubes capable of operating in light ranges to which they will be exposed. Cameras in public or exposed locations shall be out of reach of the public and protected by weatherproof, tamper resistant housing with easily replaceable lenses. Security systems include CCTV, remote surveillance devices, video recorders, intrusion and motion detectors, tamper detectors, smoke or chemical detectors, and alarms.

Since constant surveillance by on-site personnel is often infeasible, the practice must be supplemented with other measures that can expand the ability of security staff to monitor large facilities. Surveillance equipment may be particularly appropriate in high-traffic and high-value areas since these systems can be integrated with other monitoring and communications systems to create a coordinated oversight and response center.

While remote surveillance and detection systems are important for identifying suspicious activity, MDT's response plan should consider what actions to take once these activities have been identified. If possible, the systems should be designed so that a response team can prevent the threat from being carried out. In order for this to occur, there needs to be contact between those monitoring the alarms and local responders so that action can be taken quickly. Where possible, additional mechanisms, such as secondary locks or

barriers, high-pitched alarms or pepper spray, should be used to thwart an attacker, to provide time for a response team to arrive and intercede.

Cameras can be either stationary or remotely/locally adjustable (pan/tilt/zoom) to make sure that they provide surveillance to the entire target area. A surveillance system that feeds video to a monitor for real-time observations is generally considered better for security, but is labor-intensive and requires constant diligence. As such, these systems should be tempered with other measures: operationally, technically or both. Real-time observations can be supplemented if the surveillance system has integrated sensors and alarms. This "exception detection" method alerts security personnel when something abnormal occurs. Recorded feeds to be used for investigation are another option.

Sending feeds to a central, off-site location is preferable to on-site monitors. While some agencies prefer cameras and monitors to be available to on-site staff, remote monitoring can be more effective in the event of an evacuation. Consider how emergency responders can plug in locally to video feeds for on-site cameras.

When designing a remote surveillance system, it is important to consider potential obstacles to full surveillance, such as structural columns and sharp corners, when positioning cameras. Where a single camera cannot capture the entire area, multiple cameras can be set up to provide overlapping coverage areas. Consider motion detectors and other alarm systems as part of the security system design, to provide maximum coverage with a minimum of false alarm opportunities. These systems can be used in combination with other access management tools to provide an efficient and dependable security system.

These security measures can be used as deterrents if they are designed to be obvious. Conspicuous surveillance measures provide a heightened sense of security, but they are also more vulnerable to vandalism. Vandal-proofing of these systems is key to their proper functioning. Agencies should consider placing cameras, detection devices, and wiring beyond reach in secure enclosures. Surveillance cameras and other security technology can also be used to monitor an area covertly.

8.1.3.3 LEVEL 1 SECURITY HARDWARE DEVICES

8.1.3.3.1 Locking Devices

An effective lock and key issuance and control system is essential to the safeguarding of property and controlling access.

Access to critical security area portals shall be controlled by a high security pin tumbler key activated, combination activated or electrically activated locking mechanism.

Access to critical equipment shall be controlled by a high security tubular, key activated locking cylinder with multiple tumblers and driving pins arranged to provide two lines of cleavage and fast key operated combination change.

8.1.3.3.1.1 Locksets

Locksets shall be heavy duty mortise type with corrosion resistant parts and finish, and shall contain a dead locking latch with a minimum of a 3/4 inch latch throw and stops in face and a one inch throw, saw resistant deadbolt, mechanically or electrically controlled.

8.1.3.3.1.2 Doors

Doors shall be constructed of solid metal, metal clad solid wood core, or hollow metal with horizontal metal stiffeners.

8.1.3.4 KEY CONTROL

Procedures and policies shall be prepared to control access to the various security levels by appropriate transit employees and shall be accomplished through key control and color coded identification cards. Issuance of keys should be kept to a minimum and take place under constant key control supervision. The following requirements apply:

- Keys, coded cards, and push-button combinations should be accessible only to those persons whose official duties require access to them.
- Combinations to push-button locks should be changed following the discharge, suspension, or reassignment of any person having knowledge of the combinations and at such other times as deemed appropriate. Combination changes should be done at least every six months.
- Keys that are not issued should be stored in a locked container that has been approved by the security manager.
- Access lists for persons authorized to draw keys should be maintained in the key storage container.
- Key containers should be checked periodically and all keys accounted for by documented semi-annual inventories.
- Keys must be retrieved from personnel transferred, discharged, suspended, or retiring and the employee's security codes should immediately be removed from electronic access systems. At times, it may be worthwhile to consider additional measures, such as changing locks, when a disgruntled employee leaves.

- Periodic re-keying of locks to secure areas should be considered to address normal key attrition problems.
- Key control systems should be inspected regularly and malfunctioning equipment repaired or replaced.

– Intentionally Left Blank –

8.2 SYSTEM PROCEDURES SECURITY CRITERIA

- A. A receptionist/guard shall be positioned at the main entrance of the Administration Facility. Transit employees shall be permitted to enter upon displaying their identification card, which will then be worn on the front, outside of their clothing while they are in the facility. Designated personnel should conduct roving safety and security patrols in facility areas with limited or irregular staff presence.
- B. Visitors to the Administration Facility shall be required to sign in and out with the receptionist/guard who will issue a color coded card which will restrict the visitor to a particular area or floor. The visitor will be required to wear the color coded card on the front outside of his/her clothing while in the facility. As the threat level dictates, the facility should develop a verification process to ensure that all persons requiring access to the facility have valid business at the facility. Vendors, contractors, truck drivers, and visitors should be scheduled in advance to the maximum extent possible. If their arrival is not prearranged, entry should be prohibited until their need to enter is verified and vehicle inspected.
- C. If the Maintenance Facilities are located in an area which presents security problems, there should be security guard patrols of the facilities perimeter. Guards should check vehicle drivers and passengers for proper identification, and check the vehicle for suspected bombs and suspicious packages. Persons arriving by motorcycle should be required to remove helmets to assist in identification. Guards should admit only authorized vehicles. Guards should detain visitors whose arrival is not expected at the entrance until cleared by authorized personnel.
- D. Revenue transportation shall be by the most protected, efficient,

expedient means available. Vehicles operate as part of larger transit systems that have many components, such as stations, stops, tracks, and roadways. A vehicle's overall design must result in the vehicle being physically and operationally compatible with the other elements of the system. Likewise, the vehicle's security-related design elements must be compatible with facility elements, during both everyday operations and emergency situations.

The security of vehicles affects the security of facilities, and vice versa. While this chapter presents design-oriented considerations specific to transit vehicles, agencies should be aware that attacks on vehicles can have serious consequences for transit facilities and that incidents occurring in transit stations will also impact the vehicles. MDT will benefit if vehicles are designed to promote the security of both the vehicles themselves and the other components of the transit systems.

- E. If fare encoding equipment is used, access to the equipment and its use shall be held to a practical minimum of authorized transit employees. Procedures shall be developed which will identify any employee misusing his or her responsibility. Employees using fare encoding equipment shall be subject to a thorough background investigation and to appropriate methods of testing. Fare encoding equipment shall receive the same physical protection as if it were revenue.
- F. To the extent feasible, the handling of cash by transit employees shall be kept to a minimum. Policies and procedures shall be developed which will remove the opportunity for transit employees to convert revenues to their own use. These employees shall be subjected to thorough preemployment investigations and appropriate methods of testing.

- G. Police patrols on trains shall be used for special situations only and shall not be a regular part of the of the security system.
- H. The law enforcement officers assigned to the transit system shall be on a permanent basis. They shall be provided with special training by the transit system to contend with problems unique to a rail rapid transit system. A well-trained and equipped security force provides an effective means for implementing and monitoring the provisions of an agency's access management program. The guard force should be used as an extension of access management systems and represents a major opportunity for risk reduction through effective implementation of facility security policies and procedures.

There are many options for security forces including a sworn police department, guards employed by the transit agency, contract guards, or a combination of these arrangements. The type of force(s) employed, types of operations and the tactics utilized (uniformed/uniformed; patrol/fixed post/random; mounted/K-9/cycle) can be tailored to the specific transit agency.

- I. The Security Console at the Central Control Facility (CCF) shall have redundant telephone communication capabilities to the central dispatching facility of the law enforcement agency. In light of the potential for a system attack or other destructive event, MDT should consider their level of reliance on communications systems and agency resilience to attack. MDT should also consider how well they can communicate accurate, timely information when reacting to an emergency event:
- To allocate resources and prioritize responses

- With other emergency services to coordinate a response
- With the traveling public to keep them aware of service interruptions and changes in service

Emergencies provide a significant challenge to current telecommunications systems, particularly since technology may be compromised at the very moment that the demand for information is greatest. In addition, most transit agencies do not have the ability to directly communicate with other emergency responders.

MDT should consider how to improve methods of communicating during emergencies, both internally and with emergency responders. Transit agencies should also be aware of what other area public safety agencies are doing, or planning to do, to achieve interoperability among their respective communications systems. They may also consider being part of a state or metropolitan area initiative with those area agencies.

- J. Law Enforcement will be responsible for the enforcing of all present and future laws and ordinances on transit system property. They shall assist in the development of fast and vigorous prosecution of persons arrested on transit property. Security forces can include:
- Uniformed guards
 - Fixed posts
 - Random foot patrol within post area
 - Directed patrol within post area
 - Visibility posts
 - System or zone-wide random patrol
 - System or zone-wide directed patrol
 - Vehicle patrol

- Mounted patrol
 - K-9 patrol
 - Alternate vehicles (bicycle, scooter, electric cart)
 - Fare inspection
 - Emergency services unit
 - Monitoring surveillance cameras
 - Armed individuals
- K. The Office of Safety and Security shall be responsible for providing the trained manpower requirements of security which do not include direct law enforcement, such as security guards, watchmen, etc. Contract guard requirements, responsibilities, and qualification criteria should be established and considered in the decision to employ a contract security guard force.
- L. All transit system employees shall be provided with color coded photo identification cards which shall be worn on the front outside of their clothing while at their assigned tasks. If a computerized access system or timekeeping system is adopted, the identification card can be used for the dual purpose. Access control technology is advancing rapidly; many of the biometric devices currently in use were not available until recently. When used in conjunction with physical barriers and CCTV, access control systems enable security personnel to monitor and protect vital assets, such as power facilities, control centers, and computers, more effectively. Electronic access control systems, such as key card systems, have the advantage over conventional key systems in that lost or revoked credentials can be immediately deactivated with minimal cost. In addition, automated entry-point screening systems can sometimes replace guards at some entrances.

Material screening systems complement access control measures. Access control limits who enters a facility or a secured area, while screening systems limit what enters those areas. Screening systems can detect the presence of prohibited items, such as weapons, explosives, or chemical/ biological / nuclear radiological (CBNR) materials. They utilize a range of technologies (such as x-ray machines and metal detectors), and can be deployed at entry points or throughout a facility.

- M. There shall be a separate internal audit unit within the transit agency responsible for the auditing of all transit revenue funds, for assigning accountabilities and for the investigation of suspected larceny. Procedures shall be developed and monitored by the auditors which will protect the transit revenues for the proper authority.
- N. The Office of Safety and Security shall be responsible for conducting pre-employment investigations of transit employees who will be operating in critical areas or who have anything directly to do with revenues. Pre-employment background screening should be performed as a means of verifying applicant data prior to hiring. This may be included as part of the Transportation Worker Identification Credential (TWIC) program initiated by the Transportation Security Administration. Also note that background screening requires in-depth knowledge of the federal Fair Credit Reporting Act (FCRA) and the laws of all 50 states.

Suggested security measures include:

- Pre-employment screening should apply to all regular and non-regular positions, including rehires for designated positions (e.g., front-line operations, maintenance employees, and

security/law enforcement) and rehires with a separation greater than 30 days for any position.

- A waiver policy should be established to handle hiring prior to completion of background screening for non-designated positions. No exemptions to pre-employment background checks involving designated positions should be permitted.
 - Criteria for evaluating background reports should be established. Policies should be in place to determine whether the agency will employ someone with a less than perfect background. Acceptable past events (e.g., youthful offenses, non-violent crimes, arrests without prosecutions, etc.) should be defined.
 - Develop appropriate security practices for voluntary and involuntary termination of employees. Issues include how the employee's agency identification is recovered, how the security staff is notified, and how credentials are revoked.
 - Any decision on employment, or on discipline or termination of a current employee, as a result of information generated by the background checks should be reviewed for consistency and endorsed by recruiting and employment, security and labor/employment law.
 - Background reports by their nature are sensitive and confidential, and by law must be restricted to those individuals who are directly involved in the hiring process.
- O. The Office of Safety and Security shall be responsible for developing a comprehensive incident reporting and filing system based upon APTA proposed standardized forms (Vandalism and Passenger Security, American Public Transit Association, prepared for Department of

Transportation, September, 1973, distributed by National Technical Information Service, Ch. III, Appendix D, Page 35) for uniform reporting, records keeping and the interchange of information with other rail rapid transit properties.

- P. The Office of Safety and Security shall be responsible for enforcing all security rules and regulations developed by MDT on transit property.

- Q. Station Attendants, operating, maintenance and key operations personnel shall receive special security training to prepare them to cope with security threats to patrons, employees and the system. Training shall be comprehensive, but tailored to the needs of the specific work assignment. The effectiveness of the security system depends upon the proper use of security equipment and communications procedures, so the training shall be based upon the recommendations of law enforcement and emergency assistance agencies.

- R. Those transit employees who will have direct regular contact with the public, such as Station Attendants, shall receive first aid training and periodic refresher courses conducted by a recognized authority.

8.3 SYSTEM ELEMENT SECURITY DESIGN

8.3.1 STATION FACILITIES

8.3.1.1 GENERAL

Each station should be reviewed with respect to its location in the context of crime exposure for that area to establish the most appropriate security equipment. Transit stations are designed for convenient access, typically by large numbers of riders and agency staff. Stations may include access for a single, discrete transit line, or may feature transfers to other lines or services. For safety and security reasons, there are areas that must be inaccessible to the public and still other areas that must be inaccessible by vehicle.

8.3.1.2 STATION PERIMETER

The station concourse area shall be protected by a formidable physical barrier. Refer to Volume II Section 1.04.9.2.

The design of the barrier shall allow maximum natural light and ventilation and visibility to the interior of the station and shall be constructed in a manner which will preclude its use as a means of scaling. All entrances and exits shall be designed to permit easy positive closure by operating personnel and shall contain locking devices.

It is impractical to establish a strong perimeter around a transit station, even though it is often necessary to pay and pass through admissions-control barriers to enter the platform. Stations must be as accessible as possible to potential patrons arriving both by foot and in vehicles.

A transit station may have a range of other entrance types depending on the modes served, including tunnel portals for rail service or on-the-road throughways for buses to approach docking areas. Some of these entrance

types may warrant additional security measures to prevent inappropriate vehicle access, which need not compromise passenger mobility. In addition, selecting a site where it is possible to maintain unobstructed sightlines around key access points or critical areas may also improve security without compromising the station's accessibility.

8.3.1.3 ANCILLARY SPACES

All ancillary spaces shall be physically separated from the public areas by independently securable barriers to deter entry by unauthorized persons. A means shall be provided to detect intruders.

8.3.1.4 VISIBILITY

Stations shall feature as much open area as possible with long unbroken lines of sight, eliminating all dark or obscure areas on both the concourse and platform levels. Natural elements, such as rolling hills and steep terrain, can provide hiding places for aggressors and hinder visual surveillance by security personnel. High points on the site elevate buildings where they are easily visible from off-site and therefore vulnerable to weapons fire from unsecured areas. Consider avoiding topography and vegetation that prevents clear lines of sight from the site to avoid making it easy for potential attackers to approach the site without notice.

Dense trees and shrubbery present similar challenges. Portions of sites (especially larger sites) are often left in their natural state, which can include steep terrain and dense vegetation. This occurs for a variety of reasons including unsuitable terrain, zoning or environmental regulations, and land banking for future use. Where these situations exist, consider perimeter protection to separate those areas from the developed portion of the site, to prevent them from being used for a covert approach to valuable assets.

8.3.1.5 CONCESSIONS

Concessions of all types shall be prohibited in the station area, other than newspaper vending machines in the free area only. All other concessions will be at MDT's discretion.

8.3.1.6 RESTROOMS

Restrooms in passenger stations shall be of the single occupancy type for the use of transit system personnel and for the emergency use of transit system patrons, located within the paid area of the concourse close to the Station Attendant's booth and under his/her visual or electronic surveillance. The restroom door shall have no identifying signage and shall normally remain closed and locked. The restroom door lock shall be electronically controlled by the Station Attendant to admit one person. A push to talk call box within the facility shall allow a person to signal the Station Attendant at the booth.

8.3.1.7 STATION PROTECTION

The station design shall provide access for emergency vehicles as close to the station structure as possible. A means shall be provided for fast and easy access into the station structure for emergency assistance personnel. A station's emergency response plan should consider the capacity of the station and the fact that many users will not be familiar with the layout of the station and its emergency exits. Emergency systems can direct occupants to safe exit locations, especially if there are additional exits that are not commonly used for station access.

Consider including emergency communications systems, including blue-light phones and public address systems, in the plan, to allow rapid communications between remote areas of the station. Stations should be

equipped with emergency lighting, sprinkler systems and safe rooms, if there are subway or elevated platforms.

8.3.1.8 LIGHTING

Station facilities illumination shall be in accordance with Volume II Chapter 4 Station Electrical Design Criteria of this Compendium. Security shall be a major design consideration in the selection of illuminating levels. Non operating hours illumination shall be equivalent to emergency illumination levels, or one foot candle, whichever is greater. (See section 8.1.2.5.1.3 for Types of Lighting)

8.3.1.9 LOCKERS

Public lockers shall be excluded from the design of all stations.

8.3.1.10 PARKING FACILITIES SECURITY

- A. The design of the parking structure shall allow maximum natural light and visibility to the interior of the structure. The structure shall be provided with an attendant on duty during the operating hours or by regulated security patrols.

The Designer shall consult with MDT on the need for special rooms/booth or other support facilities needed in parking structures.

All vehicle and pedestrian entrances to the facility should be illuminated.

Lighting at manned entrances must be adequate to identify persons, examine credentials, inspect vehicles entering or departing the facility premises through designated control points (vehicle interiors should be clearly lighted), and prevent anyone from slipping unobserved into or out

of the premises.

Entry lighting should be sufficient to allow for personnel identification during times of darkness and extreme environmental conditions.

Lighting intensity at entrances should be planned to ensure that arriving drivers can readily recognize the premises and see where to drive their vehicle.

Lighting should not be placed to cause blinding of the driver.

Semi-active and unmanned entrances should have the same degree of continuous lighting as the remainder of the perimeter, except that additional, standby lighting should be available to provide the same illumination required for manned entrances when the entrance becomes active.

Gate houses at entrance points should have a reduced level of interior illumination to enable the security guards to see better, increase their night vision adaptability, and avoid illuminating them as a target.

- B. Parking facilities shall be provided with access control to minimize the exposure of patrons and their vehicles to injury, loss or vandalism. Vehicle controls can most appropriately be applied at those transit facilities that are not typically open to the public-such as administrative offices, maintenance facilities, and operation control centers-as a way to deter unauthorized or illegal access. Some of the methods listed here may also be applied around suburban transit stations or other public facilities with significant available parking and a steady flow of pick-

up/drop-off traffic.

Agencies should follow these vehicle control and parking guidelines for vehicle inspection, facility parking/traffic control, adjacent parking, parking registration/vehicle ID, unauthorized vehicles, vehicle access points, high-speed vehicle approaches, drive-up/drop-off locations, and electronic vehicle access control;

1. Where required, access to non-public parking should be limited to transit agency vehicles, personnel, contractors, and authorized visitors. This can be accomplished by use of a trained guard force, parking lot barriers such as barrier arms, or at a minimum, designation and identification of authorized parking spaces.
2. Visitor parking should be clearly marked and should be as close as possible to the visitor reception area of the facility. Parking should not be permitted close to or against perimeter barriers. Handicapped parking may be allowed within the established buffer zone if the vehicle and operator are identified to the staff responsible for parking control.
3. Whenever possible, parking areas for all transit and staff vehicles should be located inside the perimeter of protected areas.
4. Where possible, parking areas for general vehicles should be located outside a facility's buffer zone. Parking should not be allowed within 100 feet (30.5 meters) of the building exterior, when possible. Parking areas may be fenced and should be well lighted in accordance with the existing illuminance specification.
5. Parking within the facility should be restricted only to those areas indicated in a facility physical security plan.
6. Parking lot activity should be monitored either visually or by CCTV.

7. Parking regulations should be strictly enforced.
 8. Emergency communication speakers should be installed in the parking area in order to broadcast emergency procedures and/or instructions.
 9. Vehicle entry and exit routes should be clearly marked.
 10. A facility should have formal procedures for controlling vehicle access and parking.
- C. Illumination of the parking facilities shall be consistent with other operating and security requirements in accordance with lighting requirements as per Volume II Section 4.07 of this Compendium.

Parking areas should be provided with uniform illumination sufficient to allow for personnel identification during times of darkness and extreme environmental conditions.

Parking lot and entry emergency lighting systems at facilities should be connected to the emergency power system, to ensure they remain operational during periods when commercial power is interrupted at critical facilities

8.3.1.11 TRACTION POWER EQUIPMENT

A. Traction Power Substation Structure

Access to the Traction Power Substation structure shall be controlled by appropriate locking devices. There shall be a means of detecting intruders. Exterior equipment shall be protected by a nonscalable barrier. Remote or unmanned equipment plays a less visible, but critical, role in the transit. The isolated locations and open design of these facilities make them vulnerable to attack. The most effective strategies

for mitigating attacks on these facilities are physical hardening and providing redundancies within the transit system's power or communications network, along with access management for particularly critical structures or those located in notably vulnerable locations.

The probable objective of any attack on a substation is to incapacitate it through damage or destruction, and prevent it from providing power to the transit system.

Most substation sites are small areas with no on-site personnel. Typically, the only equipment on-site are transformers and associated equipment; there may also be a small utility building. Since transit agencies generally obtain their power through the public grid system, agencies might have little or no control over the siting, design, and construction of these substations. When the agency does own the substation, they can use the principles of hindering accelerated approaches, access control, and remote surveillance as appropriate. Many of these same attributes apply to other remote or unmanned structures, including communications towers, etc.

Current practice and applicable codes require clearances around substations along with other requirements, based on fire protection concerns rather than blast-related stand-off distances. These standards also dictate that access be limited to qualified personnel.

B. Gap Tie Stations

Gap tie station structures shall receive the same security protection as the Traction Power Substations.

8.3.2 GUIDEWAY FACILITIES

8.3.2.1 BARRIERS

At-grade sections of the guideways shall be protected by a nonscalable barrier of suitable height to deter the hurling of objects onto the guideway. Security barriers shall be used on all structures, overpasses and other appropriate areas to protect the rapid transit vehicles and guideways from thrown objects. Bollards are used frequently to surround the limits of the structure or facility to protect the facility from "bumping" by vehicles. These are typically passive barriers, such as concrete-filled bollards, designed to stop accidental collisions.

8.3.2.2 EMERGENCY ACCESS

At regular intervals along the guideways, provisions shall be made for controlled access to the guideway for emergency assistance agency respondents. Emergency Access to all guideways shall be as per NFPA-130 as well as AHJ directions. Some rights-of-way are wide enough to provide a drivable or navigable area along side the track. Others sections through remote locations or those flanked by building are less accessible. In this case the only access is along the right-of-way itself. Consider developing emergency evacuation and access routes for all segments within the rights-of-way as part of an emergency response plan. Also consider factoring the presence of a live "third rail" into any plans involving the evacuation of passengers by responding emergency personnel.

8.3.2.3 INTRUSION DETECTION

Where the at-grade guideway centerline of main track is within 25 feet of the curblines of a parallel major arterial roadway; where the maximum allowable speed on that roadway is sufficient for an automotive vehicle to intrude onto the at-grade guideway and no adequate barrier protection is provided,

methods of detecting the intrusion of such automotive vehicles in said areas shall be proposed to MDT.

Where the elevated guideway support columns are within 10 feet of the curblineline of a parallel or intersecting major arterial roadway; where the maximum allowable weight of an automotive vehicle traveling at the maximum allowable speed could inflict structural damage to a support column and no adequate barrier protection is provided, methods of detecting the intrusion of such automotive vehicles in said areas shall be proposed to MDT.



8.3.3 TRAIN CONTROL SECURITY

8.3.3.1 THE CENTRAL CONTROL FACILITY

Access to Central Control, also known as Central Control Facility (CCF), shall be strictly controlled. It is probable that the Central Control Room will be a prime attraction to visitors. Consideration should be given to permit visitors to view the Central Control Room without entering, such as through a large window. Provisions shall be made to detect intruders into the Central Control Room. Operations activities include ongoing supervision of tracks and

signals, vehicle tracking, communications with all fleet vehicles, and emergency response.

8.3.3.2 SITE ANALYSIS

Central Control Facility sites differ from most other types of transit infrastructure in that they do not need to be located for public convenience and are best sited in out-of-the-way, inconspicuous locations. For activities that are critical to system operation, such as operations control, redundant facilities in separate locations may help ensure full or partial operations in the event of an attack on a primary facility. Because hardened facilities may be expensive to establish and maintain, a transit agency may consider co-locating some of their facilities with other agencies that have similar security goals.

Most importantly, planners should consider a site with a securable perimeter, setting the building back from any public roadways. Within the site perimeter, on-site parking can also be setback from the building, potentially with separate areas for visitor and employee parking, and entrances located so they do not face the street directly. Consider planning a buffer zone that separates the facility from neighboring land uses with unobstructed sightlines. Designers may use lighting to improve visibility from the structure at night as well as to produce glare that may hinder any approaching attackers. Although sensitive sites should generally be inconspicuous and vaguely labeled, "keep out" signs may help protect nonpublic areas.

8.3.4 COMMUNICATION SECURITY

8.3.4.1 GENERAL

Communications is one of the most essential components of a dependable security system. As such, the equipment shall receive special attention from

the Reliability and Maintainability disciplines. Where practical, there shall be redundant transmission systems with automatic switchover capabilities for critical equipment.

In a transit agency, communication system assets include all of the stationary and mobile elements, including control centers, transmission towers and signal repeaters, in-station systems, on-vehicle systems, and handheld personal devices.

In light of the potential for a system attack or other destructive event, agencies should consider their level of reliance on communications systems and agency resilience to attack. Agencies should also consider how well they can communicate accurate, timely information when reacting to an emergency event:

- Within an agency to allocate resources and prioritize responses
- With other emergency services to coordinate a response
- With the traveling public to keep them aware of service interruptions and changes in service

Emergencies provide a significant challenge to current telecommunications systems, particularly since technology may be compromised at the very moment that the demand for information is greatest. In addition, most transit agencies do not have the ability to directly communicate with other emergency responders.

MDT should consider how to improve methods of communicating during emergencies, both internally and with emergency responders. Transit agencies should also be aware of what other area public safety agencies are doing, or planning to do, to achieve interoperability among their respective

communications systems. They may also consider being part of a state or metropolitan area initiative with those area agencies.

8.3.4.2 STATION COMMUNICATION

- A. The Station Attendant shall have immediate communication with The Central Control Facility by emergency telephone in the Station Attendant's booth. Also see Volume VII Section 7.05.12. MDT should consider including emergency communications systems, including blue-light phones and public address systems, in the plan, to allow rapid communications between remote areas of the station.
- B. Communications equipment accessible to the public shall be vandal resistant in design and material.
- C. Patrons shall have direct communication with the Station Attendant by means of two-way voice communications devices which shall be located at various strategic locations in the station.

Patron's request for assistance shall be by Passenger Assistance telephones strategically located throughout the public spaces of the station. All emergency phones shall be connected to appropriate facilities at the Central Control Facility which shall have dedicated telephone line communication with the dispatch facilities of all emergency assistance units serving the transit system.

Transportation Systems (ITS) technology now makes it possible to provide service updates in real time; transit agencies can use these technologies to disseminate information during an emergency:

- i. Public address (PA) systems (in-station and in-vehicle)

- ii. Variable message sign (VMS) systems (in-station and in-vehicle)
 - iii. Emergency intercoms for passenger use (in-station and in-vehicle)
 - iv. Service area-wide broadcast methods (transit agency Web site, local media outlets)
- D. Provisions shall be made in the Station Attendant's booth for a public address system, through which the Attendant may address the concourse level and the platform level.
- E. Law Enforcement
Arrangements shall be made for law enforcement officers assigned to the transit system to communicate with transit system security officers.

More information is provided in Volume VII, Section 7.05.

8.3.4.3 INTRUSION ALARMS

Silent intrusion alarms shall be monitored by the Station Attendant at their booth and at the Central Control Facility as part of the Access Control and Intrusion Detection (ACID) System. There shall be installed within the Station Attendant's booth a Panel in the form of a small mimic board for that station covering the areas monitored by intrusion devices. The panel shall indicate the detector locations by illuminating when alarmed. The visual signal shall be accompanied by a sonic alert until acknowledged by the Attendant. Alarms shall be programmable to be silent or non-silent. The mimic board shall be positioned in the Station Attendant's booth for their ease of viewing, but also to be viewed from outside the booth by emergency assistance personnel during nonoperating hours. Summary signals by security controlled areas shall be transmitted from each station to the Central Control

Facility. During operating hours, the Central Control Facility monitor will be notified when the Station Attendant acknowledges the intrusion alarm. During nonoperating hours, the Central Control Facility will have the capability to identify the area of the station to which emergency assistance agency personnel should be dispatched. An Access Control & Intrusion Detection (ACID) System is a combination of integrated electronic components, including sensors, control units, transmission lines, and monitoring units, that detect one or more types of intrusion into an area protected by the ACID. An ACID includes both interior and exterior systems, and also includes electronic entry control devices and may interface with the CCTV for alarm assessment.

ACID can be useful throughout transit system operations, allowing security personnel to monitor the movements of authorized people in restricted-access areas and to alert security personnel of potential breaches by unauthorized persons. At perimeters an ACID provides improved security-response time. Pairing intrusion-detection systems with remote surveillance technology enables event-triggered surveillance. There are numerous types of interior and exterior sensors that agencies can deploy to signal security personnel when an intruder crosses a threshold, opens a door, or breaks a window. These include area sensors, barrier sensors, point sensors, and volumetric sensors. Intrusion sensors may be buried in the ground or mounted to a fence, wall, ceiling, floor, door, or window. Sensing technologies include magnetic or mechanical switches, pressure sensors, infrared sensors, acoustic sensors, and video cameras.

8.3.4.4 MONITORING

The Central Control Facility shall house all central monitoring of security devices and communications, including provisions for a special Security Console with electronic recording and play back facilities.

This and other communication monitoring points shall be so positioned, or provided with acoustics, to reduce transmission of cross conversations.

8.3.4.5 ELECTRONIC SURVEILLANCE (CCTV)

- A. The system shall employ electronic surveillance of station platforms, concourse areas and vulnerable areas not under the unobstructed view of the Station Attendant. Surveillance needs shall be based upon station characteristics and location.
- B. All electronic surveillance cameras shall be protected to prevent vandalism and shall be mounted to afford optimum visibility and minimum access to vandals. The cameras shall be equipped with appropriate adjustment capabilities and/or equipment to be effective. CCTV surveillance systems may include fixed cameras and pan/tilt/zoom cameras that security personnel can remotely control, and often include video-recording systems.
- C. Human factors engineering shall dictate the maximum number and location of electronic surveillance monitors in each Station Attendant's booth.
- D. Electronic surveillance recorders shall be provided in stations. The recorder shall be designed to be programmable to record from any electronic surveillance camera or sequence of cameras. Duration of video storage shall be determined by MDT. Recording system shall be compatible with the existing MDT system.
- E. Electronic surveillance shall be utilized in the Administration Facility to

provide optimum protection to critical areas and to reduce security manpower requirements.

- F. Electronic surveillance shall be utilized to monitor the access to, as well as the interior of, the Fare Sorter/Counter area.
- G. Electronic surveillance shall be provided for security sensitive areas of the Maintenance Facilities not within unobstructed view or range of the Yard Control Tower Attendant. The security electronic surveillance monitors should be installed together, along with those which are used for operational purposes.

8.3.5 PASSENGER VEHICLES

Refer to Volume VII Section 5.9.2 for Security Strategies for Vehicle Design.

8.3.6 ADMINISTRATION FACILITY

A. Access Control

There shall be only one main ingress/egress point in the facility. Other means of entering or exiting the facility shall be minimized in accordance with local building code requirements. These other means shall present a formidable barrier from the outside with panic type hardware on the inside, sonic deterrents and means for detecting intruders. The following sub-sections present an overview of access management at administrative buildings and CCFs for perimeter security, vehicle access, and human access.

B. Perimeter Security

The CCF and other administrative buildings are not typically open to the public, so stringent perimeter security can be implemented without

compromising the facilities' intended uses. When planning access to the facilities, designers need to accommodate employees, job applicants, deliveries, visitors seeking tours, public officials, and contractors or others doing business with the transit agency. Agencies should consider consolidating entrances to the site to a minimal number of access points and monitoring them for access control, in addition to developing a means for screening visitors in vehicles, pedestrians, or bicyclists.

C. Vehicle Access

Within the site perimeter, designers should consider traffic circulation and parking areas that minimize the opportunity for vehicles to drive close to site structures, to crash into a structure at a high speed, or to enter a structure through one of its entrances.

D. Human Access

Within the facility, access management techniques can be used to differentiate between employees and visitors and to enforce different levels of security clearance for different types of employees. For example, employees who are not responsible for operations control may not be allowed access to those systems or to the areas of the building where the systems are located. Locks, card-key access, biometrics, and pass code protection can all help enforce appropriate access among employees, as well as make it more difficult for outsiders to break in.

In addition, surveillance and intrusion-detection techniques can be used for early discovery of an intruder. The interior building design can minimize hidden spaces such as niches, blind corners, or isolated passageways in order to facilitate surveillance. Wherever possible, designers should consider clear fields of vision so that all areas of the

building are in plain view of security personnel and other employees. Cameras can help expand the surveillance area of live personnel, while intrusion alarms such as motion detectors and alarmed doors can help alert personnel to points of intrusion.

E. The Central Control Facility

The Central Control Facility is among the most critical areas within the transit system. As such, it shall have the most stringent security controls. There shall be a minimum number of ingress/egress points allowable under applicable fire ordinances and no exterior building windows. Access to the facility shall be strictly controlled.

8.3.7 MAINTENANCE FACILITIES SECURITY

A. Lighting

- Lighting of the Maintenance Facilities shall be consistent with other operating and security requirements, in accordance with lighting requirements as per Volume II Section 4.07.
- Where perimeter lighting is required, the lighting units for a perimeter fence should be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area both inside and outside the fence.
- Perimeter lighting should be continuous and on both sides of the perimeter fence and should be sufficient to support CCTV and other surveillance equipment where required.
- The cone of illumination from lighting units should be directed downward and outward from the structure or area being protected. Cones of illumination should overlap to provide coverage in the event of bulb burnout.
- The lighting should be arranged so as to create minimal shadows

and minimal glare in the eyes of security guards.

B. Enclosure

The Maintenance Facilities should be enclosed by a nonscalable barrier of sufficient height to deter intruders. There should be a suitable clear zone on each side of the barrier to avoid offering protection or concealment to vandals or intruders.

C. Access

There shall be a single ingress/egress point for normal surface traffic which shall be a suitably monitored security gate. Other ingress/egress points necessary for operations shall be appropriately secured.

8.3.8 LANDSCAPING

Landscaping of the parking facilities shall conform to security requirements by the use of vegetation which will not afford protection to miscreants nor interfere with electronic or visual surveillance of the site. Natural elements, such as rolling hills and steep terrain, can provide hiding places for aggressors and hinder visual surveillance by security personnel. High points on the site elevate buildings where they are easily visible from off-site and therefore vulnerable to weapons fire from unsecured areas. Agencies should consider avoiding topography and vegetation that prevents clear lines of sight from the site to avoid making it easy for potential attackers to approach the site without notice.

Dense trees and shrubbery present similar challenges. Portions of sites (especially larger sites) are often left in their natural state, which can include steep terrain and dense vegetation. This occurs for a variety of reasons including unsuitable terrain, zoning or environmental regulations, and land

banking for future use. Where these situations exist, agencies should consider perimeter protection to separate those areas from the developed portion of the site, to prevent them from being used for a covert approach to valuable assets.

8.3.9 FARE COLLECTION

Fare collection equipment shall be constructed of material which will frustrate attempts to penetrate the equipment. Provisions shall be made to strictly control access to the mechanical and electric components and the funds contained therein. There shall be a means of detecting unauthorized entry.

The design of fare gates and access to them shall include provisions which will tend to frustrate fare evaders without creating emergency exit hazards.

Access to the fare sorting/counting area shall be among the most tightly controlled, separate from and independent of any other access control of the facility in which it is housed.

8.3.10 TRACKWORK

Wayside facilities shall be protected by tamper resistant covers on switch machines and controls and vandal resistant track electrical connections. Diligent remote surveillance and tamper detection are the best protection against the intentional destruction of tracks and switches. Derailments can be caused by explosives and by tampering with the installation of track rails and switches, such as loosening the track connectors (spikes and clips) along a continuous length of track. The first train over the damaged or altered track may not be derailed, but as subsequent trains pass by, the misalignment of the rail worsens. The rails in switches have similar vulnerabilities; switches are also vulnerable through their mechanical components and the integrated

signaling hardware.

Advanced telemetry systems can be used that remotely monitor the conditions of track and the operations and setting of switches, and report this information to an operations center. These systems can be programmed to alert transit staff if tampering or incorrect settings are detected. Frequent human inspection of track, switches and associated equipment is an alternative.

8.3.11 FIRE AND ACCESS CONTROL AND INTRUSION DETECTION MANAGEMENT

A. Intrusion Detectors

Portal type intrusion detectors shall be the seated plunger type installed in the door jamb or rotary switch type incorporated into the door hinge. Intrusion detectors on equipment cabinets shall be the plunger type.

An Access Control and Intrusion Detection (ACID) System is a combination of integrated electronic components, including sensors, control units, transmission lines, and monitoring units, that detect one or more types of intrusion into an area protected by the ACID. An ACID includes both interior and exterior systems, and may also include electronic entry control devices and an interface to the CCTV for alarm assessment.

ACIDS can be useful throughout transit system operations, allowing security personnel to monitor the movements of authorized people in restricted-access areas and to alert security personnel of potential breaches by unauthorized persons. At perimeters ACIDS provide improved security-response time. Pairing intrusion-detection systems

with remote surveillance technology enables event-triggered surveillance.

There are numerous types of interior and exterior sensors that agencies can deploy to signal security personnel when an intruder crosses a threshold, opens a door, or breaks a window. These include area sensors, barrier sensors, point sensors, and volumetric sensors. Intrusion sensors may be buried in the ground or mounted to a fence, wall, ceiling, floor, door, or window. Sensing technologies include magnetic or mechanical switches, pressure sensors, infrared sensors, acoustic sensors, and video cameras.

B. Intrusion Alarms

All intrusion alarms shall be monitored by the Station Attendant and at the Central Control Facility, to include any alarms programmed to be silent or nonsilent.

8.3.12 STATION ATTENDANT'S BOOTH

Station security shall include a Station Attendant at each passenger station during operating hours. The Station Attendant shall normally be stationed in or near a booth specifically for that purpose.

The Station Attendant's booth shall be positioned to allow the Station Attendant maximum visibility to patrons in need of assistance and afford the Attendant a clear view of as much of the concourse level as possible. Provisions shall be made to secure the booth when the attendant is not present.

See Volume II Chapter 1 for additional information on the Station Attendant Booth.

– Intentionally Left Blank –

8.4 OTHER REFERENCE MATERIALS

The Designer shall consult the items listed below for additional information on Security issues.

- APTA, Manual for the Development of Rail Transit System Safety Program Plans
- APTA, Standard for Rail Transit System Emergency Management
- Department of Defense, MIL-STD-882 Systems Safety Standard Practice
- Department of Homeland Security Publications
- Department of Transportation, 49 CFR 659 Rail Fixed Guideway System State Oversight
- Department of Transportation, Circular 5800.1 Safety and Security Management
- Department of Transportation, Compliance Guidelines for States with New Start Projects
- Department of Transportation, Critical Incident Management Guidelines
- Department of Transportation, Handbook for Transit Safety and Security Certification
- Department of Transportation, The Public Transportation System Security and Emergency Preparedness Planning Guide
- Department of Transportation, Transit Security Design Considerations
- Department of Transportation, Transit Security Handbook
- Department of Transportation, Transit Security in the 90's
- Department of Transportation, Transit Security Procedures Guide
- Department of Transportation, Transit System Security Planning Seminar

- Department of Transportation, Transit System Security Program Planning Guide
- Florida Fire Protection Code
- Guidelines for Major Capital Projects
- Illumination Engineers Society (IES) Publications
- Institute of Electrical and Electronic Engineers (IEEE) Publications
- Insulated Cable Engineers Association (ICEA) Publications
- Metropolitan Dade County Fire Prevention and Safety Code
- Miami Dade Transit, Safety and Security Certification Plan
- National Electric Manufacturers Association (NEMA) Publications
- National Electric Safety Code (NESC) Publications
- NFPA 10, Portable Fire Extinguishers
- NFPA 101, Life Safety Code
- NFPA 13, Installation of Sprinkler Systems
- NFPA 130, Standard for Fixed Guideway Transit and Passenger Rail Systems
- NFPA 14, Installation of Standpipe, Private Hydrant and Hose Systems
- NFPA 2001, Clean Agent Extinguishing Systems
- NFPA 70, National Electrical Code
- NFPA 72, National Fire Alarm Code
- Occupational Health and Safety Act (OSHA) Regulations
- Ordinances of the City of Miami, Miami Dade County, and other Authorities Having Jurisdiction
- Transit Research Board, Deterrence, Protection and Preparation
- Transit Research Board, Emergency Preparedness for Transit Terrorism
- Transportation Security Administration Publications

APPENDIX A: ACRONYMS

ACID	Access Control and Intrusion Detection
ADA	Americans with Disabilities Act
ANSI	American National Standards Institute
APTA	American Public Transportation Association
CBNR	Chemical, Biological, Nuclear, Radiological
CCF	Central Control Facility
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control
CDPD	Cellular Digital Packet Data
CFR	Code of Federal Regulations
CPTED	Crime Prevention Through Environmental Design
DCS	Distributed Control Systems
DHHS	Department of Health and Human Services
DOD	Department of Defense
EMI	Electro-Magnetic Interference
FMP	Fire Management Panel
FTA	Federal Transit Administration
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identification
IDS	Intrusion Detection System
MDT	Mobile Data Terminals
NFPA	National Fire Protection Agency
TVA	Threat and Vulnerability Assessment
UHF	Ultra High Frequency
VHF	Very High Frequency
VMS	Variable Message Sign

– Intentionally Left Blank –

APPENDIX B: DEFINITIONS

Acceptance Tests (Subsystems): Procedures designed to evaluate correct performance of that subsystem's components in a static environment. These tests are usually performed prior to complete system integrated testing.

Baseline Documents: Drawings, specifications, standards, design criteria, definitions, and program plans which define the project form, fit and functional requirements, as well as any other contract and management document designated as subject to documentation controls.

Configuration Management: Formal process instituted to control the documentation of the design, evaluation, acceptance, operation and maintenance of a project.

Configuration Management Log Sheet: Record of all activities pertaining to deviation requests for baseline documents.

Contractor: A private sector enterprise engaged to provide services or products within agreed limits specified by a procuring activity.

Corrective action: A documented design, process, procedure or materials change implemented and validated to correct the cause of failure or design deficiency.

Criticality: A relative measure of the consequences of a failure mode or hazard and its frequency of occurrences.

Design Review Package: The project design documents issued for review at a specified design stage.

Detection Mechanism: The means or methods by which a failure can be discovered by an operator under normal system operation or can be discovered by the maintenance crew by some diagnostic action.

Deviation Request: Request to deviate from the established design, procedural baseline, final schedule or other baseline items.

Emergency: A situation which is life threatening to passengers, employees or other interested citizens or which causes damage to any transit vehicle or facility or results in the significant theft of services and reduces the ability of the system to fulfill its mission.

Environment: The conditions, circumstances, influences, stresses and combinations thereof, surrounding and affecting systems or equipment during storage, handling, transportation, testing, installation and use in operation.

Failure: An inability to perform an intended function within prescribed limits.

Failure mode and effects analysis (FMEA): A procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity.

Fault Tree Analysis: A deductive analysis procedure which graphically presents undesired events to determine possible causes of that event.

Final Design Package: The series of documents and documentation that represent and support the final design review and completion and which become part of the bid package.

Hazard: Any real or potential condition that can cause injury, death, or damage to or loss of equipment or property.

Hazard Analysis: Any analysis performed to identify hazardous conditions for the purpose of their elimination or control. Hazard analysis is done to identify safety problems and possible solutions and present options to decision makers.

Hazard Cause: A condition that contributes to a hazard. It could be unsafe design, environmental factors, failure, human error, etc.

Hazard Controls: Measures that eliminate a hazard or reduce the severity or probability of its potential effect.

Hazard Probability: The probability that a hazard will occur during the planned life expectancy of a system. Hazard probability may be expressed in quantitative or qualitative terms.

Hazard Severity: An assessment of the worst credible mishap that could be caused by a specific hazard.

Hazard Resolution: The analysis and subsequent action taken to reduce, to the lowest level practical, the risk associated with an identified hazard.

Integration Test: A test performed to demonstrate that a system or systems function satisfactorily when connected to interfacing systems.

Interface: The junction points within or between systems or subsystems where matching or accommodation must be properly achieved in order to make their operation compatible with the successful operation of all other functional entities.

Malfunction: Any anomaly or failure wherein the system, subsystem or component fails to function as intended.

Operating Hazard Analysis (OHA): Identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering: operation, test, maintenance, repair, transportation, handling, equipment or removal of the system.

Preliminary Hazard Analysis (PHA): An inductive analysis performed to obtain an initial risk assessment of a concept or system.

Redundancy: The existence in a system of more than one means of accomplishing a given function.

Reliability: The chance that an item can perform its required function for a specified time under specified conditions.

Resolution: Changes that are made in the system or subsystem design, procedures or activities which eliminate or control the identified hazard to an acceptable level.

Revenue Service: The transportation of fare-paying passengers.

Risk: An expression of possible loss over a specific period of time or number of operational cycles. It may be indicated in terms of hazard severity and probability.

Risk (residual): The risk remaining after hazard controls have been applied.

Safety Certification: The process of verifying that safety-related requirements are incorporated into a transit system, thereby demonstrating that it is operationally ready for revenue service and safe for passengers, employees, emergency responders and the general public.

Safety Design Criteria: An organized listing of safety codes, regulations, rules, design procedures, standards, recommended practices, handbooks and manuals prepared to provide guidance to project designers in the development of technical specifications that meet minimum safety parameters.

Safety Requirements: The specification of safety design criteria into the technical documents and drawings that comprise the detailed designs, procedures, plans and processes required to deliver the project.

Security: Freedom from intentional danger.

Security Breach: An unforeseen event or occurrence which endangers life or property and may result in the loss of services or system equipment.

Security Incident: An unforeseen event or occurrence which does not necessarily result in death, injury or significant property damage but may result in minor loss of revenue.

Security Threat: Any source that may result in a security breach, such as vandal or disgruntled employee; or an activity, such as an assault, intrusion, fire, etc.

Severity: The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage or system damage that could ultimately occur.

Single failure point: The failure of an item which would result in failure of the system and is not compensated for by redundancy or alternative operational procedure.

Subsystem: An element of a system that in itself may constitute a system.

System: A composite of people (employees, passengers, others), property (facilities and equipment), environment (physical, social, institutional) and procedures (standard operating, emergency operating, and training) which are integrated to perform a specific operational function in a specific environment.

System Safety: The application of engineering and management principles, criteria and techniques to optimize safety within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle.

System Safety Engineering: An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria and techniques to identify and eliminate hazards or reduce the risk associated with hazards.

System Safety Management: An element of management that defines the system safety program requirements and ensures the planning, implementation and accomplishment of system safety tasks and activities consistent with the overall program requirements.

System Safety Program: The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of the system life cycle.

System Safety Program Plan: A description of the planned methods to be used by the contractor to implement the tailored requirements of this standard, including organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort and integration with other program engineering and management activities and related systems.

System Security: The application of operating, technical and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources

System Security Management: An element of management that defines the system security requirements and ensures the planning, implementation and accomplishments of system security tasks and activities.

System Security Program: The combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of a system life cycle.

Threat: Any real or potential condition that can cause injury or death to passengers or employees or damage to or loss of transit equipment, property and/or facilities.

Threat Analysis: A systematic analysis of a system operation performed to identify threats and make recommendations for their elimination or mitigation during all revenue and nonrevenue operation.

Threat Probability: The probability a threat will occur during the plan's life. Threat probability may be expressed in quantitative or qualitative terms. An example of a threat-probability ranking system is as follows: (a) frequent, (b) probable, (c) occasional, (d) remote, (e) improbable and (f) impossible.

Threat Resolution: The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.

Threat Severity: A qualitative measure of the worst possible consequences of a specific threat:

Unsafe Condition or Act: Any condition or act which endangers life or property.

Vulnerability: Characteristics of passengers, employees, vehicles and/or facilities which increase the probability of a security breach.

Verification: Documented conformance, demonstrated through testing, inspection or other means that the designed or delivered project, system, subsystem or item ensuring the accuracy or correctness in comparison with a safety requirement.

APPENDIX C: SAMPLE THREAT AND VULNERABILITY ANALYSIS REPORT

– Intentionally Left Blank –



APPENDIX C: THREAT AND VULNERABILITY ANALYSIS REPORT

**PROGRAM MANAGEMENT CONSULTING
FOR THE PEOPLE'S TRANSPORTATION PLAN
PROJECT NO. E03-MDT-01**

NORTH CORRIDOR EXTENSION PROJECT

Submittal Date
November 14, 2006

DRAFT REVISION #1

Prepared by:
DMJM Harris
800 Douglas Road Suite 770
Coral Gables, Fl 33134

– Intentionally Left Blank –

TABLE OF CONTENTS

SECTION 1.0: NORTH CORRIDOR EXTENSION PROJECT DESCRIPTION	127
1.1 Overview	127
SECTION 2.0: THREAT AND VULNERABILITY ANALYSIS PROCESS.....	129
2.1 INTRODUCTION	129
2.2 PURPOSE	129
2.3 OBJECTIVES.....	129
2.4 SCOPE	130
2.5 APPROACH.....	130
2.6 Define the System.....	131
2.7 Identify System Critical Assets.....	131
2.8 Identification of Threats and Vulnerabilities	132
2.9 Countermeasures	133
2.10 CPTED.....	134
2.11 Access Management	134
2.12 Surveillance	134
2.13 Intrusion Detection	134
2.14 Emergency Response Features.....	135
SECTION 3.0: THREAT AND VULNERABILITY CATEGORIZATION.....	136
3.1 Resolution of Threats and Vulnerabilities.....	138
SECTION 4.0: TRANSIT STATIONS	141
4.1 Potential Threats.....	141
4.1.1 Arson	141
4.1.2 Explosives.....	141
4.1.3 Weapons of Mass Destruction (WMD).....	141

TRANSIT

4.1.4	Hostage or Violent Event	142
4.2	Perimeter Security	142
4.3	Human Access.....	142
4.4	Emergency Response and Egress.....	142
4.5	Systems and Services	142
SECTION 5.0: ADMINISTRATIVE BUILDINGS AND CENTRAL CONTROL FACILITY		
.....		145
5.1	Potential Threats.....	145
5.1.1	Explosives.....	145
5.1.2	Arson	145
5.1.3	Tampering.....	145
5.1.4	Hostage Situation or Violent Incident.....	145
5.1.5	Weapons of Mass Destruction	146
SECTION 6.0: ELEVATED STRUCTURES		147
6.1	Potential Threats.....	147
6.1.1	Explosives/Fire	147
6.1.2	Ramming	147
SECTION 7.0: RIGHT-OF-WAY, TRACK, AND SIGNALS		149
7.1	Potential Threats.....	149
7.1.1	Explosives	149
	Tampering/Disabling.....	149
7.1.3	Cyber Attacks	149
SECTION 8.0: REMOTE EQUIPMENT AND UNMANNED STRUCTURES		151
8.1	Potential Threats.....	151
8.1.1	Explosion/Fire	151

TRANSIT

8.1.2	Collision	151
8.1.3	Tampering.....	151
SECTION 9.0: COMMUNICATIONS.....		153
9.1	Threats to Transit Communications	153
9.1.1	Physical Damage to Agency Equipment.....	153
9.1.2	Loss of Power	154
9.1.3	Cyber Attacks	154
9.2	Protection Strategies.....	154
9.2.1	Hardening and Access Management.....	155
9.2.2	Redundancy.....	155
9.2.3	Backup Power Supply.....	157
9.2.4	Prioritization Service and Dedicated Landlines.....	157

– Intentionally Left Blank –

FOREWORD

Miami-Dade Transit (MDT) recognizes that public transit is a frequent target of terrorist activities nationwide as well as worldwide. Design and construction of the MDT North Corridor Extension Project will incorporate a security strategy to deter and minimize the effects of attacks against their facilities, riders, employees and the general public.

This document is a resource intended to aid MDT decision makers, members of the design team, construction and operations departments, security and law enforcement personnel, and consultants and contractors in developing a security strategy following the completion of a threat and vulnerability assessment and development a comprehensive plan that's affordable and effective. In developing a security strategy, MDT must first determine which of its security issues are most critical, and then develop a timeline for addressing them. The ultimate goal of the strategy is to move closer to achieving an integrated security system. MDT can implement their strategy incrementally, and make discrete decisions as to which counter measures are most appropriate.

DMJM Harris performed this Threat and Vulnerability Analysis (TVA) for the Peoples Transportation Plan, Miami-Dade Transit (MDT) Authority North Corridor Extension Project. For each of the threat/vulnerabilities listed in this report, possible controlling measures are identified that will reduce these threats/vulnerabilities to an acceptable level of risk.

MDT will need to determine which of these possible controlling measures will actually be implemented and whether the implemented measures will result in the desired risk reduction. It is MDT's responsibility to implement mitigating and corrective actions such as resolving non-conformances to the design documents and specifications, developing a comprehensive inspection and maintenance program, training employees, and implementing safety-related operating procedures.

– Intentionally Left Blank –

SECTION 1.0: NORTH CORRIDOR EXTENSION PROJECT DESCRIPTION

1.1 Overview

The MDT North Corridor Extension Project is the first major transit project to be undertaken in Miami-Dade County under the area's new People's Transportation Plan (PTP). The project consists of extending the existing Metrorail (elevated, heavy rail) line by constructing approximately 9.5 miles of new guideway that will operate along the N.W. 27th Avenue corridor from approximately the existing Martin Luther King Metrorail Station to the Miami-Dade/Broward County line. MDT has previously stated that the North Corridor Extension will operate at 4.5 minute peak headways and 7 minute off-peak headways. However, these headways may change as MDT currently reviews the planned operations.

Seven stations are planned along the corridor. Proposed station locations include N.W. 82nd Street, N.W. 119th Street (Miami-Dade College), Ali-Baba (City of Opa-Locka), N.W. 163rd Street, N.W. 183rd Street, N.W. 199th Street (Dolphins Stadium), and N.W. 215th Street (Calder Race Course). The key trip generators to service are at Miami-Dade College North Campus, Dolphins Stadium, Northside Shopping Center, and the Florida Turnpike. All stations will have surface parking areas. The project scope currently includes an additional 16 vehicles to be procured for the project.

Revenue service is now scheduled for December 2012. Preliminary estimates indicate that the project would represent an increase of 18,000 additional Metrorail daily boardings in the year 2015, representing 11,250 new transit riders.

– Intentionally Left Blank –

SECTION 2.0: THREAT AND VULNERABILITY ANALYSIS PROCESS

2.1 INTRODUCTION

All transit agencies are faced with the dilemma of maintaining open systems versus making them more secure. Transit agencies must operate systems in which public access not only is crucial to their daily operations; it also fulfills the agency's mission. The complexity of the transit environment dictates the importance of using a system approach to integrate the diverse functions, technologies, and operating relationships.

Transit security is defined as freedom from intentional danger for passengers, employees and the system. The MDT Safety and Security Management Plan (SSMP) is designed to eliminate and/or control identified threat and vulnerability issues to the lowest practical level. Perceived security is as important to a transit agency as actual security performance. Patron fear reduces ridership and heightens passenger anxiety. Security is communicated to patrons not only by the actual security performance of the system, but also by the perceptions patrons form about the system. A security program must address both perceived and actual security problems if it is to reassure patrons, maintain or increase ridership, and earn public trust.

This Threat and Vulnerability Analysis presents a detailed assessment of potential security issues that may be associated with the North Corridor Extension Project. It is based on the preferred alignment and preferred conceptual design alternatives. The analysis is provided as part of the North Corridor Extension Project preliminary engineering stage, in order to identify security issues and eliminate them through design, mitigates them by control measures, or determines them to be acceptable as-is. It is envisioned that this document will be expanded and finalized during subsequent phases of the project.

2.2 PURPOSE

A Threat and Vulnerability Analysis is a comprehensive study of a system to identify threats and vulnerabilities and to make recommendations for their elimination or control during all life cycle phases. Combating security issues facing transit agencies today involves integrating changes to administrative policies, new technologies and physical protection of structures and developing a formalized process to identify, eliminate and control threats and vulnerabilities. The goal is to clarify and systematically assess conditions that make the system vulnerable to acts of violence.

A threat and vulnerability resolution process outlines how actual and potential threats will be identified, evaluated and resolved. Proper threat identification, categorization, and data collection are crucial to this process.

2.3 OBJECTIVES

Threat and Vulnerability Analysis objectives are to:

- Identify potential threats and vulnerabilities on the system elements
- Assess potential threats and vulnerabilities on system elements

- Perform threat and vulnerability precedence
- Identify measures that will prevent security incidents by eliminating or controlling the underlying threats and vulnerabilities
- Resolve and document threat and vulnerability resolutions

2.4 SCOPE

The analysis presented in this document is meant to assist MDT staff in identifying potential security issues associated with the North Corridor Extension Project, which is currently in the design stages. The Threat and Vulnerability Analysis is not intended to be a comprehensive list of all security issues potentially occurring on the North Corridor Extension Project. The analysis focuses primarily on hazards and vulnerabilities that may result in fatal or severe injury, or catastrophic or substantial loss or damage to the operating system. The Federal Transit Administration document “Transit System Security Planning Seminar”, was used as a guide to prepare this report.

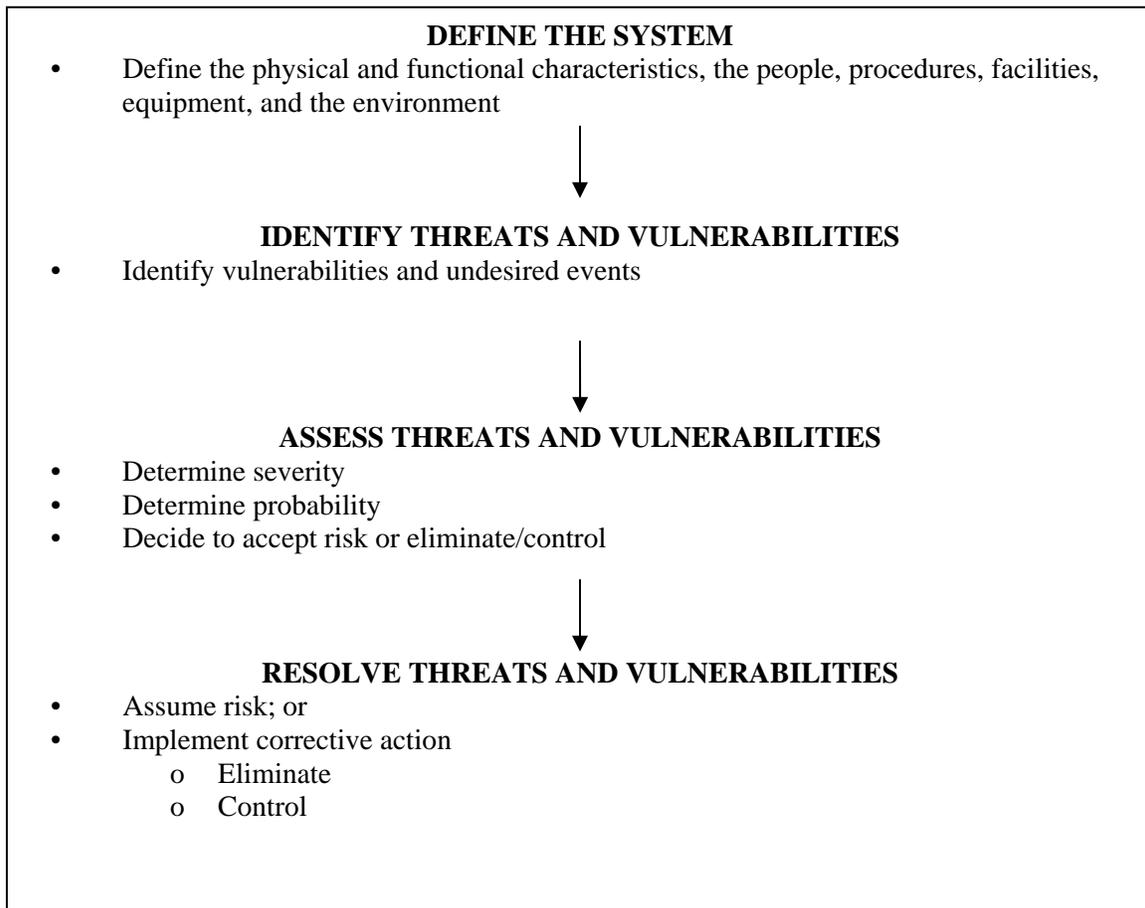
The North Corridor Extension project is defined by its systems, facilities, and rolling stock, and the environment in which they operate. The threats and vulnerabilities identified and recommended corrective actions relate to the equipment, environment, procedures, and public interfaces in the North Corridor Extension. A number of threats and vulnerabilities identified are generic in nature and are applicable to most light rail projects. Hazards and vulnerabilities that are specifically unique to the North Corridor Project are also identified.

2.5 APPROACH

System Security is the application of special technical, engineering, and managerial skills to the systematic, forward-looking identification and control of threats and vulnerabilities. The System Security concept calls for security analyses and threat and vulnerability control actions.

Threat and Vulnerability Analysis is an essential function in design, from the concept phase through development. The System Security approach focuses on the prevention of security incidents by eliminating and/or controlling threats and vulnerabilities in a systematic manner. The goal is to reduce the identified threats and vulnerabilities to the lowest practical level through the most effective use of resources. This process helps assure that threats and vulnerabilities are identified and translated into risks, which are then analyzed, assessed, prioritized, and resolved, accepted or tracked to closure. The primary goal is incident prevention through an informed decision-making process. The Threat and Vulnerability Identification and Resolution Process is shown in Figure 1.

Figure 1 – Threat and Vulnerability Identification and Resolution Process



2.6 Define the System

The initial step in the Threat and Vulnerability Analysis process is to define the physical and functional characteristics of the system to be analyzed. These characteristics are presented in terms of the major elements that make up the system. An understanding of how the individual system elements interface with each other is essential to the threat and vulnerability identification effort. The North Corridor Extension Project's systems have been identified through the design criteria, conceptual and preliminary engineering design specifications and drawings, and other project documents.

2.7 Identify System Critical Assets

North Corridor Extension Project System Assets include:

- People
- Right-of-Way
- Administrative Facilities
- Construction Sites
- Stations, Stops, Terminals and Intermodal Facilities
- Systems and Data

TRANSIT

- Vehicles
- Utilities
- Bridges

Each asset has its own level of risk, attractiveness as a target, vulnerabilities, accessibility and criticality to the system. The diversity of assets leads to a range of possible threats and countermeasures. Results of attacks or incidents might include:

- Loss of life or physical injury to transit riders, staff, and/or passer-by
- Physical damage to transit agency equipment or infrastructure, and possibly to the surrounding environment
- Loss of power through direct attack or external event
- Failure outside the transit agency that affect operations, service delivery or maintenance
- Excessive traffic on communications networks
- Breach of communications or operations network security/hacking

This Threat and Vulnerability Analysis will aid MDT management with prioritizing risks through threat and vulnerability assessments and select sets of countermeasures that provide the best overall risk reduction for the system as a whole.

2.8 Identification of Threats and Vulnerabilities

After defining the system and establishing a critical assets list, the second step in the Threat and Vulnerability Analysis process involves identifying hazards threats and vulnerabilities associated with operating the North Corridor Extension. These security issues include (listed in alphabetical order):

- All acts of Terrorism
- Arson
- Bomb Threats
- Burglary
- Drunk Driving
- Drunkenness
- Gambling
- Homicide
- Kidnapping
- Liquor Law Violations
- Loud Music
- Motor Vehicle Theft
- Narcotics
- Other Sexual Offences (indecent exposure, etc...)
- Public Expectoration/Urination
- Rape (forcible and attempted)
- Robbery (weapon and strong arm)
- Rowdy Behavior
- Smoking, Eating, Drinking on the System

TRANSIT

- Theft (pickpocket, purse-snatch, automobile burglary, automobile accessories, bicycle, computer fraud, vending machine fraud)
- Trespassing
- Vagrancy
- Vandalism
- Weapon Law Violations

Social costs of transit crime include:

- Personal harm to victims
- Poor perception of security
- Reduced quality of life on system

Financial costs of transit crime include:

- a. Increased financial burden of operating system
 - Law enforcement
 - Liability/compensation to victims
 - Repairs
 - Schedule disruptions
 - Security equipment
- b. Reduction of revenues collected
 - Fare evasion
 - Internal theft
 - Lost ridership

2.9 Countermeasures

It is difficult to prepare for terrorist attacks or other emergencies that might require a coordinated response because such incidents are largely unpredictable. The problems experienced in one emergency may be different during the next. With each new event, agency personnel may be confronted with a shifting set of problems to handle. However, lessons from prior events suggest the following types of strategies help protect a transit system from the effects of a terrorist attack:

- Hardening against a physical attack
- Redundancy, with both duplication and variety
- Backup power supplies
- Prioritization service and dedicated lines
- Network and cyber security

The principal strategies to counter terrorist attacks can be grouped into efforts to:

- Deter attackers from attempting an attack;
- Detect potential threats promptly

- Minimize the impact from an attack
- Respond and recover (or resume critical operations as quickly as possible)

Applying these concepts to the physical design of infrastructure leads to several general strategies that are applicable to transit assets. No single security strategy is appropriate for every agency. MDT should consider its operations, infrastructure and communications needs, threat assessments, budget, and existing systems to determine which combinations of countermeasures best fit its circumstances.

2.10 CPTED

The concept of Crime Prevention through Environmental Design (CPTED) has evolved as a means to reduce the opportunities for crimes to occur. This is accomplished by employing physical design features that discourage crime, while at the same time encouraging legitimate use of the environment. CPTED design considerations, which have been employed in recent years by transit agencies in the design of safer public facilities, such as transit stations and bus stops, are transferable to endeavors to secure and harden elements of an agency's infrastructure from terrorist attacks. Major elements of the CPTED concept are defensible space, territoriality, surveillance, lighting, landscaping, and physical security planning.

2.11 Access Management

Controlling who (or what) may access restricted areas and assets in the system plays an important role in protecting transit infrastructure. A core principle of access management is that valuable assets are protected behind multiple "layers" of secure spaces, with security measures becoming more stringent for deeper layers. Access control may focus on discerning between employees and visitors, on maintaining locks, on screening for weapons, or on barring unauthorized vehicle entry to a transit property. Access management techniques may include procedures and policies, physical barriers, identification and credentialing technology, security personnel, communications systems, surveillance, and intrusion-detection systems.

2.12 Surveillance

Surveillance can include closed-circuit televisions, security personnel, or vigilant vehicle operators or station clerks, who are often the first line in security measures. The presence of agency staff can deter an attack. The presence of surveillance equipment acts as a deterrent not only because an area is being watched remotely, but also because activities are recorded and intruders are aware of the possibility of detection and capture. Surveillance is also useful in warding off attacks against remote, unmanned infrastructure, such as communications towers and power substations. Transit agencies should consider what combination of equipment and personnel are needed to achieve optimal security coverage. Placement should be based on the volume of human and vehicular traffic, the layout of the watched or guarded asset, as well as the location of any blind spots resulting from overlapping or peripheral areas.

2.13 Intrusion Detection

Devices aimed at detecting unwanted or unauthorized persons or vehicles are helpful in protecting multiple forms of assets. Such devices may detect motion in an unmanned area or passage into a restricted area gained by tampering with a security device. Such methods are useful in access management for unmanned infrastructure as well as for administration or operations centers. These devices may sound an

alarm at the site of the intrusion and/or send a silent alarm to a desk in the operations center or security headquarters. When intrusion-detection devices are used in remote or unmanned areas, they should be carefully configured to account for the natural movement of items in the surrounding environment, such as animals or wind-blown objects.

2.14 Emergency Response Features

Lives may be saved in an emergency if physical systems are designed to facilitate rapid evacuation or to shelter people in place while enabling quick entry by responders. Site layout can incorporate exits that are easy for users to locate and access. Technical solutions can include planning independent energy sources for emergency lighting and communications systems, and installing detection alarm systems that promptly signal an emergency situation.

The third step in the TVA process is to categorize the identified hazards in terms of each vulnerability severity or consequence and the probability of occurrence. The United States Department of Defense document *Standard Practice for System Safety*, MIL-STD-882D, establishes system security criteria guidelines for determining threat and vulnerability severity and probability. The threat and vulnerability severity categories listed in Table 1 provide a qualitative indication of the relative severity of the possible consequences of the vulnerable conditions. For this TVA's purposes, the severity category assigned was based on the "worst-case" event. For example, if a trespasser is struck by a light rail vehicle in the LRT right-of-way the event could result in injury, but this is also very likely to result in a fatality. Therefore, "Death" is the severity category.

SECTION 3.0: THREAT AND VULNERABILITY CATEGORIZATION

The third step in the threat and vulnerability analysis process is to categorize the identified threats and vulnerabilities in terms of each threat and vulnerability severity or consequence and the probability of occurrence. The United States Department of Defense document *Standard Practice for System Safety and Security*, MIL-STD-882D, establishes system security criteria guidelines for determining threat and vulnerability severity and probability. The threat and vulnerability severity categories listed in Table 1 provide a qualitative indication of the relative severity of the possible consequences of the vulnerable conditions.

Table 1 – Threat and Vulnerabilities Severity Categories

Category	Severity	Characteristics
I	Catastrophic	Death or system loss
II	Critical	Severe injury, severe occupational illness, or minor system damage
III	Marginal	Minor injury, occupational illness or system damage
IV	Negligible	Less than minor injury, occupational illness or system damage

Source: MIL-STD-882D

The threat and vulnerability probability levels listed in Table 2 represent a qualitative judgment of the relative likelihood of occurrence of an accident/incident caused by an uncorrected or uncontrolled threat and vulnerability as a result of a particular event or series of events. The table provides a qualitative probability category for a particular event occurring within the entire inventory of substations.

Table 2 – Threat and Vulnerability Probability Categories

Description	Level	Specific Individual Event
Frequent	A	Likely to occur frequently
Probable	B	Will occur several times in the system’s lifecycle
occasional	C	Likely to occur sometime in the system’s lifecycle
Remote	D	Unlikely, but possible to occur in the system’s lifecycle
Improbable	E	So unlikely it can be assumed occurrence may not be

Together, the threat and vulnerability severity and probability properties measure magnitude and the priority for applying control measures. Threats and vulnerabilities are then examined, qualified, addressed, and resolved based on the severity of a potential outcome and the likelihood that such an outcome will occur. The value derived by considering severity and probability is the Threat and Vulnerability Risk Index. The resulting risk index is a measure of the acceptability or undesirability of the threat and vulnerability and is applied to the Threat and Vulnerability Assessment Matrix, as shown in Figure 4.

Table 3: Threat and Vulnerability Assessment Matrix

Frequency of occurrence	Hazard Categories			
	I Catastrophic	II Critical	III Marginal	IV Negligible
(A) Frequent	1A	IIA	IIIA	IIVA
(B) Probable	1B	IIB	IIIB	IIVB
(C) occasional	1C	IIC	IIIC	IIVC
(D) Remote	1D	IID	IIID	IIVD
(E) Improbable	1E	IIE	IIIE	IIVE

Threat and Vulnerability Risk Index

Risk Decision Criteria

- IA, IB, IIA, IIB, IIIA  Unacceptable
- IC, ID, IIC, IID, IIIB, IIIC  Undesirable (Management Decision Required)
- IE, IIE, IIID, IIIE, IVA, IVB  Acceptable with Review by Management
- 

IVC, IVD, IVE

Acceptable Without Review

The Threat and Vulnerability Assessment Matrix assists the decision-making process in determining whether a vulnerable condition should be eliminated, controlled, or accepted, in terms of severity and probability. If the potential for a security incident reveals a Category I (catastrophic) occurrence with a Level A (frequent) probability, the system security effort should be to eliminate the vulnerability through design or at the very least to implement redundant vulnerability control measures prior to entering the transit system or extension's operational phase. An extreme (Category I) or severe (Category II) threat and vulnerability risk may be tolerable if it can be demonstrated that its occurrence is highly improbable. A probable or Level B threat and vulnerability may be tolerated if it can be demonstrated that the result of the occurrence would be marginal (Category III) or negligible (Category IV). This provides a basis for logical management decision-making, considering vulnerability's severity and probability.

3.1 Resolution of Threats and Vulnerabilities

After completing the threat and vulnerability assessment, identified threats and vulnerabilities can be resolved either by assuming the associated risk with the threat and vulnerability or by eliminating or controlling the threat and vulnerability. The most cost effective and technologically efficient approach is to eliminate a known threat and vulnerability by changing the design on paper rather than retrofitting a design once the project is placed into operation. Thus, adequate elimination or control of risk depends on the ability to accomplish the necessary tasks as early as possible in a project's design phases. As threats and vulnerabilities are identified, there is an order of precedence in the threat and vulnerability control process known as the *Threat and Vulnerability Reduction Precedence Sequence*. Various means are employed to reduce the risk to an acceptable level, including:

Threat and vulnerability reduction precedence

- a. Design to eliminate
- b. Design to control
- c. Security devices
- d. Warning devices
- e. Special procedures
- f. Training/Drills
- f. Accept

Factors influencing the threat and vulnerability resolution process

- a. Technological considerations
- b. Time considerations
- c. Relative effectiveness
- d. Feasibility

Design for Minimum Risk

The System Safety Threat and Vulnerability Reduction Precedence Sequence's first step is to eliminate the vulnerability. For example, collisions at grade crossings may be eliminated by grade separating the crossing. In some cases, vulnerabilities are inherent and cannot be eliminated completely through design. In other cases eliminating vulnerabilities is not practical or financially feasible. If the vulnerability cannot be eliminated, it should be reduced to an acceptable level by incorporating fail-safe devices and principles in design, incorporating high- reliability system components, and using redundant or backup hardware and software devices.

Security Devices

Vulnerabilities that cannot be eliminated or minimized through design may be controlled by using appropriate security systems. Security systems include CCTV, remote surveillance devices, video recorders, intrusion motion detectors and smoke or chemical detectors. These are permanent system design features that improve security by automatically controlling the risk of security incidents. Examples of security devices include protective enclosures, guards or barriers, fences and gates, admission control equipment, surveillance equipment

Warning Devices

If designing for minimum risk and using security devices cannot effectively control the threat, warning devices should be used. Warning devices do not provide definitive protection but help prevent and/or reduce the consequences of security related incidences. Intrusion alarms, fire alarms and enunciator panels are examples of warning devices. Since warning devices require a human response, the design should minimize the possibility of human error in that response.

Since constant surveillance by onsite personnel is often infeasible, the practice must be supplemented with other measures that can expand the ability of security staff to monitor large facilities. Surveillance equipment may be particularly appropriate in high-traffic and high-value areas since these systems can be integrated with other monitoring and communications systems to create a coordinated oversight and response center.

Procedures and Training

In addition to controlling threats and vulnerabilities by designing for minimum risk and reducing the associated risk with warning devices, procedures and training should be used. However, this

is the lowest level of control, and relies on training to recognize the threats and vulnerabilities and personnel actions to minimize effects of security incidents.

Threat and Vulnerability Acceptance/System Disposal

Where it is not possible to reduce a threat and vulnerability by any means, a decision must be made to either accept the threat and vulnerability or dispose of the system.

SECTION 4.0: TRANSIT STATIONS

Transit stations are facilities where passengers board and alight from transit vehicles. Stations may serve one or more modes of transit and differ in their levels of design complexity. All transit stations have some component that is at-grade, to connect with the surrounding pedestrian landscape. Stations are typically divided into 3 types of areas, each of which has different security concerns and mitigation measures.

- Unpaid public areas are those locations within the site that passengers occupy before paying their fares (including entryways, lobbies, fare vending space, and concessions).
- Paid public areas are those locations that passengers occupy after paying their fares but before entering a vehicle (including additional passageways, platforms and waiting areas)
- Non-public areas are intended only for authorized transit staff (including administrative offices, electrical and mechanical rooms, HVAC and maintenance areas, and vendor skills

4.1 Potential Threats

Stations are likely targets because they are high-profile facilities that serve large numbers of people in enclosed, relatively small spaces, are easily accessible, and centrally located.

4.1.1 Arson

While stations are designed to be fire resistant, they are still vulnerable to an arson attack ignited either from an accelerant (flammable substance used to increase the spread of fire) brought to the station or from incidental materials such as garbage, vendor goods, and passenger baggage within the station. Any fire that does occur may damage the station and other property, as well as injure passengers and employees.

4.1.2 Explosives

A vehicle carrying explosives that approaches the outside of a station or enters the station could generate a large explosion. The closer the detonation is to the station and its key components, the greater the potential for damage.

Stations are also vulnerable to people hand-carrying explosives into the facility. While the amount of explosives a person can carry produces a smaller blast, human carriers can penetrate deep within a station without detection and can choose a detonation point with the maximum destructive impact on people or structures. Explosives may be detonated on the carrier (a suicide attack) or be hidden in the station for future detonation.

Explosions can cause injuries and fatalities to the passengers and employees in a station, property damage or structural collapse of the station itself, and cause subsequent fire.

4.1.3 Weapons of Mass Destruction (WMD)

As with explosives, someone could carry a WMD device into a station without detection and position it in a location for maximum destructive effect. Substances may be released by hand or hidden for future dispersion, and may cause property damage as well as irritation, injuries, and fatalities among the patrons

and employees exposed. Riders moving through the transit system can inadvertently spread a harmful substance to which they have been exposed, greatly increasing the consequences of such an attack.

4.1.4 Hostage or Violent Event

Stations may be seen as prime targets for a violent event because they are easily accessible, heavily populated by the public, and generally enclosed.

4.2 Perimeter Security

It is impractical to establish a strong perimeter around a transit station, even though it is often necessary to pay and pass through admissions-control barriers to enter the platform. Stations must be as accessible as possible to potential patrons arriving both by foot and in vehicles.

A transit station may have a range of other entrance types depending on the modes served. Some of these entrance types may warrant additional security measures to prevent inappropriate vehicle access, which need not compromise passenger mobility. In addition, selecting a site where it is possible to maintain unobstructed sightlines around key access points or critical areas may also improve security without compromising the station's accessibility.

4.3 Human Access

While transit stations are generally designed to make human access as easy as possible, agencies should consider preventing after-hours access and access to non-public parts of the facility. When the facility is closed, the facility should be secured at its outermost perimeter, with locked gates or doors. Outdoor lighting can be used to illuminate station access points. Intrusion alarms and surveillance may also be helpful.

Since the non-public parts of a transit station may be located in publicly accessible spaces, a combination of access management measures may be necessary to consider. Locks, surveillance, credentialing technology, and highly visible locations may help secure the equipment from tampering. Designs can also cultivate an atmosphere of exposure, which is useful in both discouraging and detecting any unwanted activity. The combination of staff, surveillance technology, and unobstructed sightlines can help both transit personnel and the public to serve as watchdogs, helping to deny the opportunity for covert endeavors, and making any unusual activity easily detectable. In any areas of the station where direct surveillance by staff is difficult or impractical, call boxes can help connect patrons with authorities.

4.4 Emergency Response and Egress

A station's emergency response plan should consider the capacity of the station and the fact that many users will not be familiar with the layout of the station and its emergency exits. Emergency systems can direct occupants to safe exit locations, especially if there are additional exits that are not commonly used for station access.

MDT should consider including emergency communications systems, including blue-light phones and public address systems, in the plan, to allow rapid communications between remote areas of the station.

4.5 Systems and Services

Building systems play a critical role in transit stations because of the large numbers of people present, especially in enclosed facilities. The continuous supply of electricity and ventilation after an attack can improve the ability of people to evacuate the facility. Signage is also critical during an emergency, because many users will be unfamiliar with the station layout and locations of emergency exits. Considerations should be given to incorporating communications systems into the facility, both to direct occupants during an emergency and to enable riders to notify transit staff of any problems or threats they observe.

– Intentionally Left Blank –

SECTION 5.0: ADMINISTRATIVE BUILDINGS AND CENTRAL CONTROL FACILITY

Administrative offices and Central Control Facility (CCF) are the facilities from which transit systems are managed. Administrative functions at these sites include strategic planning, engineering and construction, revenue processing, real estate and community development, and customer service. Operations activities include ongoing supervision of tracks and signals, vehicle tracking, communications with all fleet vehicles, and emergency response. Facilities are typically not open to the public, although administrative offices generate some business-related visitor traffic.

5.1 Potential Threats

CCFs and administrative buildings are potential targets for attack because they are necessary for transit operations and are often linked to the entire system. Terrorists may target a centralized facility as a means of halting service, or of obtaining documents and sensitive information about the system. These facilities are not likely targets for attacks meant to inflict civilian injuries, since they are not usually open to the public and typically contain fewer people than other types of facilities.

5.1.1 Explosives

A vehicle could deliver a large explosive device to the exterior of a facility, or a human carrier could carry a smaller device into a CCF or other administrative building. In addition to injuries, potential property damage, and structural collapse; an explosive blast and any ensuing fire may damage equipment that is necessary for system operations or emergency response, potentially disrupting service or disabling the entire system.

5.1.2 Arson

A fire, especially one deliberately set in a critical area of a CCF or administrative facility, could have the same effect as an explosive blast: injuries, property damage, and destruction of critical equipment that results in the disruption of transit service.

5.1.3 Tampering

Critical operations control and computer systems at administrative buildings and CCFs are at risk of being tampered with because of their importance throughout the transit agency's network. An attacker may tamper with systems to gain control of the system, to inhibit emergency response capabilities, or to obtain information about the system to use in a later attack; all of which potentially endanger transit users and assets throughout the network. Documents that reveal information such as confidential operating procedures or details of the system's design may also be vulnerable to tampering or theft in support of a later attack. Attacks on information systems and documents may be particularly easy for an insider to carry out.

5.1.4 Hostage Situation or Violent Incident

An attacker may use a hostage situation or violent incident in an attempt to gain control of systems operations. Staff could be violently coerced to manipulate the system in a manner that endangers staff, riders, and equipment.

5.1.5 Weapons of Mass Destruction

WMD may be used to contaminate the facility, putting transit employees at risk of illness, injury, and fatality. If the site is contaminated, evacuation of the site may disrupt systems operations. Any substance that proves difficult or impossible to eradicate from the facility could extensively disrupt operations and cause property damage.

SECTION 6.0: ELEVATED STRUCTURES

Bridges and other elevated structures provide a throughway for transit vehicles and their passengers over barriers such as waterways and sites that might otherwise obstruct the right-of-way and airport approaches/takeoffs. Elevated structures provide valuable connections, linking key pieces of infrastructure that enable the movement of people and goods. However, as connectors rather than hubs, these structures do not necessarily host large numbers of people at one time.

Security challenges lie primarily in protecting the integrity of the structure, preserving its usability, and ensuring the safety of its users. Loss of elevated track or bridges can be a major obstacle to continued service, especially for rail-based systems that may be impossible to reroute, and for bridges spanning bodies of water. Rebuilding a damaged elevated structure takes considerable time and expense.

6.1 Potential Threats

Bridges and other elevated structures can impose a major disruption of service because of their role as unique connections within a transit system. Attacks will most likely be designed to cause structural damage that destroys them or renders them unusable, possibly while a transit vehicle is on the structure. Security strategies should focus on protecting components that are critical for structural integrity.

6.1.1 Explosives/Fire

An explosive blast may disrupt services, hurt people, and damage or destroy an elevated structure. Explosives can be delivered to a bridge by several means: a car, truck, or other vehicle driven over, under, or near the elevated structure; a boat or barge positioned under or near the structure; or carried onto the bridge by hand, or positioned by hand on the structure itself. The greater the opportunity to position a large amount of explosives near important structural members of the bridge, the more extensive the damage that can result. Resulting fires may cause damage or collapse to an elevated structure or to nearby assets such as any vehicles on the deck. It may also imperil any passengers or personnel using the elevated structure at the time.

6.1.2 Ramming

A collision of sufficient magnitude may impose a shock to the structure comparable to that of an explosive event. Any vehicle such as a boat, car, truck, bus, or airplane with the opportunity to approach important structural components at great speed may endanger the facility.

– Intentionally Left Blank –

SECTION 7.0: RIGHT-OF-WAY, TRACK, AND SIGNALS

Assets within the right-of-way include track, signaling equipment, power conductors and ancillary assets. Track hardware supports and guides vehicles.

Signaling equipment is a system of visual indicators along the right-of-way informing vehicle operators of transit system conditions and when to stop, slow down, or proceed at full speed. Historically, signals regulate the spacing of trains on a section of track (a “block”) to prevent collision between trains, advise of switch conditions, and coordinate railroad-crossing controls (automatically or manually) to avoid collisions of trains with roadway vehicles and pedestrians. Newer technology now enables some of these functions to be incorporated into alternate communication methods, including wireless systems and data transmission through third rails.

Power is supplied to vehicles via an electrified third rail. Auxiliary equipment along rights-of-way includes such items as fencing, signage, and barriers.

7.1 Potential Threats

Damage or destruction of the track, signaling system, or power conductor along a right-of-way can have significant consequences. These could cause a derailment involving a high number of casualties, damage to vehicles and equipment, or a prolonged disruption of service.

Right-of-way assets also have strategic value to terrorists. With the increased awareness of vulnerability to terrorist attacks, communities are creating Emergency Response Plans, which often rely on transit systems as a means of carrying out mass evacuation and/or delivery of law enforcement and medical services to the affected area. Disabling the transit system by damaging the right-of-way prevents its use as part of such a plan.

Rights-of-way are vulnerable to attacks because of their extensive size and insecure nature. They may pass through locations that are remote, infrequently observed and difficult to secure.

7.1.1 Explosives

The detonation of an explosive device is an effective method of attack within a right-of-way. The device could be set to explode anywhere along the alignment, or when a train passes over the track, inflicting mass casualties and temporarily closing down the line. Explosions can also destroy switches and signaling equipment with the same interruptions of service. The nature of transit rail networks would make it difficult to reroute service around the damage, further disrupting the transit service.

Tampering/Disabling

Sabotage carried out against the track, especially signaling equipment, can cause collisions and derailment. Perpetrators with technical knowledge of track and signal operations could tamper with the signaling and switching equipment in a manner that incapacitates the line, or causes casualties.

7.1.3 Cyber Attacks

As signaling and communications systems merge, they become more centrally controlled by computers. This makes them vulnerable to cyber attacks by computer hackers.

SECTION 8.0: REMOTE EQUIPMENT AND UNMANNED STRUCTURES

Unmanned and remote structures include all of the support structures owned, managed or maintained by a transit agency: electrical substations, communications relay towers, and the like. Though less visible, they are vital to the daily operation, maintenance and management of transit systems.

Remote or unmanned equipment plays a less visible, but critical, role in the transit. Ownership and responsibility for these structures vary among systems. They are not always owned and operated by the transit agency; a separate utility company or other organization may operate them instead. Since they are not high-profile sites and typically have no ongoing staff presence, their value as a terrorist target is exclusively a strategic one: the destruction of a substation or communications tower could prevent effective management of the system or disrupt transit operations. The isolated locations and open design of these facilities make them vulnerable to attack. The most effective strategies for mitigating attacks on these facilities are physical hardening and providing redundancies within the transit system's power or communications network, along with access management for particularly critical structures or those located in notably vulnerable locations.

8.1 Potential Threats

The probable objective of any attack on a substation is to incapacitate it through damage or destruction, and prevent it from providing power to the transit system. The same can be said of communications towers and relays, which allow communication between operations control, emergency response personnel, and vehicle operators or field staff. This would cause a disruption in the control, coordination and/or operation of the transit system. The same result can be achieved by destroying the power lines or tampering with the networking cables leading to or from the facility. This is extremely difficult to prevent.

8.1.1 Explosion/Fire

The detonation of an explosive device is a potential method of attack on an unmanned structure. It would not only incapacitate the facility, but would also create a noticeable event and possibly spread environmentally harmful, flammable on-site substances (coolant in transformers, etc). An attack of this kind would not require direct access to equipment controls or technical knowledge of operations.

8.1.2 Collision

Ramming with a vehicle could incapacitate a substation or tower by destroying key components such as the power poles serving the site. Communications arrays can be somewhat more fragile, and are more endangered by heavy objects that can be thrown or hurled at the structure, damaging its antennae or other critical components.

8.1.3 Tampering

A more sophisticated attack on an unmanned structure is sabotage. Terrorists with technical knowledge of facility operations could activate or modify components of the facility in a manner that not only incapacitates the equipment, but causes damage to other system components as well. This method requires direct access to on-site components.

– Intentionally Left Blank –

SECTION 9.0: COMMUNICATIONS

Most transit agencies use communication systems every day in a multitude of capacities to better serve and protect passengers and employees and to ensure the continued operation of transit service.

In a transit agency, communication system assets include all of the stationary and mobile elements, including control centers, transmission towers and signal repeaters, in-station systems, on-vehicle systems, and handheld personal devices.

Emergencies provide a significant challenge to current telecommunications systems, particularly since technology may be compromised at the very moment that the demand for information is greatest. In addition, most transit agencies do not have the ability to directly communicate with other emergency responders.

9.1 Threats to Transit Communications

While a transit agency's communications system is not a likely target for a terrorist attack intended to inflict civilian injuries, terrorists may target a communications system as a means of halting service, of providing misinformation, or of obtaining sensitive information about the system. Communications systems may be also affected indirectly by an attack elsewhere that compromises communications capabilities.

When analyzing threats to its communications system, MDT should consider threats against physical components of systems and against communications capabilities. These include:

- Physical damage to agency equipment
- Loss of power
- Communications failures outside the agency
- Network failure from excessive demand
- Cyber attacks

Not all of these threats are necessarily caused by intentional actions; some may be the result of accidental extraordinary circumstances, such as region-wide power outages.

9.1.1 Physical Damage to Agency Equipment

Direct physical damage to communications infrastructure is one source of failure. The loss of one or more critical pieces of equipment can render an entire system inoperable.

- **Example** - Damage to towers or repeaters used to broadcast radio transmissions or to the various telephone and communications cables (either buried or strung in the air) with junction connections, could disrupt communications links between the control center and field equipment and vehicles.

Components located in geographically isolated spots may be particularly vulnerable to an attack, since attempts at sabotage are more likely to go unnoticed. However, communications infrastructure may also be destroyed as collateral damage in an attack on an unrelated target, or by accident.

- **Example** - In the terrorist attacks of September 11, 2001, numerous agencies lost communications capabilities due to the physical damage suffered in the World Trade Center. The Port Authority's central communications system was located in the World Trade Center, and its loss affected operations throughout the agency. The New York City Fire and Police departments also lost radio towers and repeaters located on or in buildings in the World Trade Center complex, which compromised their radio communications.

9.1.2 Loss of Power

Since most communications technologies require electricity, loss of electrical power—either locally or over a broader service area—can pose a major problem for communications systems such as radio systems, email, Internet, cell phone, voicemail and call sorting, and computer-aided dispatch. Loss of electricity could be the result of an intentional attack or unintentional event, either within the agency or outside the agency, but either case could hinder a transit agency's ability to communicate effectively.

- **Example** - The Trans-Hudson Emergency Transportation Task Force in the New York area identified communications technology as the leading problem during the 2003 Northeast power outage. Most transportation agencies did not realize the frailty of their technology and thought that they had better backup power than they in fact had. As a result, one major bus agency was without communications between the operations control center and its fleet for over four hours. Several other agencies in the Northeast lost radio communications altogether—either because repeaters failed or backup battery supplies expired—and suspended service as a result.

9.1.3 Cyber Attacks

As communications systems become more advanced, they rely heavily on computers and digital networks for their operation. As with all digital systems, these are susceptible to electronic sabotage by hackers and others intent on disrupting operations. Computer viruses, even those not directly targeted at transit agency communications systems, also pose a significant threat. MDT should consider whether their communications hardware, software, and networks are able to withstand cyber attacks.

9.2 Protection Strategies

It is difficult for any organization to prepare for terrorist attacks or other emergencies that might require a coordinated response because such incidents are largely unpredictable. The problems experienced in one emergency may be different the next emergency.

In considering how to protect its communications systems and ensure those systems can respond to an emergency, a transit agency should consider two issues: protecting its *physical assets* (e.g., communications hardware), and protecting its communications *capabilities*. Striving to do both will result in a communications system that is more robust and, ultimately, more versatile.

Lessons from prior events suggest the following types of strategies can help protect a communications system from the effects of a terrorist attack:

- Hardening and access management
- Redundancy

- Backup power supply
- Prioritization service and dedicated landlines
- Network security

Each transit agency faces a particular set of circumstances and needs; no single communications security strategy is appropriate for every agency. MDT should consider factors such as its communications needs, threat assessments, budget, and existing systems to determine which of the above strategies best fit its goals.

9.2.1 Hardening and Access Management

The most straightforward approach to protecting a transit agency's communications system is to safeguard the physical components of that system. Preventing unauthorized access to transmitters, relay towers, and computer control centers through access management and perimeter control helps to ensure that the components will not be sabotaged, stolen, or misused. Similarly, reinforcing the components and the structures that house them helps to prevent damage to the components in the event of an attack or similar situation.

9.2.2 Redundancy

An agency should ensure that it has built in sufficient redundancy to survive damage to a part of the system, and should strive for a layered approach to communicating with its major audiences. A layered approach means either having duplicate equipment, so that second-string infrastructure can be utilized in case the usual system becomes incapacitated, or having multiple forms of communications, so that even if one type of communications technology is not working, another might remain operable.

9.2.2.1 Redundancy by Duplication

This type of redundancy helps an agency reduce vulnerability to single points of failure within its communications systems by avoiding reliance on an individual facility or piece of hardware. For example, preparing an alternate antenna system would allow agency communications to continue if the main antenna goes off line because of either manmade or natural events. Agencies should consider locating primary and duplicate equipment in separate locations to reduce the likelihood of both sets being compromised during an event.

Feasibility

The expense of procuring and maintaining duplicate equipment may be beyond the limits of a MDT's available resources, and may be hard to justify for what might be considered an unlikely event. Off-site locations also imply additional capital and operating expenses. Careful positioning of duplicate equipment may be warranted, depending on the vulnerability of the main communication systems and the criticality of continued communications for operations activities. MDT should assess duplication within its own unique environment; some systems and equipment might be more worthwhile to bolster with redundancy than others.

In general, equipment that might be feasible and worthwhile to duplicate include:

- Antennas that support mobile (radio) communications
- Essential landlines
- A communications center

9.2.2.2 Redundancy by Variety

This type of redundancy means including different options that might each continue to work under different sets of adverse circumstances. This strategy may offer an agency more resiliency than duplication, because circumstances sometimes might preclude the use of a certain type of equipment altogether.

- **Example** - In New York and Washington, D.C. on September 11, 2001, immediate communication with agency field staff and emergency responders was difficult because telephone landlines were damaged and mobile communications systems were overloaded or did not provide adequate coverage. In this case, extra landline telephones or cell phones would not have been useful, but an independent system such as a dedicated internal phone line might have worked.

Feasibility

While redundancy by duplication may be prohibitively costly, redundancy by variety may be more feasible since there may be inexpensive alternatives that, although not perfect substitutes for a primary system, may be sufficient in an emergency situation.

Handheld radios and pagers can provide a low-cost redundant system for communications among field staff.

- **Example** - Using handheld radios, NYCT was able to evacuate 400,000 people in three hours during the 2003 Northeast blackout and to ensure staff members were in place at key locations. Such a system is also scalable, since the number of units purchased and operated can be expanded or reduced depending upon each agency's requirements.

An easy way for agencies to incorporate redundancy is to keep obsolete equipment even after it has been replaced by a newer, upgraded system.

- **Example** - When the Suburban Mobility Authority for Regional Transportation in the Detroit area lost an ISP connection during the 2003 blackout, an old dialup modem (and backup generators) allowed the authority's communications center to stay connected during the outage.

MDT might consider any combination of the following options to assemble a resilient communications "toolkit":

- A dedicated digital trunked mobile radio communications system
- Conventional and mobile phone service with prearranged priority
- An internal analog phone system
- Dedicated landlines
- Walkie-talkies

- PDAs and pagers
- Backup point-to-point microwave link
- Backup access to a satellite communication service
- Transit agency radio system linked to public safety agencies through interoperability
- Joining an area-wide digital public safety radio system

9.2.3 Backup Power Supply

Since most agency communications equipment requires electricity to function, backup power supplies are essential for any capabilities to be maintained in case of an emergency.

An agency may want to be prepared to support its own mobile radio communications system, onsite computer equipment, and telephone switch. Each agency must assess which systems warrant backup and the amount of necessary reserve power. Agencies have a number of backup power source options, including batteries and generators.

For each piece of communications equipment, the agency should consider the full ramifications of both a brief interruption and an extended outage, in order to be prepared for both types of events. Considering every piece of equipment in different scenarios helps reduce the chances of surprises later. A conventional telephone system may not require power from the grid in order to function, but if an on-site telephone system has a computer-automated call-handler, or if the telephones onsite require electricity in order to function, the agency might not have access to the conventional telephone system during a power outage.

- **Example** - During the 2003 blackout, transportation agencies learned to keep some low-tech phones on hand and to arrange for a dial-around option that circumvented the computer-automated voicemail system in case of a power outage. Other agencies realized, during an extended outage in August, that computer equipment supported by backup generators would require air conditioning to maintain a safe operating temperature. If computer equipment is supported by backup power, agencies may consider allowing air conditioning equipment to be looped into the backup system if the computers must run for an extended period during hot weather.

In addition to servicing key functions at an agency's communications center, a transit agency should consider which field equipment should also be supported with backup power, if possible.

- **Example** - Remote towers and transceivers could be equipped with auxiliary power and cabling protection at the main communications towers.

9.2.4 Prioritization Service and Dedicated Landlines

Since communications networks can sometimes be overwhelmed with use, especially during emergencies, transit agencies can ensure their own communications capabilities by arranging for prioritized access to network services, or by obtaining their own internal dedicated phone lines.

The federal government has instituted services that help designated agencies complete priority calls through both the landline and wireless telephone networks. The Government Emergency Telecommunications Service⁵⁰ (GETS) and the Wireless Priority Service⁵¹ (WPS) provide pre-approved

users with priority routing of landline (GETS) and wireless (WPS) calls during times of emergency and crisis, even during periods of peak demand. GETS and WPS are available to federal, state, and local government agencies, as well as to private companies and organizations, with responsibility for national security or emergency preparedness. On September 11, 2001, and the days following, there were more than 18,000 GETS calls with a completion rate that exceeded 95 percent. During the 2003 blackout, there were about 1,800 calls made.

Another option is to invest in an internal analog phone system that is not dependent on the commercial telephone system to connect points within the agency or to connect the agency's communications center to essential partner agencies. Dedicated lines may be valuable assets in times when the conventional telephone service is unavailable, or when the commercial telephone system is overwhelmed.

System: Stations Subsystem: Systemwide PHA No.: A1.1 & A1.2 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet ___ of ___ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/System		Possible Controlling Measures and Remarks	Resolution
A1.1	Criminal acts against passengers or employees (e.g. robbery, assault, etc.)	Inadequate CCTV coverage Isolation of station platform from public view	Minor to serious injury or loss of life due to exposure to fire and smoke	Before Resolution II-B Residual After Resolution II-E	Provide roving station security personnel for isolated stations Provided CCTV coverage Restrict and lock station facilities	
A1.2	Vandalism of station platform	Unlocked station facilities (break room) Inadequate lighting Obstructed lines of sight on station platform	Loss of personal property		Provide emergency communications for patrons Provide adequate lighting	

System: Stations Subsystem: Systemwide PHA No.: A1.3 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet ___ of ___ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
A1.3	Theft from MDT revenue collection or the concessionaire	Inadequate CCTV coverage Isolation of station platform from public view Unlocked station facilities (break room) Inadequate lighting Obstructed lines of sight on station platform	Minor to serious injury or loss of life Loss of revenue Loss of personal property	Before Resolution II-B Residual After Resolution II-D	Provide roving station security personnel for isolated stations Provided CCTV coverage Restrict and lock station facilities Provide adequate lighting	

System: Stations Subsystem: Systemwide PHA No.: A1.4 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
A1.4	Vehicle intentionally rams operations equipment	Mechanical rooms / ancillary rooms located too close to road and parking areas	Minor to serious injury or loss of life due to explosives Damage to critical operations equipment	Before Resolution II-B Residual After Resolution II-E	Set all operations equipment and mechanical rooms back from roads and parking areas Set physical barriers such as bollards, road spikes, and fencing to enforce setbacks and/or prevent ramming Design minimum number of vehicle entrances into station area Avoid obstructed sightlines surrounding the station	

System: Stations Subsystem: Systemwide PHA No.: A1.5 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet ___ of ___ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
A1.5	A perpetrator hiding behind a kiosk, ad, column or other blind corner attacks a patron	Station design allows for unnecessary sightline obstructions	Minor to serious injury or loss of life. Loss of personal property	Before Resolution II-B Residual After Resolution II-D	Design interior station with unobstructed sightlines minimizing hidden areas or remote passageways Position kiosks, ads and information to not obstruct sightlines Minimize use of columns and blind corners Consider security mirrors on columns and corners Position operator booth for maximum presence and visibility within station	

System: Stations Subsystem: Systemwide PHA No.: A1.6 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet ___ of ___ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/System		Possible Controlling Measures and Remarks	Resolution
A1.6	Perpetrator attempts to vandalize mechanical rooms or other critical assets	Critical asset is located too close to perimeter Critical asset is located in isolated area Inadequate lighting Obstructed lines of sight	Minor to serious injury or loss of life Damage to critical equipment	Before Resolution II-B Residual After Resolution II-E	Locate critical assets in transit stations wherever possible, with adequate surveillance Provide roving station security personnel for isolated stations Provided CCTV coverage Secure critical equipment with gates, locks, or other access control measures Provide adequate lighting	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
A1.7	Unattended suspicious package goes unreported	Terrorist plants package in station area to be detonated by remote control	Minor to serious injury or loss of life due to explosives Damage to critical operations equipment	Before Resolution II-B Residual After Resolution II-E	Post and/or broadcast instructions on how to report suspicious activities Use bright paint colors to increase ambient lighting Consider installing CCTV Smart Systems	
A1.8	Package containing bomb detonates inside station area				Design stations using shatter-proof glazing Design station using façade materials that resists explosive blasts Design stations utilizing fire retardant construction materials	

System: Stations Subsystem: Systemwide PHA No.: A1.9 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
A1.9	Potential perpetrator attempts to hide in or near station area in order to attack an unsuspecting victim.	Inadequate surveillance at critical station points. Insufficient lighting	Minor to serious injury or loss of life Loss of personal property	Before Resolution II-B Residual After Resolution II-D	Install appropriate surveillance at entrances, at access points to non-public areas, and throughout the station. Insure sufficient lighting for nighttime surveillance. Install intrusion alarms at access points to non-public areas	
					Sheet __ of __	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT & VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
System: Stations Subsystem: Park and Ride Lots and Garages PHA No.: A2.1 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Prepared by: M. Cephas Reviewed by: Approved by:	Date: Date: Date:
A1.1	Criminal acts against passengers or employees (e.g. robbery, assault, car theft, etc.)	Inadequate CCTV coverage Isolation of lot/garage from public view Inadequate lighting Obstructed lines of sight in lots and garage Lack of security patrols	Minor to serious injury Loss of personal property	Before Resolution II-B Residual After Resolution II-D	Provide roving station security personnel for Park and Ride lots and garages Provide CCTV coverage Provide emergency communications for patrons Provide adequate lighting Provide non sight obstructing landscaping, (i.e. low shrubs and limbed-up trees)	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		HAZARD RISK INDEX	CORRECTIVE ACTION	
No.	Threat & Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
A3.1	Unauthorized trespass across tracks or unregulated entry across tracks	Unrestricted access to tracks and platforms	Minor to serious injury	Before Resolution I-B Residual After Resolution I-E	Provide warning signs Design station crossing to direct personnel across the specific locations Direct and channel pedestrians and vehicular circulation with sidewalk treatments, paving, vegetation, bollard and chain/cable, railings, or other treatments Enforce use of pedestrian access points Maintain walkways, fences, warnings, signs, and treatments at stations	

System: Communications Subsystem: Telephone PHA No.: B1.1 to B1.3 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Hazard Description	Potential Cause(s)	Effect on Subsystem/System		Possible Controlling Measures and Remarks	Resolution
B1.1	No payphone or emergency phone provided	Vandalism Phone removed by utility due to low revenue Not provided	No communications to emergency services No communications with central control Can be a contributing factor in criminal act	Before Resolution II-C Residual After Resolution II-E	Install payphones Install passenger information/emergency phones Utility agreement, which keeps all phones in service irrespective of revenue	
B1.2	Damaged or missing payphone or emergency phone	Lack of maintenance Vandalism	Loss of communications with external agencies		Periodic inspections and reporting procedures to report damaged or missing phones Utility maintenance agreement	
B1.3	Central control phone system failure	Broken utility wire or other service outage Power failure			Alternate communications system – radio or cell phones Emergency generator or UPS	

System: Communications Subsystem: Public Address System PHA No.: B2.1 to B2.2 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet ___ of ___ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
B2.1	PA & VMS System inoperable during a bomb threat	Loss of power at station Loss of power at CCF	Audio and visual evacuation messages will not transmit Minor to serious injury or loss of life due to lack of communication	Before Resolution II-B Residual After Resolution II-E	Install UPS System capable of supplying at least 4 hours of power	
B2.2	Voice transmission unintelligible when trying to communicate an evacuation notice					

System: Communications		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet __ of __			
PHA No.: B2.3					Prepared by: M. Cephas		Date:	
Rev. No.: DRAFT					Reviewed by:		Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION			
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution		
B2.3	Communication links become inoperable during an emergency	Terrorist damages towers or repeaters used to broadcast radio transmissions or to the various telephone and communications cables	Disruption of communication links between control center and field equipment and vehicles Minor to serious injury or loss of life due to lack of communication	Before Resolution II-B Residual After Resolution II-E	Prevent unauthorized access to transmitters, relay towers, and computer control centers through access management and perimeter controls Reinforce the components and structures that house communications equipment including hardening the perimeter			

System: Facilities Subsystem: Operations Control Center (CCF) PHA No.: C1.1 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C1.1	Vehicle intentionally rams CCF	Terrorists attempt to detonate explosives Criminals attempt to gain access to building	Minor to serious injury or loss of life Potential hostage situation Damage to CCF facility	Before Resolution II-B Residual After Resolution II-E	Design CCF facility to be set back from roads and parking areas Consider installing barriers such as bollards, road spikes, and/or fencing to enforce setbacks and prevent ramming Minimize the number of access points to the facility	

System: Facilities Subsystem: Operations Control Center (CCF) PHA No.: C1.2 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C1.2	Employees victimized while attempting to enter CCF facility	Facility is situated in an obscure location- Building entrances facing unsecured areas	Minor to serious injury or loss of life Potential hostage situation Damage to CCF facility	Before Resolution II-B Residual After Resolution II-E	Locate facility in an area that's visible and has unobstructed sightlines Avoid designing entrances facing unsecured areas Design facility maximizing surrounding the building	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C1.3	Intruder hides in obscure corner of the CCF interior waiting to pounce on an unsuspecting victim	Building design contains unnecessary blind corners and hidden areas	Minor to serious injury or loss of life Potential hostage situation	Before Resolution II-B Residual After Resolution II-E	Segregate zones of activity and building uses Buffer critical assets from public or vulnerable areas Minimize ability to isolate critical areas and maintain operations Secure critical areas and equipment with gates, locks, or other access control measures	

System: Facilities Subsystem: Operations Control Center (CCF) PHA No.: C1.4 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS		Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:		
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C1.4	Terrorist plants bomb inside CCF facility	Building layout provides obstructed sightlines and hidden areas Building is infiltrated due to the lack of adequate surveillance equipment	Minor to serious injury or loss of life Potential hostage situation	Before Resolution II-B Residual After Resolution II-E	Building design should minimize hidden areas and blind corners Install adequate surveillance equipment Design should minimize obstructed sightlines and hidden areas Avoid designing entrances facing unsecured areas	

System: Facilities Subsystem: Operations Control Center (CCF) PHA No.: C1.5 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C1.5	Bomb detonates inside CCF	Terrorist plants package in CCF facility to be detonated by remote control	Minor to serious injury or loss of life Damage to CCF facility	Before Resolution II-B Residual After Resolution II-E	Design stations using shatter-proof glazing Design station using façade materials that resists explosive blasts	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C2.1	Unmanned electrical substation is incapacitated due to an explosion	Terrorist detonates explosive device	Damage to building and equipment Possible disablement of rail service	Before Resolution II-B Residual After Resolution II-E	Locate key equipment towards the center of the site Utilize reinforced structures Secure access doors with multiple locks or other access control measures Provide emergency shutdown mechanisms Provide surveillance and intrusion alarms Provide redundant power supply systems and routings	

System: Facilities Subsystem: Unmanned Structures PHA No.: C2.2 Rev. No.: DRAFT		MIAMI DADE TRANSIT NORTH CORRIDOR EXPANSION PROJECT THREAT AND VULNERABILITY ANALYSIS			Sheet __ of __ Prepared by: M. Cephas Date: Reviewed by: Date: Approved by: Date:	
GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
C2.2	Unmanned electrical substation or communications relay tower is compromised and vandalized	Intruder unlawfully enters the facility	Damage to building and equipment Possible disablement of rail service	Before Resolution II-B Residual After Resolution II-E	Secure access doors with multiple locks or other access control measures Provide surveillance and intrusion alarms Provide redundant power supply systems and routings	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
D1.1	Vehicle intentionally rams critical structure support	Structure support located too close to road and parking areas	Minor to serious injury or loss of life Damage to elevated structure	Before Resolution II-B Residual After Resolution II-E	Restrict access to land below structure, where possible Set all structure supports back from roads and parking areas Set physical barriers such as bollards, road spikes, and fencing to enforce setbacks and/or prevent ramming Avoid obstructed sightlines under and around structure Design adjacent roadways to inhibit high-velocity ramming of columns	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
D1.2	Bomb explodes in track area of elevated structure at or near a revenue train	Terrorist plants and detonates a bomb on or near a revenue train on an elevated structure	Minor to serious injury or loss of life Damage to elevated structure	Before Resolution II-B Residual After Resolution II-E	Design the elevated structure's emergency access points to be easily assessable for emergency personnel Design to provide protected locations for limited mobility occupants to wait for emergency personnel. Secure emergency and maintenance access points with gates, locks, or other Choose materials that make columns difficult to climb and use fire retardant construction materials	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
D1.3	Vandals deface elevated structure supports	Supports located in an obscure area	Minor to serious injury or loss of life to the vandal attempting to deface the structure Damage to elevated structure	Before Resolution III-B Residual After Resolution III-C	Install motion detectors or intrusion alarms at vehicle entrances and other restricted-access areas around the structure	
D1.4	Vandal attempts to damage or tamper with electrical conduits and utilities located on elevated structure	Electrical conduits and utilities exposed			Build electrical conduits and utilities into the elevated structure to reduce exposure to vandals and fire	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
E1.1	Bomb explodes in switch or signal device	Terrorist plants and detonates a bomb in vital track component, causing a train collision or derail	Minor to serious injury or loss of life Damage to train and/or track area	Before Resolution II-B Residual After Resolution II-E	Design right-of-way with unobstructed sightlines, where possible Provide right-of-way set back from roads and parking areas Provide physical barriers such as bollards, fencing and grade changes, where possible Secure emergency and maintenance access points with gates, locks, or other access control measures	

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
E1.2	Signal system is disabled and switch fails to operate correctly	Vandal tampers with switchbox and/or signal box	Possible derail	Before Resolution II-B Residual After Resolution II-E	Control signal boxes and switchboxes should be secured with locks or other access control measures. Secure emergency and maintenance access points with gates, locks, or other access control measures to deter vandals Install tamper resistant equipment	
E1.3	Switchbox and/or signal box is vandalized		Possible train collision Minor to serious injury or loss of life Damage to trains and/or track area			

GENERAL DESCRIPTION		THREAT AND VULNERABILITY CAUSE/EFFECT		THREAT AND VULNERABILITY RISK INDEX	CORRECTIVE ACTION	
No.	Threat and Vulnerability Description	Potential Cause(s)	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
E1.4	Signal box and/or signal box maliciously altered	Vandal tampers with switchbox and/or signal box	Possible derail Minor to serious injury or loss of life Damage to train and/or track area	Before Resolution II-B Residual After Resolution II-E	Install motion detectors or intrusion alarms on critical equipment Consider installing a remote surveillance system	

– Intentionally Left Blank –