U.S. Department
of Transportation

Federal Transit
Administration

Transit Security Design Considerations

Final Report
November 2004

FTA Office of Research Demonstration and Innovation

FTA Office of Program Management

Prepared for the FTA by:

Research and Special Programs Administration

John A. Volpe National Transportation Systems Center
Cambridge, MA 02142-1093

FTA-TRI-MA-26-7085-05
DOT-VNTSC-FTA-05-02

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Trade or manufacturers' names may appear herein solely because they are considered essential to the objective of this report. The United States Government does not endorse products or manufacturers.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE November 2004	3. REPORT TYPE AND DATES COVERED Final Report January 2003 to January 2005

4. TITLE AND SUBTITLE
Transit Security Design Considerations

5. FUNDING NUMBERS
TT890
BM177

6. AUTHOR(S) Matthew Rabkin, Robert Brodesky,* Frank Ford,* Marsha Haines,* Jordan Karp,**** Kristin Lovejoy,* Terry Regan,** Linda Sharpe,*** Margaret Zirker***

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Research and Special Programs Administration
Volpe National Transportation Systems Center
55 Broadway, Kendall Square
Cambridge, MA 02142-1093

8. PERFORMING ORGANIZATION REPORT NUMBER

DOT-VNTSC-FTA-05-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Transit Administration
Office of Research Demonstration and Innovation/Office of Program Management
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

FTA-TRI-MA-26-7085-05

11. SUPPLEMENTARY NOTES

*EG&G Technical Services, Inc. **Planners Collaborative ***Cambridge Systematics ****Chenega Advanced Solutions & Engineering, LLC

12a. DISTRIBUTION/AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This document provides security design guidance on three major transit system components – bus vehicles, rail vehicles, and transit infrastructure. It provides a resource for transit agency decision makers, members of design, construction and operations departments, security and law enforcement personnel and consultants and contractors, in developing an effective and affordable security strategy following the completion of a threat and vulnerability assessment and development of a comprehensive plan.

Developed by the Federal Transit Administration in collaboration with transit industry public and private sector stakeholders, these design considerations provide actionable steps that transit agency staff can select from to create a security strategy.

14. SUBJECT TERMS
Public transit, security, transit security, design, threat and vulnerability assessment, access management, systems integration

15. NUMBER OF PAGES
341

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

This page left intentionally blank

Preface

As transit agencies across the United States take steps to protect their systems from possible terrorist attacks, agency decision makers are confronted with numerous security issues and demands. They must assess passengers, system assets, and potential threats, and determine which threats are most likely and which have the potential to cause the most damage.

To help the public transit industry manage these high-risk security demands, the Federal Transit Administration (FTA) has collaborated with the Volpe National Transportation Systems Center of the U.S. Department of Transportation (the Volpe Center), the Transit Cooperative Research Program (TCRP) of the Transportation Research Board (TRB), the American Public Transportation Association (APTA), and other stakeholders to develop an approach for protecting public transit systems that recognizes the fundamental interconnectivity of transit systems, and emphasizes the importance of readiness and vigilance.

This document provides an overview of the major assets of transit systems—bus vehicles, rail vehicles, and transit infrastructure and communications—as well as a preliminary assessment of the vulnerabilities to various methods of attack inherent in each asset. In addition, this document addresses the topics of access management, systems integration, and communications—all crucial to the protection of transit assets. Although many of the subject areas are addressed discretely in the document, users of the resource must recognize the interconnectivity of the considerations and hardening strategies that are presented. For this reason, consulting the sections on both infrastructure and access management will provide additional value when developing a strategy for protecting and hardening a maintenance facility or rail terminal.

The FTA transit security initiative recognizes that public transit is a frequent target of terrorist activities—nationwide as well as worldwide. FTA has based the next phase of its transit security program on the objectives of the National Strategy for Homeland Security, which was issued on July 17, 2002. When a transit agency improves the security of its assets and infrastructure, there are direct benefits through protecting people and indirect benefits through operational and service enhancements. This, and other security-related efforts, will help transit agencies meet their highest priority—the protection of passengers, employees, vendors, and contractors, and the general public.

The FTA's Office of Research, Demonstration and Innovation (TRI) and Office of Program Management (TPM) sponsored the development of these *Transit Security Design Considerations,* and sincerely thanks Task Managers Rhonda Crawley from TPM and Lewis Clopton from TRI for their management and leadership.

The FTA acknowledges the efforts of Richard Gerhart (TPM) and Ronald Jackson, Office of the Chief Counsel, and the contributions of Marcel Belanger, Brian Cronin, Quon Y. Kwan, Henry Nejako, Sean Ricketson, and Terrell Williams from TRI on various transit industry working groups.

The FTA extends sincere thanks to the team at the Volpe Center for their research, coordination, and preparation of these considerations, with particular thanks to Matthew Rabkin, project team leader, and Joseph LoVecchio, team leader for the chapter on communications. Analysts and writers include: Robert Brodesky, Frank Ford, Marsha Haines, and Kristin Lovejoy from EG&G Technical Services; Terry Regan from Planners Collaborative; Linda Sharpe and Margaret Zirker from Cambridge Systematics; and Jordan Karp from Chenega Advanced Solutions & Engineering. The FTA also appreciates the efforts of the editing team of Elizabeth Bent, Katherine Blythe, Nathan Grace, and Cassandra Oxley from Chenega Advanced Solutions & Engineering.

In addition, the FTA acknowledges the contributions of the members and staff of APTA and the Community Transportation Association of America, along with the staff of the TRB. The FTA also acknowledges the contributions of Nicholas Bahr and Robert Lauby of Booz Allen Hamilton, along with David Wagner and Kevin Chandler of Battelle.

Finally, the FTA would like to acknowledge the input of the following transit industry members who provided technical expertise as members of the Transit Security Working Group, Systems Integration Working Group, Credentialing Working Group, Access Management Working Group, Surface Infrastructure Working Group, Tunnel Infrastructure Working Group, Bus Vehicle Working Group, Rail Vehicle Working Group, and Communications Working Group. Names of individual working group members are listed in the Transit Industry "Working Groups" reference material following the appendices.

Executive Summary

Since the events of September 11, 2001, the Federal Transit Administration (FTA) has initiated an aggressive effort to assess and strengthen the security readiness of the public transit industry. For many transit agencies in the United States, particularly small- to medium-sized agencies, the need for greater security awareness and preparation has reshaped the task of providing transportation services to the public. To assist the public transit industry in managing these new demands, FTA has developed security-oriented design considerations for transit bus and rail vehicles, and for the transportation infrastructure. These considerations are intended to aid transit agencies in developing security strategies.

FTA developed these design considerations in collaboration with transit industry public and private sector stakeholders. They are not intended to provide industry-wide standards, but rather a compendium of actionable steps from which transit agency staff can select from when creating a security strategy. Intended to guide public transit agencies in their efforts to deter and minimize the effects of attacks against their facilities, riders, employees, and the general public, these considerations can be implemented as part of efforts to harden and retrofit transit agency assets. This document provides guidance on three major components of transit systems—bus vehicle, rail vehicles, and transit infrastructure—addresses the topics of systems integration, access management, and communications, all of which are crucial to the protection of transit assets.

This document is a resource for transit agency decision makers, members of design, construction and operations departments, security and law enforcement personnel, and consultants and contractors, in developing an effective and affordable security strategy following the completion of a threat and vulnerability assessment (TVA) and development of a comprehensive plan. In developing a security strategy, a transit agency must determine which of its security issues are most critical, and then establish a timeline for addressing them. The ultimate goal of the strategy is to move a transit agency closer to achieving an integrated security system by combining to varying degrees (depending on the issues) design, access management, communications, technology, and system integration practices.

Transit agencies can implement their strategy incrementally, and make discrete decisions as to which countermeasures are most appropriate for new construction, reconstruction and retrofits, and vehicle procurements. If security strategy is implemented with a systems approach in mind, a transit agency could eventually build an integrated security system—one that is flexible and scalable and transmits information and data in real time. This, however, requires vigilance to ensure that security considerations are incorporated into the agency's programmatic, operational, and financial decisions.

This document consists of nine chapters and several appendices. The first four chapters present a macro view of transit security, beginning with a discussion of FTA's rationale for developing security design considerations. The introductory chapters also address the dilemma facing transit agencies of maintaining open systems versus making them more secure. Public transit agencies operate systems in which public access not only is crucial to their daily operations; it also fulfills the

agency's mission. However, in the new security paradigm, agencies should consider ways to use existing and emerging design applications and technologies to harden physical assets and ensure that the sensitive areas of systems are accessible only by those permitted to be there.

The introductory chapters also take into account the multiple ways in which public transit systems are in fact systems, connected not only physically but also through an intricate network of technology, law, and regulation, linked together and to other elements of the regional transportation network. These chapters also emphasize the importance of developing a security strategy based on the criticality of the agency's vulnerabilities, and consider priorities for addressing them. The discussion recognizes the complexity of the transit environment, by advocating the importance of using a system approach to integrate the diverse functions, technologies, and operating relationships.

The following chapters present specific design considerations relating to an agency's physical assets—bus and rail vehicles, infrastructure components, and communications equipment and systems, along with a discussion of the tools necessary for building an integrated security system—access management, communications, and systems integration.

Table of Contents

List of Figures

List of Tables

1.0 Introduction

Since the events of September 11, 2001, the Federal Transit Administration (FTA) has initiated an aggressive effort to assess and strengthen the security readiness of the public transit industry. For many transit agencies in the United States, particularly small- to medium-sized agencies, the need for greater security awareness and preparation has reshaped the task of providing transportation services to the public. To assist the public transit industry in managing these new demands, FTA has mobilized not only its own resources but also those of other stakeholders to develop an approach to protecting public transit that emphasizes the fundamental interconnectivity of transit systems and the importance of readiness and vigilance.

This document offers preliminary security-oriented design considerations for transit bus vehicles, transit rail vehicles, and transit infrastructure as a whole. These considerations are intended to assist public transit agencies in their efforts to deter and minimize the effects of attacks against their facilities, riders, employees, and the general public. The public transit industry has a long history of defining its own infrastructure needs and designing and constructing to meet them; consequently, these design considerations are intended to supplement and assist, not to impose a standard.

This effort reflects an increased awareness of the importance of the physical components of public transit. The threat of terrorism and other acts of large-scale violence can be combated not only through administrative policies and new technologies—although both are important—but also through the physical protection of the structures of which public transit is comprised. The FTA security design considerations will provide the transit industry with suggested security-oriented modifications to the physical and technological infrastructure of rail and bus systems. In addition to providing guidance on three major components of transit systems—bus vehicles, rail vehicles, and transit infrastructure—this document addresses the topics of systems integration, access management, and communications, all of which are crucial to the protection of transit assets.

This chapter provides an overview of:

- The importance of security for transit
- U.S.DOT strategic goals
- FTA security goals
- Document **scope**
- Research **methodology**
- **Audience** for the document
- **Organization** of the document

1.1 Importance of Security for Transit

There are approximately 6,000 public transit agencies operating in the United States,[1] the majority of which provide more than one type of service and operate more than one type of vehicle. Many agencies also contract for additional services from private operators, further increasing the complexity of the provision of public transportation services. The threat of terrorism against the U.S. public transportation system historically has been low but cannot be discounted. While worldwide there are more security incidents in public transportation than other modes, it is considered a safe environment for the riding public. Appendix A, "Chronology of Terrorist Attacks Against Public Transit," lists some of the more significant attacks against public transit both in the United States and the rest of the world. Transit systems must continue to enhance their security systems, facilities, and vehicle designs to ensure the safety and security of the riding public.

Possible Impacts of Attacks

- Crippled transit service
- Multiple casualties (passengers, employees and/or bystanders)
- Damage to transit property and/or assets
- Damage to surrounding environment
- Stunted economic activity or growth
- Reduced evacuation capacity

Unlike an office building or even an airport, public transit systems cannot simply be closed off or tightly controlled without compromising their fundamental character. Security must be created in other ways, through physical modifications that do not impinge upon the openness of the system, through employee training and watchfulness, through passenger awareness and participation, and through careful planning for coordinated, efficient, and life-saving response. Each of these security-oriented elements must be knit together with the others, and with the other policies and procedures of the agency, so that security becomes a network, reflecting the integrated nature of public transit.

Despite differences of size, scale, and location, all transit agencies share the macro-level commonality of managing integrated systems and facilities, and all share the vulnerabilities inherent in that connectivity. All transit agencies:

- Have multiple physical assets, some owned, some leased, and some shared,
- Operate within a regulatory and legal framework that defines their relationships with their employees, their riders, and the rest of the transportation network, and
- Use technology.

Transit agencies across the country also face tight budgets and constrained sources of funding, limiting their ability to make unanticipated investments in expensive new equipment and technologies. Their commonalities make it possible to articulate shared vulnerabilities among transit agencies and to develop security-oriented design considerations that can be relevant throughout the public transit industry.

[1] See **http://www.apta.com/research/stats/overview/overview.cfm**.

These design considerations offer guidance for an industry that is not static, and recognize that system-wide security-oriented modifications will take time to implement.

1.2 U.S. DOT Strategic Goals

Security is only one characteristic of a successful, efficient transportation system. The U.S. Department of Transportation's current strategic plan calls for "Safer, Simpler, Smarter Transportation Solutions," and identifies five strategic goals for achieving this vision: safety, mobility, global connectivity, environmental stewardship, and security.[2] Three of these goals—safety, mobility, and security—speak specifically to the mission of this document—to present integrated security design guidance which transit agencies of all sizes would find practical and effective to implement as part of a strategy to protect and minimize the impact of a terrorist attack. Though they do not speak directly to this mission, the remaining two—global connectivity and environmental stewardship—are vital to the success of a robust, vibrant public transit system and should not be overlooked when determining appropriate security strategies.

1.3 FTA Security Goals

This project is part of an aggressive and multi-faceted FTA program to evaluate and strengthen the security readiness of the public transit industry. Globally, as shown in the "Chronology of Terrorist Attacks Against Public Transit" (see Appendix A), public transit is a frequent target of terrorist attack, an easy and accessible way to take lives, cause damage, spread fear, and impact local, regional, and national economies.

The FTA has based its transit security program on the objectives of the National Strategy for Homeland Security, which was issued on July 17, 2002, and represented one of the initial undertakings of the White House Office of Homeland Security, created in October 2001. Its program emphasizes asset protection, public awareness, and emergency response.

This project to develop security design considerations for the protection of transit assets stands alongside the other efforts described here as part of a holistic, FTA-guided process to develop and reinforce the tools needed to guard against transit-oriented terrorist attacks. Besides developing security design considerations, other FTA-sponsored security activities include:

- Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT)[3]
- Threat and vulnerability assessments of the 36 largest transit agencies

[2] See the U.S. DOT Strategic Plan 2003 – 2008 at http://www.dot.gov/stratplan2008/strategic_plan.htm#_Toc52257030 for a more detailed description of the U.S. DOT's vision, strategic goals, and objectives.

[3] http://transit-safety.volpe.dot.gov/security/pdf/protect_factsheet.pdf.

- Technical assistance to the 50 largest transit agencies
- Connecting Communities Regional Security Forums
- Top 20 Security Program Action Items for Transit Agencies
- Transit Threat Level Response Recommendations[4]
- Public Transportation Security Volumes I and II [5] (prepared by TCRP)
- Security roundtables with transit agency general managers and security chiefs
- International outreach

1.4 Scope

This document provides transit agencies with a resource for considering and selecting security-oriented design approaches to protecting transit systems and minimizing the impacts of terrorist attacks. The document can be used by a transit agency to establish a comprehensive design strategy for hardening its assets or for selecting strategies or solutions that best meet the agencies' needs.

This document provides an overview of the major assets of transit systems—bus vehicles, rail vehicles, and transit infrastructure and communications—as well as a preliminary assessment of the vulnerabilities to various methods of attack inherent in each asset. In addition, this document addresses the topics of access management, systems integration, and communications—all crucial to the protection of transit assets. Although many of the subject areas are addressed discretely in the document, agencies should recognize the interconnectivity of the design considerations and hardening strategies presented. For example, the sections on both infrastructure and access management will provide additional value when developing a strategy for protecting and hardening a maintenance facility or a rail terminal.

Transit Security Components

Assets to Protect:

- Infrastructure
- Bus Vehicles
- Rail Vehicles
- Communications

Protection Solutions:

- Access Management
- Systems Integration
- Communications
- Design Considerations

This document offers an initial assessment of the vulnerabilities common to diverse public transit systems, along with descriptions of the types of attack a public transit system might experience and their consequences. Using that measure, it offers guidance for public transit systems to modify both the design of their physical assets and the framework of their security procedures. And based on the

[4] http://transit-safety.volpe.dot.gov/Security/Default.asp, January 3, 2003.

[5] Public Transportation Security Volume 1: Communication of Threats: A Guide. Transportation Cooperative Research Program Report 86 (2002); Public Transportation Security Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers. Transportation Cooperative Research Program Report 86 (2002).

recent history of transit-oriented attacks, it provides some insight about the trends in terrorism against public transit.

With the involvement of industry and technical experts, FTA developed practical, feasible, and useable security design considerations that focus on the physical protection of a transit system's assets. Recognizing that the core mission of public transit is to equitably, efficiently, and safely serve the public, the emphasis is on methods for protecting transit assets that simultaneously protect the public and their access to transit.

1.5 Audience

This document is intended to provide information and ideas on security-oriented design modifications to transit executives, to transit senior managers, members of transit design and construction departments, operations departments, and security and law enforcement personnel. It includes general information that is intended to raise the awareness of senior staff to the importance of physical design in matters of security, and also contains some technical guidance for use by transit staff members with expertise in procurement, vehicle design, and infrastructure design. This document should be distributed to appropriate administration, engineering, and operations personnel-keeping in mind the potentially sensitive nature of the material. The document may also be of interest to project management oversight teams, consultants, contractors, and others working with public transit agencies.

1.6 Methodology

The first step in developing these transit security design considerations was to create a baseline of the vehicles most frequently used by the industry, and to determine the infrastructure components most commonly found at transit agencies. The baseline also included a review of transit system assets, threats to the system (including a review of acts of terror against transit world-wide), and the scenarios under which these assets and threats have or could come together in the form of a terrorist attack.

The next step was to review the threat and vulnerability assessments (TVAs) completed during 2001 and 2002 of the country's 36 largest transit properties.[6] These TVAs, which followed the methodology outlined in the Transit Cooperative Research Program (TCRP) report *Public Transportation System Security and Emergency Preparedness Planning Guide*, provided important insight into what the most critical threats and assets are for transit agencies. This review was followed by

[6] FTA commissioned Booz Allen Hamilton to conduct threat and vulnerability assessments on the nation's 36 largest transit agencies. This work was commissioned for use by the particular transit agency and contains information that is sensitive to each agency. Consequently, only generalized information was made available for preparing this report.

extensive meetings with working groups of industry professionals and representatives, to discuss the needs, problems, and solutions of various transit operators, manufacturers, and researchers.

1.7 Organization

This document consists of nine chapters and seven appendices.

Chapter 2: A Systems Approach to Security Design defines the concept of integration in a way that may help practitioners think about their security systems in a new way. Achieving integration is as much a conceptual challenge as a logistical challenge.

Chapter 3: Security in the Transit Environment presents the context for the treatment of security in public transportation systems today. This chapter briefly describes how security priorities have changed in recent years, and the domestic and international events that have impacted these changes. It also provides an overview of known threats to transit systems, as well as various countermeasures that have been effective at reducing some or all impacts of these threats or of the risk of the threat itself.

Chapter 4: Developing a Security Strategy presents the steps that should be followed if an agency chooses to embrace the approach offered in this document. It describes the steps involved in determining the strategy that an agency settles on, and offers a context for making this determination while considering the cost, efficiency, and effectiveness of these decisions.

The document then discusses each major component group within a transit system in its own chapter: *Access Management* (*Chapter 5*), *Infrastructure* (*Chapter 6*), *Vehicles* (*Chapter 7*), and *Communications* (*Chapter 8*). Each chapter describes the major characteristics of the highlighted component and offers design considerations that a transit agency might adopt when embarking on a comprehensive security program. They describe the threats specific to the highlighted component in each chapter, as well as the impacts that might be incurred if threats are realized. The guidance offered explains how design can reduce known security risks or their impacts and how decisions might affect other functions of a transit system and/or other components of a system.

Chapter 9: Security Systems Integration offers specific tools and guidelines for integrating the major components of a transit system. This chapter proceeds as though one has embraced the concepts presented in *Chapter 2: A Systems Approach to Security*, and describes the steps involved in developing and implementing the strategy adopted as a result of the considerations offered in *Chapter 4: Developing a Security Strategy.*

Appendices include a chronology of terrorist attacks against public transit, case studies of transit security initiatives, performance measures, vehicle barrier selection and implementation, vehicle barrier types; codes, standards, and regulations; fire safety recommendations, lessons learned from transit communications emergencies, and a list of transit industry working groups, references, and acronyms.

1.8 Navigating this document

Sections of this document will be more or less relevant to readers during different phases of a security program or of asset procurement, and readers may need to consult several sections as they make decisions. The document, therefore, contains hyperlinked text where additional information can be found on concepts or processes. If concepts are closely related and contained within the chapter they are marked in **<u>bold, blue underlined</u>** text. Where concepts are broader or more extensive, they are marked with the following graphic:

➡ ***concept overview*** - refer to Section **<u>x.x.x</u>**

This page left intentionally blank

2.0 A Systems Approach to Security Design: Adopting an Inclusive View

These security design considerations are based on a "systems approach" that encompasses all of the aspects of an organization—the people, the processes, the equipment, and the technology. Although this document offers security design strategies for each of the major elements of a transit system—access management, communications, infrastructure, and vehicles—it does so in the context of interdependence, in which each element is to be understood as one piece of a much larger whole. It is this interdependence that makes the protection of a transit system complex and challenging, as the entire system needs to be considered and secured simultaneously. An inclusive view also recognizes that public transit systems are linked to other elements of the transportation network not only physically, but also through an intricate network of technology, law, and regulation.

This chapter discusses:

- The importance of a systems approach
- Designing integration into a security system
- Moving toward security system integration

2.1 The Importance of a Systems Approach

In organizations of any kind, the incentives to build or maintain "stovepipe systems"—individual systems that operate independently of each other—are great. These include limited budgets, protection of organizational turf, staff with focused technical expertise, and the sheer difficulty of implementing an integrated system. With regard to transit security system design, the dangers of stovepipe systems are clear. To individually protect a vehicle, subway platform, computer system, or maintenance facility is not enough—a hazard placed in any of these locations could be unwittingly carried throughout the system by the standard operations of the agency, thereby turning the rapid, mobile, and open nature of public transit against itself.

A more effective level of security is possible when all aspects of the organization can work together, and timely information critical to deterring, preventing, or responding to a security event is available systemwide. When staff at all levels within the organization understand the need for connectivity among its physical, technical, procedural, legal and institutional elements, they are more able to deliver safe, accessible service to the public. A systems approach also contributes to transit security by bringing together the various parties that must design a security strategy, implement the security plan, and respond to an attack or threat.

2.2 Designing Integration Into a Security System

A transit security system encompasses all physical and logical components that contribute to the safety and protection of a transit system's sites and assets, and may include physical barriers, staff credentials, electronic devices, software applications, data management, telecommunications equipment, and security personnel. It also interfaces with other systems, such as facilities management, personnel management, and emergency services communications systems. A systems approach brings a synergistic and inclusive view to planning and implementing a transit security system, taking into account all components.[7] Transit system managers can use this holistic perspective to design a security system that more effectively:

- Integrates security devices into a coherent whole
- Integrates security devices into the transit system
- Integrates security and non-security functions
- Interfaces with non-transit agencies, e.g., emergency services, traffic management

Increasing physical security is a long-term process, as most transit agencies are constrained by fiscal realities from replacing functional vehicles or redesigning usable stations solely to integrate new security considerations. The implementation of a security strategy can be incorporated into the operation of transit agencies in stages, with simple or critical changes being made immediately and long-term modifications incorporated over time. The process is also continuous and iterative, so that refinements and adjustments are constantly made to keep up with innovations and the changing times.

2.3 Moving Toward Security Systems Integration

The systems approach to design and implementation leads to a higher degree of systems integration, which is discussed at length in *Chapter 9: Security Systems Integration.* Security systems integration implies that all types of systems and their subsystems are linked together. It applies to how the security system's components work together as a whole, as well as to how the security system communicates with other systems having related transit functions. Achieving systems integration is as much a conceptual challenge as a logistical challenge. Note that integration can be present in degrees and can be implemented as part of a phased system-development process.

Chapter 9: Security Systems Integration further describes "system" in the context of the transit security system, discusses systems integration as an outcome of the system development process, and defines a methodology for agencies to meet the challenge of building integration into systems design.

[7] FHWA, Chapter 16, "Regional Integration*," Freeway Management and Operations Handbook*, (Publication Number FHWA-OP-04-003) http://ops.fhwa.dot.gov/Travel/traffic/freeway_management.htm.

3.0 Security in the Transit Environment

Transit agencies share a common mission: to provide convenient, affordable transportation that is open, accessible, and available to all. Hundreds of thousands of people pass through bus stops and subway stations in America every hour, embodying the promise of the transit industry to equitably provide safe and reliable public transportation. Public transit systems cannot be closed off or tightly controlled like an airport without compromising their fundamental character. Security must be created in other ways, through physical modifications that don't impinge on the openness of the system (including accessibility as required under the American with Disabilities Act), through employee training and watchfulness, through passenger awareness and participation, and through careful planning for coordinated, efficient, and life-saving response.

Several recent trends highlight the dynamic nature of the transit industry and demonstrate the need for a security-oriented infrastructure. For instance, light rail is increasingly common in the United States, and more and more metropolitan areas are exploring the possibility of introducing bus rapid transit (BRT). These modes introduce new security concerns and needs that are different from the needs of traditional subway and bus systems. Both light rail and BRT operate above ground, making them vulnerable to close-range attack. Vehicles generally come equipped with large windows and doors, making them easily penetrable and open to attack from the outside. In addition, the increase in construction of light rail and BRT infrastructure means that more transit systems will be managing multiple vehicle modes, as systems expand into new neighborhoods and new lines of service with new types of vehicles. This gradual evolution adds to the complexity of protecting public transit assets, but also makes it possible for transit systems to include security considerations in their technical specifications for new vehicles. In some cases, this can be an efficient way to introduce security infrastructure, where retrofitting existing infrastructure can be difficult and costly.

This chapter describes:

- Challenges to transit system security
- Threats and countermeasures

3.1 Challenges

The core challenge of addressing the vulnerabilities of a transit system is the degree of openness fundamental to public transit. Public transit agencies operate systems in which public access is crucial not only to daily operations but also to the fulfillment of the agency's mission, but it is difficult to secure and protect any area to which the public is allowed open access. Public transit infrastructure consists of a series of layered spaces, each increasingly closed to the public. The public areas of transit systems have complete and unchecked access, but other facilities are open only to agency employees, contractors, and vendors. In the new security paradigm, efforts must be made to use the technologies of credentialing and access control to ensure that the sensitive areas of systems are accessible only by those permitted to be there.

The high passenger volumes experienced by many transit agencies can add to a transit agency's security concerns. The high concentrations of people in contained spaces—whether it be a full bus crowded with standees, or a downtown subway platform at rush hour—make transit facilities inviting targets and provide another significant challenge for agencies to address. Transit systems must accommodate thousands of daily customers, sometimes 24 hours a day / 7 days a week in many of their facilities. Customers using transit systems may circulate near restricted areas such as tunnels, control rooms, utility rooms, power supplies, or hazardous-material storage areas.

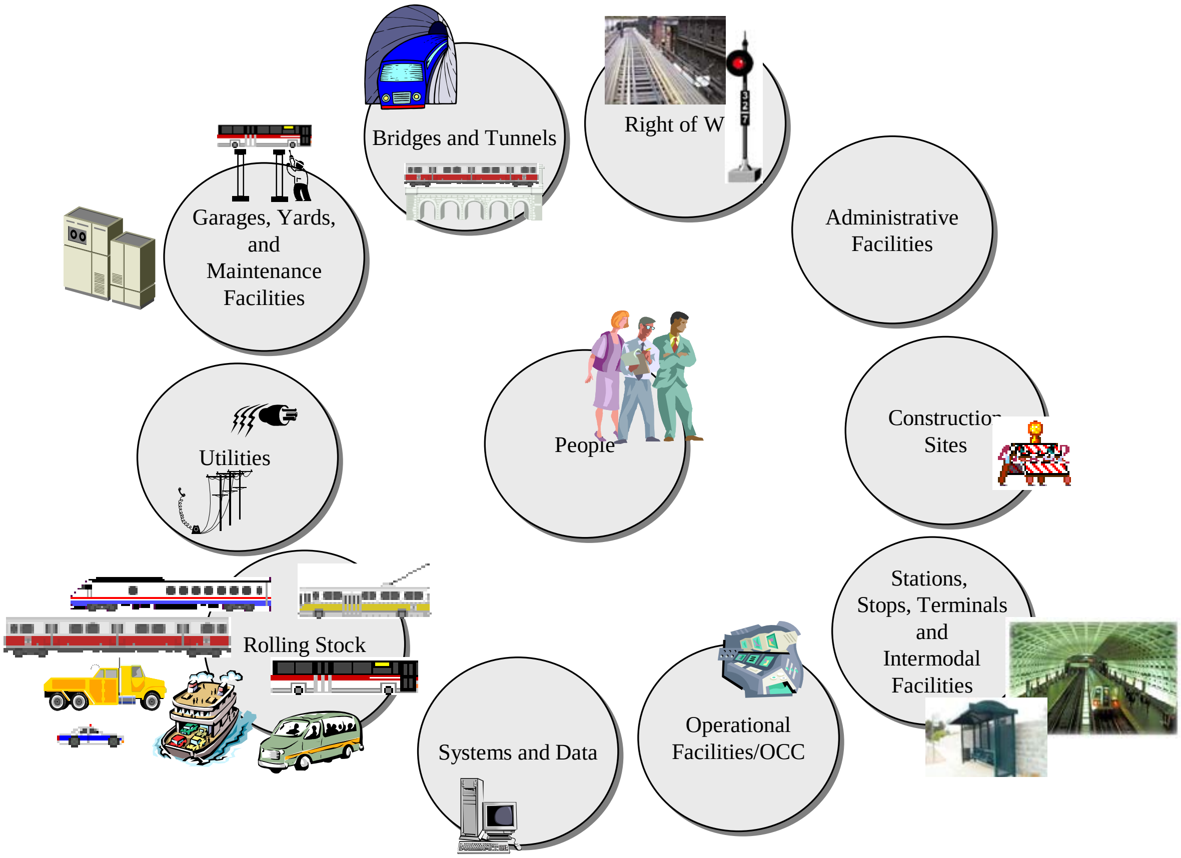

Bridges and Tunnels
Right of W
Garages, Yards, and Maintenance Facilities
Administrative Facilities
People
Utilities
Constructio Sites
Rolling Stock
Stations, Stops, Terminals and Intermodal Facilities
Systems and Data
Operational Facilities/OCC

Figure 3-1. Transit System Assets

Security systems and strategies for transit environments must work in a wide variety of settings and be effective in protecting diverse asset types (see Figure 3-1). Transit agencies are constantly faced with the challenge of managing risks to their assets. Each asset has its own level of risk based on its attractiveness as a target, vulnerabilities, accessibility, and criticality to the system. The process of evaluating risk and implementing countermeasures designed to protect specific assets requires that transit agency managers prioritize 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, security measures for each asset must be commensurate with the threats and vulnerabilities of that particular asset and the potential consequences of an attack or other disaster.

The increased awareness of the need for security within public transit systems has challenged some of the basic tenets of public transit and has highlighted competing visions of the future of public transit in America. For example, considerations of security could potentially prompt a rethinking of the use of alternative fuels, long promoted as preferable to diesel fuel for environmental and public health reasons. Concerns about security may also generate debate about the current trend toward multimodal transportation facilities, which improve the efficiency and convenience of the transit network but may also be particularly vulnerable to a devastating attack. The demand for security-oriented design may also generate renewed interest in building redundancy into the construction of new transit infrastructure, where feasible, so that agencies can maintain services after an attack or disaster. These examples highlight the ways in which the evolving emphasis on security will need to be balanced against other, long-standing policy priorities.

3.2 Threats and Countermeasures

In the weeks and months that followed September 11, 2001, most transit agencies examined how terrorists could attack their systems. They tried to identify their weakest points, and where an attack would cause the greatest loss to passengers, employees, rolling stock, and facilities. Agency staff, contractors, or the FTA conducted structured assessments. Based on these assessments, the types of security threats that a transit system could face were identified and are described in this section.

The diversity of assets that may be part of a transit system leads to a range of possible threats and countermeasures. Some assets might be targets for a terrorist attack intended to inflict civilian injuries; others might be means for providing misinformation to the public, others for crippling mobility or economic activity within a city or metropolitan area or even for obtaining sensitive information about the system. Transit systems or their components could also be affected indirectly by an attack elsewhere, which may compromise communications, operations, or maintenance capabilities. Results of attacks or incidents might include:

- Loss of life or physical injury to transit riders, staff, and/or passers-by
- Physical damage to transit agency equipment or infrastructure, and possibly to the surrounding environment
- Loss of power through direct attack or by external event
- Failures outside the transit agency that affect operations – service delivery or maintenance

- Excessive traffic on communications networks
- Breach of communications or operations network security/hacking

3.2.1 Threats

While the threat against transit targets is only now gaining broad recognition, transit systems and railways have long been considered viable targets by terrorists. Throughout the 1980s public transit systems were targeted by some terrorists with the intention of inflicting heavy casualties, while others employed more subtle tactics aimed at disrupting transit service. Threats may result in attacks aimed directly at the transit agency, or those aimed at the environment within which an agency operates.

3.2.1.1 Arson

The hazards of arson, an intentionally set fire, in a transit facility include the destruction of assets within the facility, structural damage to the facility itself, and injuries or fatalities due to direct exposure to fire or to smoke and fumes. In a major fire, ambient temperature can surpass 1,800°F (1,000°C), which may result in structural damage, as well as electrical and mechanical systems failure. Burning fuel, oil, plastics, and some paints can cause dense smoke and toxic fumes. Toxic fumes present a serious health threat and may cause death by asphyxiation. In addition, smoke can reduce visibility, obscuring exit pathways and making escape more difficult for victims. Since fires may occur accidentally as well as intentionally, there is crossover between protection against accidental fires and protection from arson. Arson and explosion-related fires, however, may cause more severe damage because they tend to target or cluster around critical systems and equipment.

3.2.1.2 Explosives

The hazards of an explosive blast include the destruction of assets within a facility, structural damage to the facility itself, and injuries or fatalities. In addition, explosions may start a fire, which may inflict additional material damage, injuries, or fatalities due to direct exposure or to heat, smoke, and fumes. An explosion is an instantaneous or almost instantaneous chemical reaction resulting in a rapid release of energy. The energy is usually released as rapidly expanding gases and heat, which may be in the form of a fireball. The expanding gases compress the surrounding air creating a shock wave or pressure wave. The pressure wave can cause structural damage to the structure while the fireball may ignite other building materials leading to a larger fire. The strength of a blast depends on the type and amount of explosive material used. A bomb that a person can carry is capable of a smaller blast than an explosive-laden truck.

3.2.1.3 Weapons of Mass Destruction

Weapons of mass destruction (WMD) typically refer to nuclear, radiological, chemical, and biological weapons capable of inflicting mass casualties. WMD can also refer to radioactive materials and other contaminants intended to quickly harm large numbers of people, such as any powders, liquids, gases, and dirty bombs; most of these come in a liquid, vapor, gas, or powder form, and are spread through air movement.

The hazards of WMD include fatalities or deleterious health effects, as well as potentially permanent contamination of a facility that may render it unusable. Many agents have little or no plainly discernable characteristics, so symptoms may be the first sign that an attack has occurred. While some chemical agents induce immediate symptoms, other agents will not produce symptoms for hours after the attack. Some biological agents may have an incubation period of up to a few days before symptoms appear.

3.2.1.4 Violent Incidents and Hostage Situations

Violent confrontations by terrorists are common on transit systems throughout the world. These include assaults carried out on board transit vehicles or at transit facilities, with the intent of inflicting casualties, property damage, or both. Violent incidents may include the taking of hostages. Transit vehicles are especially vulnerable to hostage situations because of easy public access, remoteness of the vehicle, and available civilians onboard. Such attacks are meant to create widespread fear and apprehension through public displays of violence and the interruption of public services. Attackers may use a variety of weapons, including small arms, assault rifles, shoulder-mounted rocket-propelled grenades, knives or other bladed weapons, and small explosives.

3.2.1.5 Tampering

Tampering with transit facilities' assets may be a means to achieve any of the above events, such as starting a fire or spreading an airborne chemical agent, or it may be a stand-alone act, such as tampering with track to induce derailment. It can also include the intentional ramming of a facility, with a truck, boat, or airplane, in order to cause structural damage to a facility or injury to its users. The ramming vehicle may be laden with explosives. Depending on the situation, tampering may lead to asset damage, structural damage, contamination, injuries, and/or fatalities.

3.2.1.6 Loss of Power

Loss of electrical power, either locally or over a broad area, can pose a major problem for transit systems in the form of diminished or suspended operations control, computer-aided dispatch, and radio systems. Loss of electricity could be the result of an intentional attack or unintentional event—either within the agency or in the surrounding environment—but in any case could hinder a transit agency's ability to operate or communicate effectively. Apart from service impairment, loss of power may even inadvertently result in damage to property or persons within the agency, service area or in the vicinity.

3.2.1.7 Transit Vehicle as a Weapon

Transit vehicles should be viewed not only as targets, but as weapons as well. There can be a wide range of nefarious uses for both operational and retired vehicles. Perpetrators might attempt to hijack an operational vehicle in order to steer it into a building or bridge, or may plant explosives in the vehicle while in the storage yard in hopes of detonating it at a later time. They might also seek to steal or purchase a retired vehicle, counting on the innocuous nature of a public transit vehicle to set people at ease while they carry out various terrorist activities. Attacks might be directed at the vehicle itself, at the transit system, or at the surrounding environment.

3.2.1.8 Network Failure/Cyber Attack

Transit systems rely on computerized networks to facilitate operations and enhance efficient service delivery, which makes them vulnerable to network failure and cyber attacks. While this document does not offer specific considerations on how to protect computer networks, it is crucial to understand their importance to operating and communicating among agency staff as well as with partner organizations and the public-at-large. Network failure may be caused by faulty or damaged internal components, direct cyber attack to the agency's network, direct attack to a peripheral system or network, or even a blanket computer virus. The result may be loss of communications or operations capabilities as well as misinformation by hacking into a Web site or server.

3.2.1.9 Perpetrators

Transit systems are susceptible to attack by perpetrators hoping to destroy transit property or city environments, to inflict mass casualties, or simply create a nuisance through misinformation or disrupted service. Agencies should attempt to protect themselves against the lone terrorist carrying a bomb or container of sarin gas in a backpack, as well as the cadre of terrorists coordinating to hijack a transit vehicle for more nefarious purposes. Perpetrators may be highly knowledgeable about transit operations generally or at a specific agency (they may even originate within the agency) or they may be ignorant of system operations altogether. Transit agencies or authorities hoping to be successful at providing a high level of security should consider combinations of countermeasures that would address the range of perpetrators attempting to impose a range of threats on the agency or its operating environment.

3.2.2 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 (1) deter attackers from attempting an attack; (2) detect potential threats promptly; (3) minimize the impact from an attack; and (4) 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. Every transit agency faces a particular set of circumstances and needs; no single security strategy is appropriate for every agency. Each agency should consider its operations, infrastructure and communications needs, threat assessments, budget, and existing systems to determine which combinations of countermeasures best fit its circumstances.

3.2.2.1 Deter

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.

Access Management

Controlling who (or what) may access restricted areas and assets in the system plays an important role in protecting transit infrastructure from all of the major threats identified in this section. 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.[8]

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 blindspots resulting from overlapping or peripheral areas.

3.2.2.2 Detect

Weapons Detectors and Screeners

Weapons detectors and screeners can be used to detect the presence of both tangible weapons, such as traditional or radiological explosives, and to identify more intangible ones, such as damaging chemicals. Metal detectors can be used in administrative or operations centers or sensors placed in areas of a station to gauge levels of a particular gas and/or agency staff can be charged with randomly screening the bags of transit riders in search of nefarious items. Weapons detectors can help in both preventing attacks and capturing the perpetrator(s).

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.

Site/building Layout

The physical characteristics of a site have affected the selection of security measures for safeguarding a facility. Some of these characteristics, such as building location, landscaping, and site circulation

[8] See "Access Management Guidelines for Transit" (FTA/DOT) for more information.

are under the control of the transit agency; off-site features such as topography and abutting uses, are not. Some on-site characteristics such as topography and vegetation are under limited control of the transit agency. Proper placement and orientation of buildings and other structures on the site is a major component of an effective security strategy to protect against damage from terrorist attacks. Three fundamental considerations are unobstructed space, standoff distances, and building orientation.

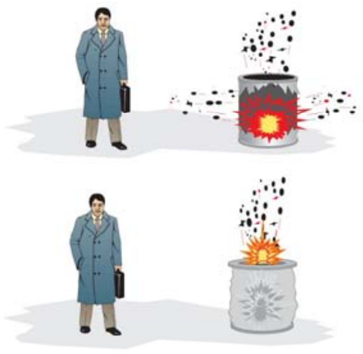


Figure 3-2. Redirection of blast force

Trash bins designed to force a blast upwards may help protect nearby people and property.

3.2.2.3 Minimize

Facility Hardening/Resiliency

Although prevention is the best strategy, minimizing potential damage in case of an event is also important, as no system can be made 100-percent foolproof. Strategies that harden a facility are those that nullify or minimize the effects of an attack when it occurs. Examples include blast-resistant structural engineering that enables a building to remain standing after a blast, and the use of non-flammable materials that hinders the spread of fire. These efforts may serve to protect both the infrastructure itself and the safety of its users.

Standoff Distances

Since the effective quantity of explosives and distance from the target are the most important factors in determining the destructive effect of an explosion, standoff distances, especially for larger vehicles, are an essential technique for minimizing the risk of damage to a target from a blast. Potentially explosive-laden vehicles should be kept as far away from would-be targets as possible. Standoff distances also diminish the risk of intentional ramming, and help create a safety zone that visibly exposes any transgressors and enhances surveillance.

Redirection of Blast Force

The impact of an attack can be mitigated by implementing methods of redirecting potentially harmful forces in a direction that will cause less damage or injury, should a blast occur. Assets that are specifically risky can be designed to “blow” away from individuals. For example, trash bins can be built to direct a blast detonated from within upwards rather than outwards (see Figure 3-2). Proper design strategies also avoid creating spaces that will concentrate or “throttle” the force from a blast, such as alleyways, overhangs, or other enclosed spaces.

Redundancy and Dispersion of Assets

All essential systems, such as vehicle monitoring and control, electricity, and fire suppression, should be safeguarded with redundant systems in case of damage or destruction of the primary system.

Whenever possible, these duplicate systems should be located at different sites or at different places within the same facility. In addition, key assets and personnel at a single facility should be dispersed throughout the site, so they cannot be disabled by a single attack. Though this might conflict with desires for a unified approach operating from a unified center, loss of multiple coordinating personnel can seriously hinder an agency's ability to effectively manage an emergency situation and/or recover from its effects.

3.2.2.4 Respond and Recover

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.

Decontamination Awareness/Materials Selection

Recovery from a chemical or biochemical attack can be difficult. Certain types of materials may speed up the decontamination process or reduce the lingering effects of the agent used in the attack. For example, materials that are porous, such as vehicle carpeting or mesh-screened walls in stations, are more difficult to sanitize and can trap chemical agents within the material. This may prolong the decontamination process or force removal of the material altogether. Agencies may choose to minimize or restrict use of construction materials and components that are less susceptible to decontamination in the event of a chemical, biological, or radiological incident, or perhaps minimize their usage in certain areas. Agencies may also consider educating staff and designer/engineer on decontamination processes and chemicals in order to minimize the post-incident cleanup time and possibly the impacts.

4.0 Developing a 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 an iterative process that involves initial assessment, planning, implementation, and constant evaluation.

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

A transit agency may develop a security strategy proactively to meet the predefined requirements of its security plan, or reactively to address a particular security breach or deficiency.

How is this chapter useful?

For **transit managers** and **security staff** it is a resource for:

- Evaluating or updating an existing security strategy
- Weighing cost and efficiency in the decision-making process
- Understanding the process behind developing a security strategy

This chapter describes design considerations for transit agencies as they navigate the process of developing and implementing a transit security strategy, including the implementation of security countermeasures.

4.1 Basis for Security Strategy

Agencies should consider preparing and implementing security strategies that are consistent with its comprehensive security plan and its threat and vulnerability assessment (TVA). The TVA can be used to help determine implementation priorities.

For guidance on preparing a security plan, refer to *The Public Transportation System Security and Emergency Preparedness Planning Guide* [FTA, 2003].

Transit agency managers 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, agencies 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.

Although there is no prescriptive approach to developing a security strategy, agencies may consider the following four phase, iterative approach:

- Consider options
- Evaluate and select countermeasures
- Develop implementation approach for countermeasures
- Implement strategy

The Basis for a Security Strategy

A **comprehensive security plan** is an overall approach for mitigating potential threats and vulnerabilities throughout the system.

A **threat and vulnerability assessment (TVA)** identifies the sources and types of threats and the vulnerabilities within a transit agency's system. A TVA helps decision makers evaluate risks, identify priorities, and select solutions.

Designing security into the system is easier and cheaper than patching it on later – security managers should be involved in the planning for all new construction and retrofit projects

4.2 Phase 1 – Consider Options

This begins with a consideration of the agency's overall security goals (as defined in its comprehensive security plan), and understanding the extent they are being met. If the agency's security goals are not being met, the agency must determine what options along with countermeasures should be considered for adding additional levels of security. Security goals might range from the specific, such as hardening critical assets, to the general, such as diversifying redundancy.

Identifying countermeasures requires an agency to:

- 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

4.2.1 Determine Level of Protection

Having assessed the problem, agencies should next consider the level of protection required for each of its assets, matching the level of protection with the level of threat. Factors that agencies may 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 4-1 is a simplified diagram depicting the degree of countermeasures as they correspond to various levels of threat.

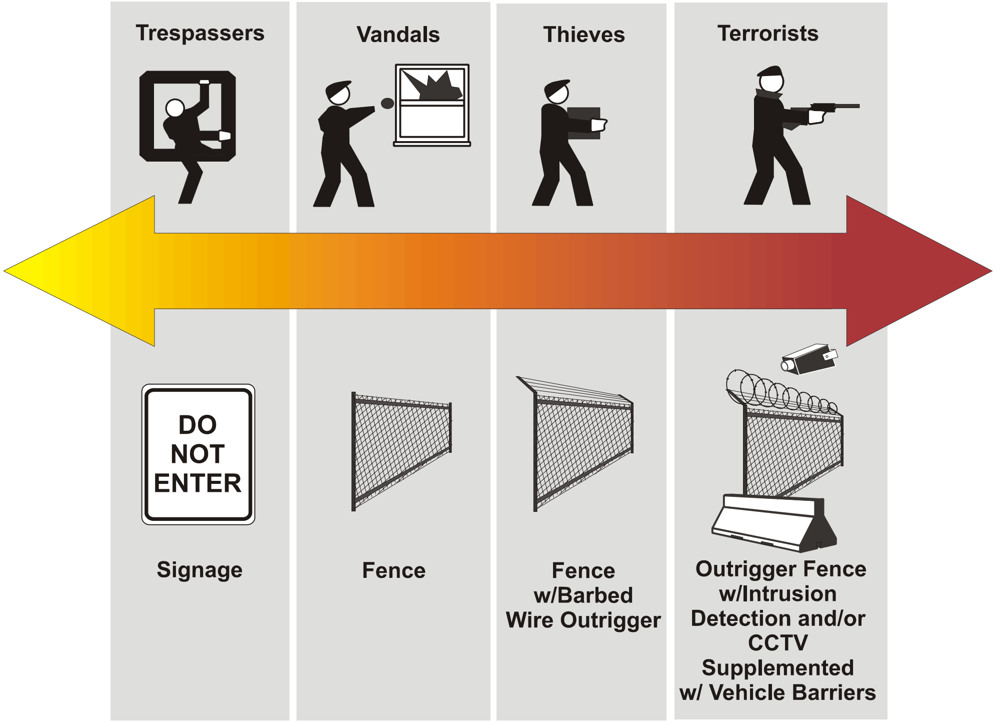

Trespassers
Vandals
Thieves
Terrorists
DO NOT ENTER
Signage
Fence
Fence w/Barbed Wire Outrigger
Outrigger Fence w/Intrusion Detection and/or CCTV Supplemented w/ Vehicle Barriers

Figure 4-1. Corresponding Threats to Level of Protection

4.2.2 Establish Functional Requirements

Based on the required level of protection and classifications, agencies should consider establishing the functional requirements for the security strategy. These are typically documented in the form of performance requirements but can also be driven by established security standards.

To supplement these transit security considerations, agencies may evaluate and adapt existing security standards and guidelines from other transit agencies, as well as other transportation and non-transportation sources. Examples of such sources (note, these are access management examples) include:

- Department of Health and Human Services (NIOSH) Publication No. 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, Radiological Attacks* [9]
- ISO and IEC wireless technology standards for identification cards 14443[10] and 15693[11]
- *Department of State Vehicle Barrier Guidelines*[12]

[9] http://www.cdc.gov/niosh/bldvent/2002-139.html

[10] http://www.wg8.de/sd1.html#14443

[11] http://www.wg8.de/sd1.html#15693

[12] See Department of State (DOS) standard, SD-STD-02.01 Revision A, Specification For Vehicle Crash Test of Perimeter Barriers and Gates, dated March 2003 (latest revision) or 12 FAH 5, Foreign Affairs Handbook for more.

- General Services Administration (GSA) Smart Card Interoperability Specification[13]
- *TSA Credentialing Guidelines*[14]
- FEMA risk management guidelines for potential terrorist attacks against building (FEMA 426[15]) and commercial building design (FEMA 427[16])
- Illuminating Engineering Society of North America (IESNA) standards[17]

Agencies should consider these standards and guidelines as starting points for developing security system performance requirements. Any security program adopted should be tailored to the needs of the particular organization.

4.2.3 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. Agencies should consider measures that are feasible, that address the identified problems, and that work within the existing security framework. Agencies should keep in mind that many countermeasures exist, and that a complete feasibility assessment of all alternatives can generate solutions that best fit that agency's 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 or vehicle control systems. It is likely that different parts of a single agency will have different needs, so the agency might rely on a combination of countermeasures to address multiple and conflicting requirements.

4.3 Phase 2 - Evaluate Countermeasures

Agencies should consider the following factors when selecting and evaluating countermeasures: performance characteristics, proven track record in a transit environment, future agency needs, families of technologies, and cost efficiencies.

4.3.1 Performance Characteristics

Security systems need to have a high degree of reliability. Agencies should consider evaluating established performance criteria, such as probability of detection, false alarm rates, and vulnerability to defeat. Agencies may also consider evaluating the potential for the selected technology to introduce new vulnerabilities into the system. Potential vulnerabilities may be inherent in a system,

[13] http://csrc.nist.gov/publications/nistir/nistir-6887.pdf
[14] See http://www.tsa.gov/public/display?theme=68 for information.
[15] http://www.fema.gov/fima/rmsp426.shtm
[16] http://www.fema.gov/fima/rmsp427.shtm
[17] https://www.iesna.org/shop/

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.

System characteristics, such as resistance of a component to compromise or counterfeiting, can be weighed against the criticality of the asset being protected and the perceived threat level. No system can be made completely secure; knowing the accompanying vulnerabilities is key to providing sensible protection with acceptable risks.

4.3.2 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)

Agencies should consider factoring in the experiences of peer agencies and other security users when selecting equipment. Appendix B presents case studies of effective practices for security initiatives at three large U.S. transit agencies and a federal government (non-transit) agency.

4.3.3 Future Agency Needs

The countermeasures selected should meet the agency's current requirements and be consistent with the long-range goals of the agency's comprehensive security plan and strategy.

When selecting security solutions, agencies should consider future needs and 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

4.3.4 Families of Technologies

When selecting specific countermeasures, agencies should make themselves aware of the wide array of available options, which may have variations designed for different purposes or locations. Agencies should consider analyzing these technology differences within a single family to determine which variation best meets its particular needs. As an example, Figure 4-2 illustrates families of technologies for exterior sensors. Detailed advantages and disadvantages for many of these types of sensors are described in the *TCRP Intrusion Detection for Public Transportation Facilities Handbook*.[18]

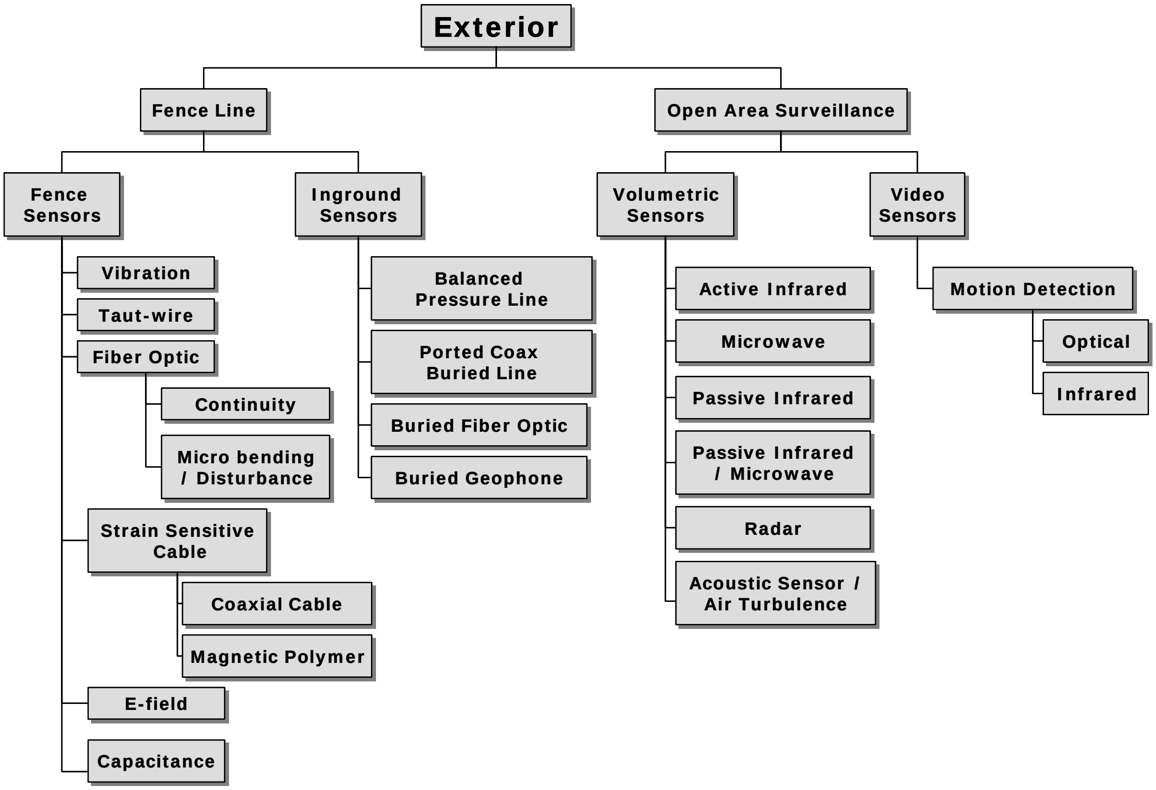


Figure 4-2. Example of Families of Technologies for Exterior Sensors

4.3.5 Evaluate Cost Efficiency

Security is one of many transit system goals competing with operations, maintenance, and other departments for limited financial, staff, and material resources. It can be difficult to obtain adequate funding for security initiatives, since security is often viewed as a cost factor with no real return on investment for the enterprise. Agency security proponents can counter this view by identifying and

[18] *Intrusion Detection for Public Transportation Facilities Handbook*, Transit Cooperative Research Program (TCRP). March 2003.

championing the potential benefits of implementing a security system. This involves assessing the negative effects of a security breach and the associated costs.

Agencies should consider security costs that are in proportion to the value or criticality of the protected asset and the level of risk. In evaluating countermeasures, agencies should consider their costs, benefits, and effectiveness, and should invest funds and other resources accordingly.

The relative costs and benefits of different security components can be challenging to quantify. Agencies should consider the following security system lifecycle ownership and operation costs:

- Equipment and related component costs
- Acquisition and transportation of primary and related equipment
- Project management, including meetings and travel
- Permitting
- Professional architectural, engineering, and design fees
- Construction costs
- Site preparation/clearance
- Structural reinforcement as required to support the equipment
- Construction for environmental enclosures
- Rigging, electrical, HVAC
- Tie-in to existing systems
- Operational costs (labor, enrollment, data management, etc.)
- Operator training and certification; including required improvements in workforce skills
- Customization, integration, installation, testing
- Maintenance, monitoring, calibration/tuning and adjusting

The Cost of a Security Breach

- Injuries and fatalities
- Loss of revenue / ridership
- Loss of trust – customers, shareholders, employees, partners
- Loss of intellectual property
- Financial fraud
- Liability
- Negative publicity
- Life expectancy
- Service restoration
- Cleanup

Agencies should also consider the following direct and indirect benefits:

- Personnel efficiencies (particularly security personnel)
- Reduced liability
- Safety
- Terrorism prevention
- Crime prevention
- Criminal investigation and prosecution support
- Improved management control
- Operational advantages

If the available funding or resources are insufficient to implement a solution to address the existing threat/vulnerability, agencies should assess again which countermeasure or combination of countermeasures provide the solution that maximizes the amount of risk reduction within the project budget. Agency management should be made aware of any system vulnerabilities and take steps to manage or formally accept any residual risk.

4.4 Phase 3 – Develop Implementation Approach for Countermeasures

Once the agency identifies countermeasures they should assess and select an implementation approach.

4.4.1 Assess Implementation Approach

Agencies should consider assessing potential implementation approaches in terms of priorities, time, capital, resource constraints, and economies of scale. Implementation approaches may include:

- Targeting key problem areas first.
- Phasing in implementation (facility-by-facility approach; countermeasure-by-countermeasure approach).
- Developing a minimum level of security across the transit agency.
- Implementing stop-gap measures (temporary solutions leading to permanent solutions) starting with lower-cost options.
- Implementing incrementally (from an operations perspective, beginning with simpler technologies can give staff time to gain proficiency).

Agencies may find using an approach that uses pilot programs and operational tests can build support for a project, since early successes are documented and publicized, allowing a move toward wide-scale deployment after full management approval.

4.4.2 Select Implementation Approach

After analyzing security requirements and assessing the implementation options, agency management can then select an implementation approach, taking into account the following factors:

- The full life cycle cost of the solution(s) (it may be desirable to provide several solution options with a range of costs).
- The full costs of non-implementation (business interruption, recovery, liability, loss of ridership, publicity).

- Risks (risk must be communicated effectively - incident history / risk probability should be shown).
- Estimates of effectiveness (expected risk reduction).

Agencies should also consider evaluating both internal and external needs, resources, and constraints. Internal factors can include available capital, resources (staff availability, contract labor), time, political climate, mandates, policies, and competing projects and priorities. External factors can include privacy, safety, legal and regulatory issues, environmental concerns, and aesthetics.

4.5 Phase 4 - Implement Strategy

As with any other plan, agencies would do well to evaluate the effectiveness of countermeasures once they are implemented, to review vulnerabilities and strategies periodically, and to take corrective action where required in light of changing threats or additional information.

4.5.1 Implementation, Monitoring, Evaluation and Feedback

Having decided on which security countermeasures to implement, the next step is implementation, followed by an evaluation of how the countermeasures are performing. After the risks have been determined and the countermeasures have been chosen, agencies should continue to implement the security strategy by considering the procurement, training and evaluation methods necessary to support the plan. Such methods should reflect the cost, efficiency, and effectiveness decisions that were made previously, and should take advantage of the agency's local and regional partners.

Agencies should then adopt measures to evaluate the program, and the performance of the various components. Agencies should consider security systems from an operational and life-cycle perspective, reviewing then documenting new or modified security systems. Documentation can include approved schematics, wiring diagrams, drawings, and specifications, and logic analyses to ensure the systems work as intended and comply with specified requirements.

Agencies should consider regular maintenance, testing, and evaluation of security countermeasures at initial installation, whenever modifications, repairs, or maintenance that may affect the system is complete, and when programmable controllers (if applicable) have been reprogrammed, in accordance with agency guidelines and/or manufacturer instructions. Security breaches or incidents can be documented and analyzed.

4.5.1.1 Tracking Security Effectiveness

The current security environment at transit facilities is optimized by an on-going security process that establishes a continuous framework for linking strategic goals to tactical execution through performance measurement. Measuring effectiveness is a means of strengthening a security program.

Agencies should consider establishing an analytical framework for assessing the effectiveness of security programs and systems over time. One approach consists of:

- *Developing a performance plan* to help evaluate the current effectiveness and levels of improvement in the security program based on established performance measures. This describes in detail how to conduct reviews of management and security controls in administrative and programmatic processes and applications.
- *Establishing acceptable levels of performance* for particular facilities, organizations or particular systems, and incorporating them into the agency's security controls.
- *Performing random and scheduled reviews* of the efficiency and effectiveness of security processes.
- *Overseeing compliance* with security standards and approved programs through a combination of inspections, tests, interviews, and record reviews.
- *Measuring performance against standards* to ensure expected standards are met and to drive process improvements.
- *Building the capacity to gather and use performance information,* possibly by using a data collection and reporting system.
- *Developing security program performance reports* to measure and document the effectiveness of security initiatives.

Progress tracking is one of the most powerful benefits of implementing risk management as a closed-loop system. Agencies can use performance measures as tools to evaluate such security areas as management, legal, administrative, human resources, infrastructure and engineering. Appendix C lists typical performance measures by category, such as input, efficiency / effectiveness, adoption, outputs, extensiveness, quality, impact, and usefulness.

Security plans and strategies or their implementation may change:

- As awareness of threats and countermeasures grows
- As criticality of specific assets changes with the growth of the region
- As new technology becomes available
- As agencies' understanding of their operational and functional strengths and weakness grows

Measuring effectiveness can be challenging, since it is difficult to control what cannot be measured. Current security measurement efforts are often limited by data availability. Empirical data are difficult to obtain, uneven in quality, and not routinely collected or reported. It may take a major effort to define the data requirements and put processes in place to collect data. Agencies should consider developing a Performance Management Information System to collect performance data covering a wide variety of metrics, and use the data to identify and quantify performance indicators.

In addition to traditional methods for measuring and evaluating security, agencies should consider alternative methods such as security benchmarking studies. Benchmarking studies identify the industry best practices surrounding security issues that, when implemented, can improve overall operations and lead agencies to exceptional performance.

4.5.2 Take Corrective Action

Agencies should consider reviewing the results of monitoring, testing, and evaluation of new and existing security components either periodically or continuously, depending on the countermeasure. Results can be fed back into the risk management process for prioritization with other known vulnerabilities, and corrective actions taken as appropriate. For example, an agency may choose to update or upgrade various systems or subsystems, retrain a particular functional group of employees, reevaluate the vulnerability assessment, or reassess specific goals as part of restarting this process. Once implemented, the agency should consider updating the TVA to reflect the new measures.

This page left intentionally blank.

5.0 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.

This chapter provides:

- An overview of access management,
- **Tools and techniques** for transit agencies to use in developing an effective access management strategy, and
- **Sample guidelines** for various access management security measures to help transit facility operators manage risks to their facilities and other assets.

How is this chapter useful?

For **transit managers and security staff** it is a resource for:

- Integrating access management into transit security
- Listing sample access management guidelines
- Identifying tools and techniques for controlling access

Note that details on the design and strategies for access management systems are beyond the scope of this chapter. Refer to **Chapter 6: Infrastructure**, for a description of design-related security measures for stationary assets in a system, such as buildings, tunnels, wayside easement, and rail lines.

5.1 Overview

This section defines the parameters of access management, the challenges of incorporating access management into the transit environment, using access management as part of a planning strategy and security plan, the security concepts behind access management, and agency challenges when implementing access management systems.

5.1.1 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. Agencies grant access for various combinations of persons and assets, depending on the needs and restrictions established by each agency.

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

What is Access Management?

Policies, procedures, and physical components controlling passage in and out of facilities or areas, determining who belongs and who does not, and tracking movement in and out of controlled areas.

In developing an access management plan, agencies should consider identifying their assets and areas of their property/facilities that should be controlled. They can then make decisions about who will be given access to those assets and areas. From there, they can decide how different access management tools—such as intrusion detection and surveillance—can work together as a part of an integrated security system.

5.1.2 Challenges in the Transit Environment

The objectives of access management and the mission of transit agencies are not always compatible with each other. The purpose of access management is to control and limit access, while public transit requires unrestricted public access to much of the system. In addition, transit systems serve mobile populations and contain mobile assets that are difficult to monitor and to secure.

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.

Access Management and the Transit Environment

Access management controls and limits access to areas.

Public transit requires unrestricted public access to much of the system.

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 5-1.).

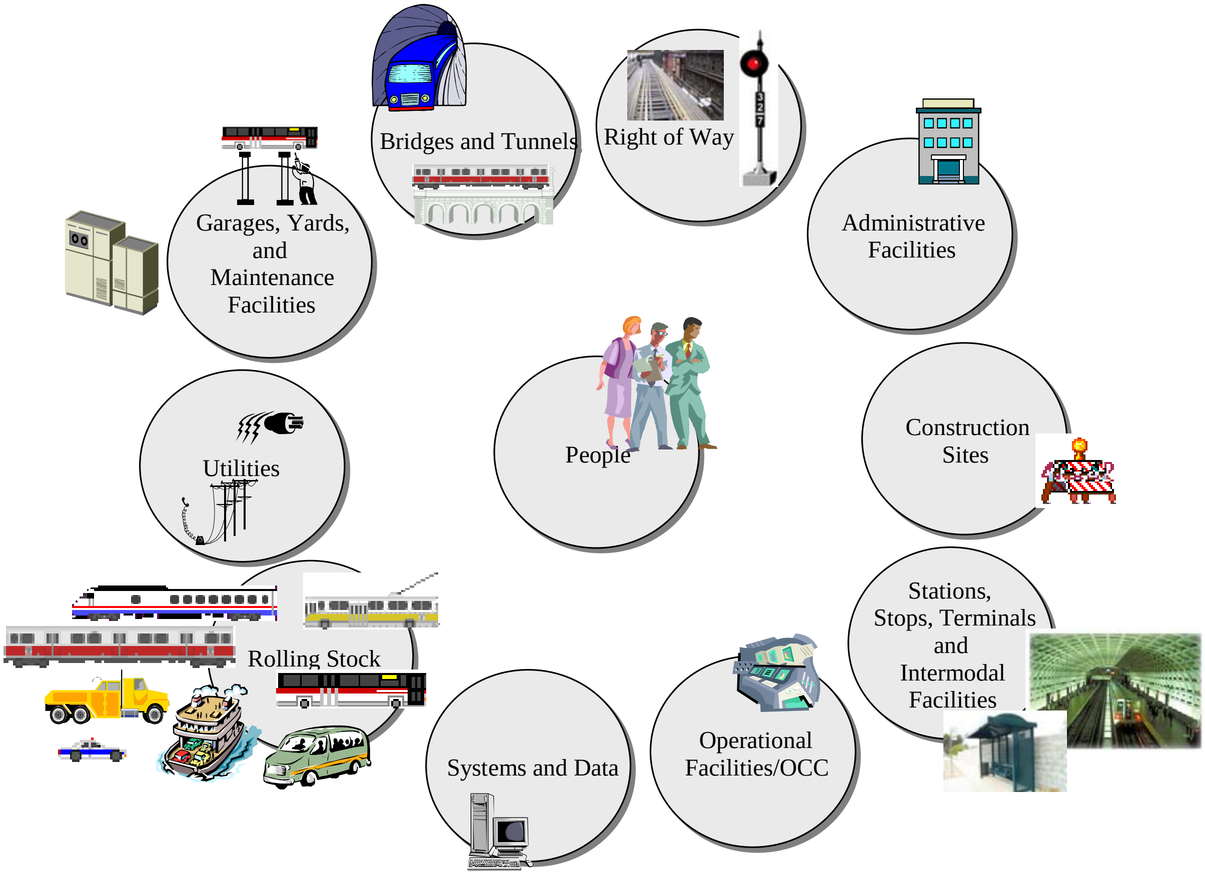

Bridges and Tunnels
Right of Way
327
Garages, Yards, and Maintenance Facilities
Administrative Facilities
People
Utilities
Construction Sites
Rolling Stock
Stations, Stops, Terminals and Intermodal Facilities
Systems and Data
Operational Facilities/OCC

Figure 5-1. Transit System Assets

Each asset has its own level of risk—attractiveness as a target, vulnerabilities, accessibility, and criticality to the system. However, transit agency managers 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, agents 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.

5.1.3 Access Management as Part of an Enterprise-wide Strategy

Access management—and security in general—is one concern within the broader operating environment of a transit agency. Agencies should consider balancing the desire for security against other objectives, such as operational efficiency, budgetary limitations, and passenger convenience. Access management strategies can be integrated into agency-wide planning efforts to ensure compatibility with other, non-security goals.

An agency's staff should consider ways in which access management systems can provide information that is useful to operational systems already in place. For example, agencies may integrate access management systems with a personnel system to track the presence of employees at restricted facilities. Security is the responsibility of all transit department staff; operational procedures and resources can be used to promote effective access management.

5.1.4 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.

Agencies should consider preparing and implementing access management strategies that are consistent with their comprehensive security plan. The TVA can be used to help determine which access management strategies to implement.

For guidance on preparing a security plan, refer to *The Public Transportation System Security and Emergency Preparedness Planning Guide*[19] [FTA, 2003].

5.1.5 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.

5.1.5.1 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.

[19] http://transit-safety.volpe.dot.gov/Publications/security/PlanningGuide.pdf.

To reduce the need for guards and technology, agencies should 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*.[20]

Transit Employee Security Awareness

Frontline transit employees are the eyes and ears of every transit system.

Bus and rail operators and maintenance employees, with the appropriate training, can be crucial in deterring, diffusing and responding to serious security incidents occurring on-board their vehicles and within transit stations or facilities.

FTA funds and supports a wide variety of safety and security training to transit agencies. Employee and public security awareness are two of FTA's focus areas. FTA-sponsored training is developed in collaboration with transit industry professionals, industry experts, and professional training institutes. One course example is the National Transit Institute's (NTI's) System Security Awareness for Transit Employees.

5.1.5.2 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. For more details on individual access management tools, refer to Section 5.2.

5.1.5.3 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. Individual surveillance components are discussed in Section 5.2.

5.1.5.4 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

[20] *Transit Security Handbook*, Federal Transit Administration, FTA-MA-90-9007-98-1, Volpe Center, Cambridge, MA. March 2, 1998. http://transit-safety.volpe.dot.gov/Publications/Default.asp.

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 5-2). 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.

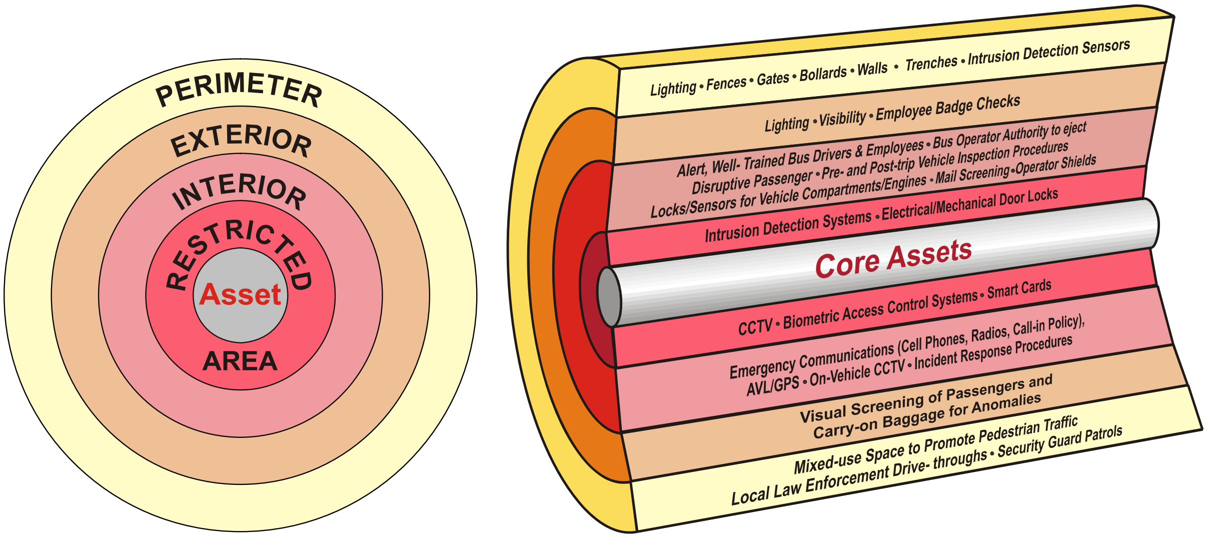

PERIMETER
EXTERIOR
INTERIOR
RESTRICTED AREA
Asset
Lighting • Fences • Gates • Bollards • Walls • Trenches • Intrusion Detection Sensors
Lighting • Visibility • Employee Badge Checks
Alert, Well- Trained Bus Drivers & Employees • Bus Operator Authority to eject Disruptive Passenger • Pre- and Post-trip Vehicle Inspection Procedures Locks/Sensors for Vehicle Compartments/Engines • Mail Screening • Operator Shields
Intrusion Detection Systems • Electrical/Mechanical Door Locks
Core Assets
CCTV • Biometric Access Control Systems • Smart Cards
Emergency Communications (Cell Phones, Radios, Call-in Policy), AVL/GPS • On-Vehicle CCTV • Incident Response Procedures
Visual Screening of Passengers and Carry-on Baggage for Anomalies
Mixed-use Space to Promote Pedestrian Traffic Local Law Enforcement Drive- throughs • Security Guard Patrols

Figure 5-2. Layers of Security

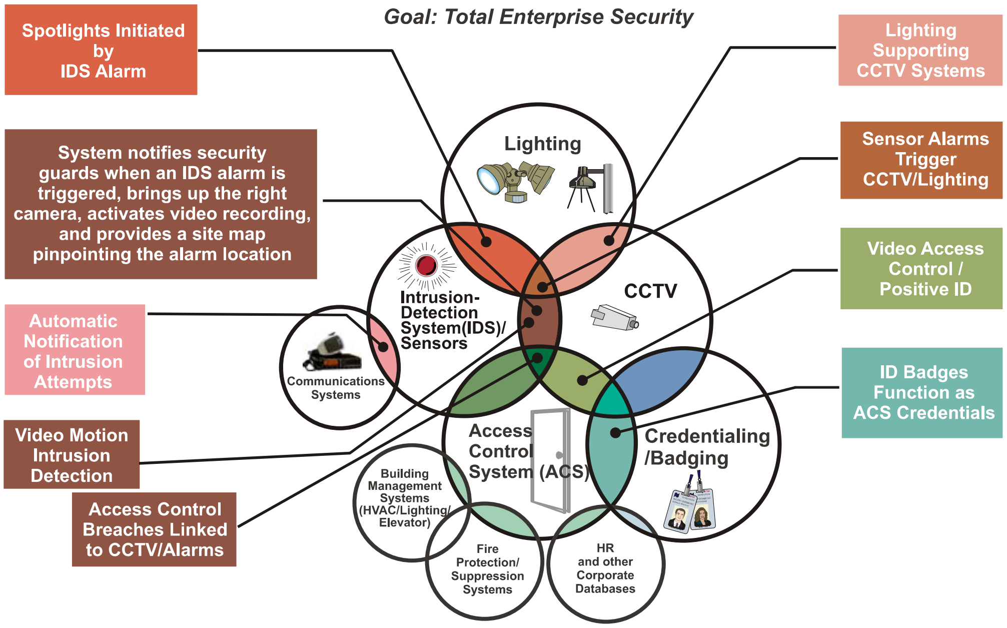

Goal: Total Enterprise Security
Spotlights Initiated by IDS Alarm
System notifies security guards when an IDS alarm is triggered, brings up the right camera, activates video recording, and provides a site map pinpointing the alarm location
Automatic Notification of Intrusion Attempts
Video Motion Intrusion Detection
Access Control Breaches Linked to CCTV/Alarms
Lighting Supporting CCTV Systems
Sensor Alarms Trigger CCTV/Lighting
Video Access Control / Positive ID
ID Badges Function as ACS Credentials
Lighting
Intrusion-Detection System(IDS)/ Sensors
CCTV
Communications Systems
Access Control System (ACS)
Credentialing /Badging
Building Management Systems (HVAC/Lighting/ Elevator)
Fire Protection/ Suppression Systems
HR and other Corporate Databases

Figure 5-3. Access Management Component Integration

5.1.5.5 Systems Integration

Integrated access management systems allow transit agencies 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 5-3 shows potential integration opportunities for access management components. A transit agency with 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.

5.1.6 Implementation Challenges

Transit agencies face many challenges when implementing access management systems. Key areas to consider include:

Cross Institutional Issues

Access management cuts across many disciplines: engineering and design, construction and maintenance, traffic engineering, law, right-of-way, real estate, disability access, and transportation and land use planning. It is important that all the individuals responsible for each of these functions are involved at the program and/or the project level. Access management also brings significant political and institutional issues to the surface.

are involved at the program and/or the project level. Access management also brings significant political and institutional issues to the surface.

Designing System Security

Designing security into the system is easier and cheaper than patching it on later—security managers should be involved in the planning for all new construction and retrofit projects

Incorporating Security Considerations Early

The ability to manage access effectively is often a function of the extent to which access management is considered in the planning stages, when agencies have the greatest opportunity to get results that are most in line with the recommended standards and guidelines established in their programs. The bigger challenge occurs when there has been little or no consideration given to managing access, requiring the retrofit of access controls, which is typically a long and challenging process.

Institutional Issues and Philosophical Differences

Access management initiatives, like all efforts to strengthen transportation security, face several long-term institutional challenges that include: (1) developing a comprehensive risk management approach; (2) ensuring that funding needs are identified and prioritized and that costs are controlled; (3) establishing effective coordination among the many responsible public and private entities; (4) ensuring adequate workforce competence and staffing levels; and (5) implementing security standards for transportation facilities, workers, and security equipment.[21]

Funding

Two key funding and accountability challenges for agencies include: (1) paying for increased access management; and (2) ensuring that these costs are controlled. The costs associated with acquiring equipment and personnel for improving transit security are significant. Many of the planned security improvements for transit facilities require costly outlays for infrastructure, technology, and personnel at a time when weakening local economies have reduced local transportation agencies' abilities to fund security improvements. Most of the technologies and policies associated with access management are scalable, however, making it possible for transit agencies to design individual access management programs that meet their own needs and available resources.

Legal Issues

Legal issues abound in the access management arena. Transit agencies and other organizations are increasingly concerned about the threat of being found liable as a result of security negligence. For example, any agency that installs CCTV without an effective policy for monitoring, recording, and managing the captured images could be held responsible for negligence. Likewise, an agency that uses vehicle barrier devices without providing proper employee training runs the risk that an individual or automobile will be injured by one of the barriers. Furthermore, organizations that do

[21] GAO. *Post September 11th Initiatives and Long-Term Challenges*. GAO-03-616T. March 31, 2001. Available at: http://www.gao.gov/new.items/d03616t.pdf.

not implement or enforce existing security policies may find these policies to be a liability. For these reasons, efforts to avoid liability due to security negligence must be at the forefront of any security strategy.

Agencies must also consider how to respond to requests for information that may compromise security, whether such requests are a result of freedom of information requests or of competitive bidding processes. Legal and policy staff should consider which documents should be released at various stages of such processes, and how to ensure that the requesting party understands the sensitivity of the information.

Agencies that outsource components or processes of their security program to security-service providers should consider a close read of their service contracts to fully understand the liability implications. Comprehensive integrated security systems can be the best "liability insurance" money can buy:

- The cost of business property theft, employee theft, and computer crime is skyrocketing.
- Limited resources mean cutbacks on what local law enforcement can do.
- Security-related litigation (based on claims that existing security was "inadequate") is producing average awards in excess of $1 million.[22]

Many security suits relate to:

- Inadequate security personnel
- Inadequate lighting
- Non-operable equipment
- Faulty equipment
- Promised security when there is no security (brochures and advertisements promising security)
- Negligent retention and training of security personnel

Other legal issues to consider include the growth of privacy as a global issue, and the possible illegality of many access management countermeasure devices in some geographic areas.

5.2 Tools/Techniques

This section provides an overview of tools and techniques transit agencies can use to manage access. These include:

- Policies and procedures
- Perimeter protection and physical barriers

What is an effective access management strategy?
A diverse set of tools and techniques creating an adaptable network of security measures.

[22] Cunningham, William C., Taylor, Todd H. *The Hallcrest Report I: Private Security and Police In America.* National Institute of Justice. June 1985.

- 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. Refer to Section **5.3** for sample access management guidelines, with details on specifications and deployment strategies.

5.2.1 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.

Agencies must have an up-to-date access management plan that 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. Access management policies and procedures should be based on the results of a system-wide TVA. Refer to the FTA's *Public Transportation System Security and Emergency Preparedness Planning Guide* for a step-by-step description of conducting a TVA.[23]

What kinds of procedures are necessary?

Agencies should consider an up-to-date access management plan that lists the *functional requirements* for access management systems, as well as *standard operating procedures* that address contingencies for security issues that may arise.

5.2.2 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: admission control and perimeter control.

[23] The FTA's *Public Transportation System Security and Emergency Preparedness Planning Guide* (2003) describes the steps in conducting a TVA. **http://transit-safety.volpe.dot.gov/Publications/security/PlanningGuide.pdf**.

- Admission-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 (refer to Section **5.3**).
- 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 line 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 (see Sections **5.3.5** and **5.3.6**).

Shrubbery and landscaping decisions along a perimeter should be based 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. Details on perimeter designs and strategies are covered in *Chapter 6: Infrastructure*. Sections **6.2.1** and **6.2.2** describe the design of the site and interior layout. Section **6.3** describes design-related security strategies for perimeter security at fixed sites and facilities (the transit infrastructure) within a system, organized by type of asset, such as transit stations and tunnels, with subsections on perimeter security for each asset.

"The Security-Oriented Design Considerations for Transit Infrastructure" chapter of the FTA Handbook also has additional information about perimeter designs and strategies.[24]

5.2.3 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, transit agencies may use screening at key high-security facilities/areas, or may selectively screen for high-risk individuals, locations, and events.

[24] Ibid.

For transit agencies, 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 admission-control device. Entry-point screening is particularly beneficial with temporary or occasional workers and visitors.

Transit agencies can utilize 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 5-4).

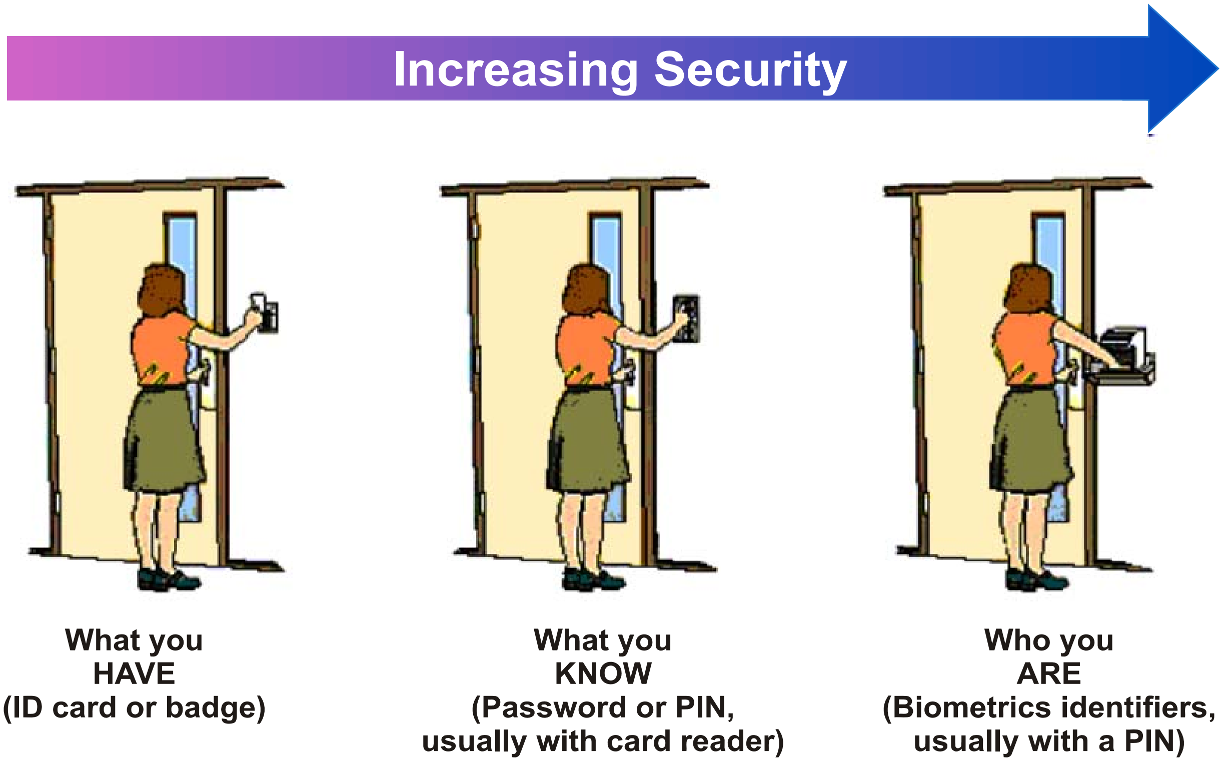

Increasing Security
What you HAVE (ID card or badge)
What you KNOW (Password or PIN, usually with card reader)
Who you ARE (Biometrics identifiers, usually with a PIN)

Figure 5-4. Entry Control Techniques

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 (see Section

5.2.5), 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.

5.2.4 Credentials and Credentialing

Credentials and credentialing are key components for an agency's access control system.

5.2.4.1 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.

TSA's Transportation Worker Identification Credential (TWIC)

The TWIC is a uniform identification credential for all transportation workers requiring unescorted access to secure areas at transportation facilities including mass transit.

The TWIC works with multiple types off access control points (vehicle gates, building, and door access) as well as multiple access control technologies (smart chips and barcodes).

Credentialing covers physical and logical access for individuals. Access management-related steps include establishing a secure ID, background checks and credentialing, enrollment, data management and procedures.

5.2.4.2 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.

Agencies should consider assigning a security classification to each part of the system, and identifying the types of users accessing each part. Many agencies also perform 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 5-5 illustrates the credentialing process for access control.

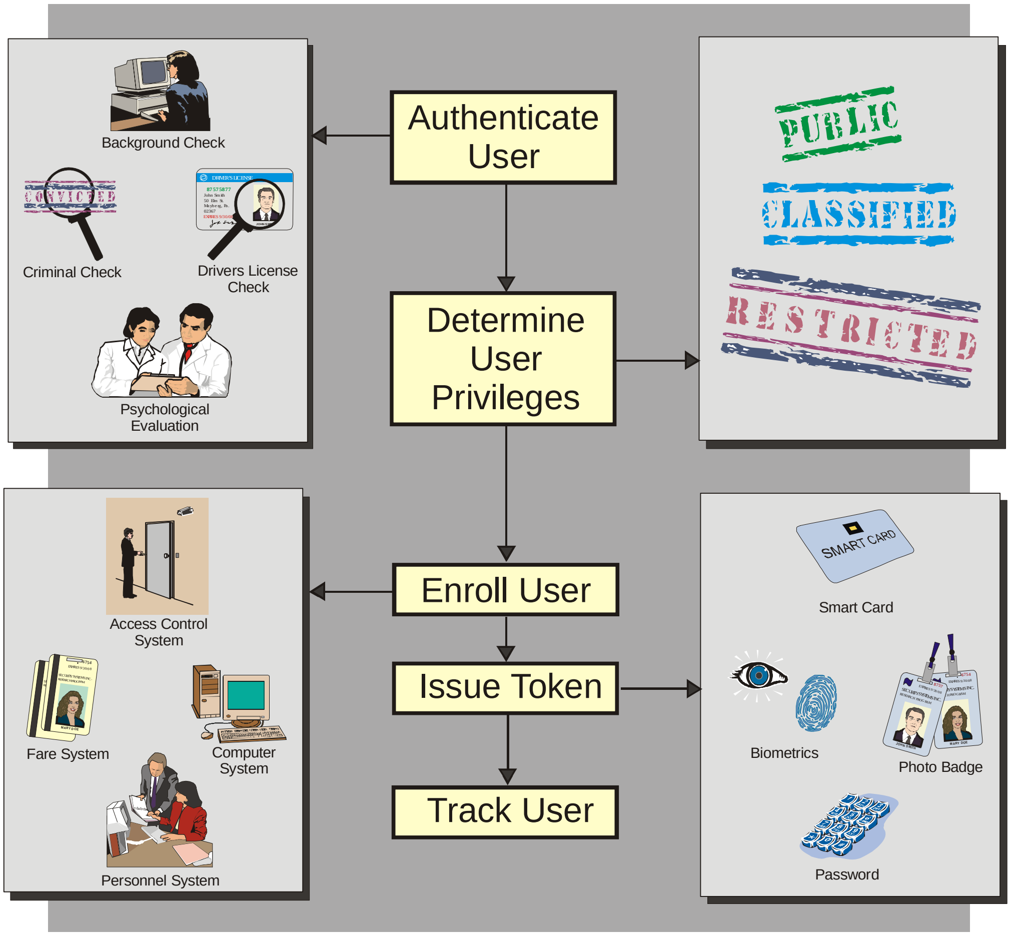


Figure 5-5. Credentialing and Access Control

Credentialing is an important access management tool. In the transit environment, its use is limited to individuals employed or contracted (including concessionaires) by the agency, 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.

A Transit TWIC Secure Area is an area of a public transportation operation where the local operator:

- Has determined that the risk of intrusion and subsequent risk of damage requires all workers and unescorted contractors in that area to obtain and carry a TWIC.
- Has determined a TWIC requirement would effectively reduce the risk of intrusion (i.e., a train platform carries the risk of intrusion and subsequent damage but a TWIC would not be an effective component of access control because a platform is a public area
- Have the authority, intent and the means to maintain the characteristics of a Transit TWIC Secure Area.

Secure areas may include: *Dispatch/Control Facility; Bus Engine Compartment/Mechanical Areas; Maintenance Facility/Garage/Yard; Central Control Facility; Law Enforcement Facilities; Revenue Rooms; Revenue Transport Train/Truck, Power Cabinets, Switch/Signal Cabinets; HVAC systems; Fuel Storage Facilities; Confidential Records Repositories; Agency Chief Operating Officer's Offices*

5.2.5 Surveillance Systems

Surveillance

Observation methods either carried out by humans or with the assistance of technology

By deploying remote CCTV surveillance systems, agencies can expand 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 (see Section 5.2.6) 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.

5.2.6 Intrusion Detection

An 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.

Intrusion-Detection Systems

Integrated electronic components for detecting intrusion into a protected area and *alerting response forces*

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. For more information on intrusion detection for tunnels, refer to Section 6.3.6.

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.[25]

[25] The TCRP program has prepared a detailed report on intrusion-detection systems that offers a detailed review of the advantages and disadvantages of many technologies. *Intrusion Detection for Public Transportation Facilities Handbook*, Transit Cooperative Research Program, March 2003.

5.2.7 Security Personnel

Many transit agencies, particularly the larger ones, deploy their own security forces to patrol facilities. 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

…security force roles have (shifted) from crime-prevention and safety to *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.[26]
- Response – responding to alarms or unauthorized entry.
- Communications – contacting law enforcement and emergency response personnel.

5.2.8 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,

Communication Systems

Enable person-to-person communications and can link various access management subsystems into a networked security system.

Information Processing Systems

Coordinate activities, record incident data, provide audit trails, and generate reports.

[26] Balog, Bromley, et al. *K9 Units in Public Transportation: A Guide for Decision Makers.* TRB TCRP Report 86: Public Transportation Security. Transportation Research Board National Research Council Volume 2: 2002.

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. Refer to the chapter on "Security-Oriented Design Considerations for Transit Communications" in the FTA Handbook for additional information.[27]

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.

5.2.9 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.

See Section **5.3.2** for additional information about lighting systems and standards.

5.3 Sample Access Management Guidelines

Transit system operators have the primary responsibility for ensuring their systems and facilities are secure. This section presents sample guidelines for various access management security measures. The intent is to provide information that will assist transit facility operators in understanding and managing risks to their facilities and other assets. These guidelines are also intended to make transit agency managers aware of the major areas that should be addressed in an access management policy and plan, and which standards and procedures should be established.

The guidelines are not exhaustive; they are an outline of general approaches to access management and are a useful resource, but each agency must identify its particular security needs and determine which access management measures are appropriate. Agencies also should 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

[27] Ibid. **http://transit-safety.volpe.dot.gov/Publications/Default.asp**.

lots and garages, and other facilities open to and used by the public. Some guidelines are best implemented in new transit infrastructure; others can be easily included as part of a retrofit or reconstruction. The bottom line is that agencies should make access management decisions on a case-by-case basis to meet the needs and available resources of their individual transit agency.

Guidelines are summarized for the following access management areas:

- Fencing and gates
- Security lighting
- Admission control
- Vehicle access control and parking
- Vehicle barriers
- Critical/restricted area access
- Windows
- Wall safeguards
- Miscellaneous openings
- Personnel security
- Key control
- Security force

> The guidelines outline general approaches to access management and are a useful resource, but each agency must identify its particular security needs and determine which access management measures are appropriate.

Note that details on asset management design and strategies are beyond the scope of this chapter and are covered in *Chapter 6: Infrastructure*. Section 6.2 is an overview of design considerations for fixed sites and facilities (the transit infrastructure) within a system. Section 6.3 describes design-related security strategies.

5.3.1 Fencing and Gates

Agencies should consider these guidelines when installing, maintaining, and controlling perimeter fences, clear zones, fence fabric, posts and hardware, openings, and gates.

Design considerations – refer to Section 6.2.1

Security strategies – refer to Perimeter Security subsections in Section 6.3

5.3.1.1 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 cost-effective 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 prevent 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.

5.3.1.2 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.

5.3.1.3 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.

5.3.1.4 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 penning 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 penned 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.

5.3.1.5 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.

5.3.1.6 Gates

Perimeter Gates

The number of perimeter gates designated for active use should be kept to the absolute minimum required for operations. Agencies should take into account sufficient entrances to accommodate the peak flow of both pedestrian and vehicular traffic, as well as adequate lighting at egress and ingress points (refer to Section 5.3.2.2).

- 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.

Unattended/Inactive Gates

Agencies should 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.

5.3.2 Security Lighting

Security lighting 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 agencies are 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. For a description of types of security lighting, refer to Section 5.3.2.3.

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. 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. Agencies should understand that undesirable shadowing will exist, and the total elimination of shadowing is not practical in all areas.

However, lighting need also be appropriate to the operating environment. Agencies should 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. Agencies should 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.

Design considerations – refer to Section 6.2.5.5

Security strategies – refer to Sections 6.3.1 transit stations, 6.3.2 transit stops, 6.3.3 administrative buildings/OCCs, 6.3.5 elevated structures, 6.3.6 tunnels

In general, agencies should consider these guidelines 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.
- 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 security lighting should be located in restricted areas, 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 power supply line(s) separated from the primary power line(s). The facility should have the ability to rapidly switch to the secondary power line(s) during power failures. Security lighting systems should be independent of the general transit facility lighting or power system.
- Power supplies for security lighting should be adequately protected.
- Standby/emergency lighting should be tested per industry standard, for example: monthly for a duration of 30 seconds and annually for a duration of 1½ hours.
- Inoperative lights and lamps should be repaired/replaced immediately.

- Materials and equipment in storage areas should not mask security lighting.

Agencies should consider these lighting guidelines for perimeter lighting and for entry, guardhouse, and parking lot lighting.

5.3.2.1 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.

5.3.2.2 Entry, Guardhouse, and Parking Lot Lighting

Entry/Guardhouse

- 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.

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 during times of darkness and extreme environmental conditions.

Emergency Power

- Parking lot and entry 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

5.3.2.3 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.

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 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.

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.

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.

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 an uninterruptible power system when possible, emergency lighting should depend on a separate, alternate power source, such as portable generators or batteries. Table 5-1 lists the standard illuminance in foot-candles for several security lighting targets.

Table 5-1. Illuminance Specification

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)	

5.3.3 Admission Control

Admission control to non-public/secure areas of a transit system is essential. The most common admission 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.

In addition to physical countermeasures, admission control relies heavily on following procedures.

Agencies should follow these admission control guidelines for facility employees, contractors, and visitors; and pick-ups and deliveries.

Design considerations – refer to Section 6.2.1

Security strategies – refer to Human Access subsections in Section 6.3

5.3.3.1 Facility Employees, Contractors, and Visitors

Requirements for identification of facility employees, contractors, and visitors can include:

- 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 (as described below) 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.

5.3.3.2 Pick-Ups and Deliveries

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.

5.3.4 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.

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.

Design considerations – refer to Section 6.2.1

Security strategies – refer to Vehicle Access subsections in Section 6.3

5.3.4.1 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. Used 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.

5.3.4.2 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.
- 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.
- Parking regulations should be strictly enforced.
- Emergency communication speakers should be installed in the parking area in order to broadcast emergency procedures and/or instructions.
- Vehicle entry and exit routes should be clearly marked.
- A facility should have formal procedures for controlling vehicle access and parking.

5.3.4.3 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.

5.3.4.4 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.

5.3.4.5 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.

5.3.4.6 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.

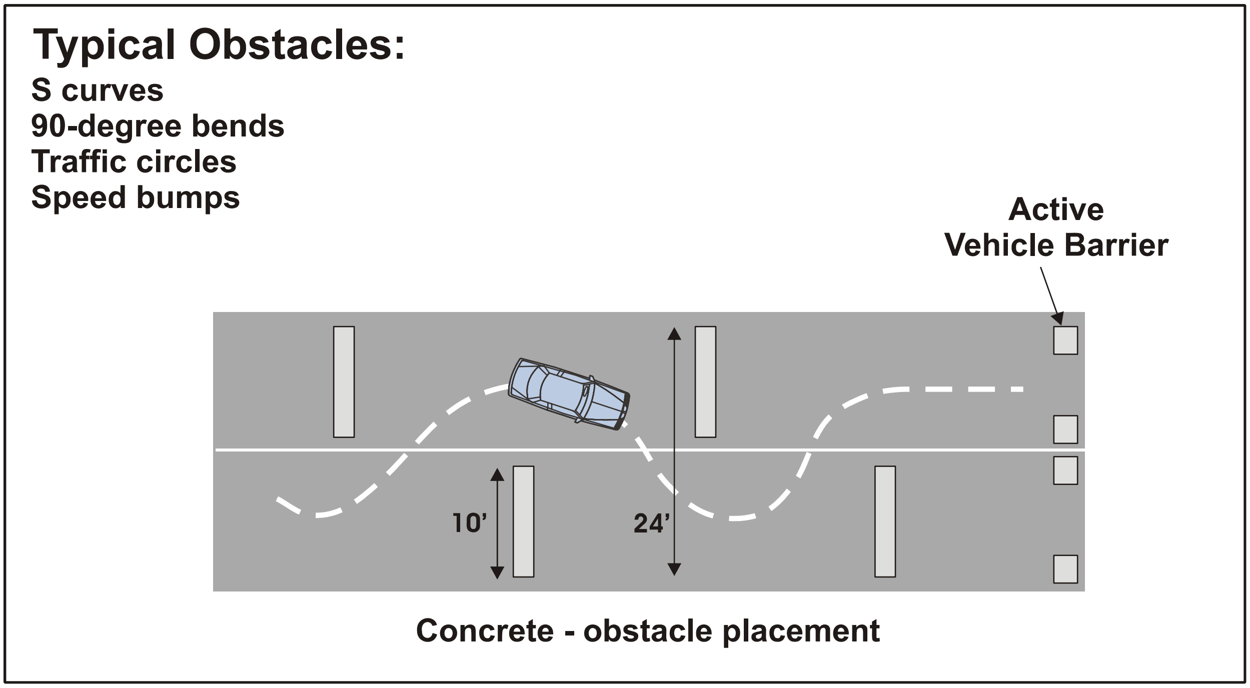
5.3.4.7 High-Speed Vehicle Approaches

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 5-6).

- 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.

5.3.4.8 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.



Source: DOD FM5-114

Figure 5-6. Speed Reduction Approach

5.3.4.9 Electronic Vehicle Access Control Systems

An electronic vehicle access control system regulates inbound and outbound traffic using an electronic device to activate a barrier or gate. Vehicle drivers display or insert the appropriate entry control device into an access card/badge reader.

Remotely operated monitoring and access control systems can give the operator full control over the remote security system and access to all data that the security system may collect. In a typical remote system, video from closed circuit television cameras, data from sensors, card readers, or biometric devices is delivered to an operator at a monitoring site in near real-time for review. In turn, data from the operator, such as the request to open a gate or a request for information, is sent to the remote site to be processed by the remote components of the system. In the case of a person wishing to access the remote site the monitor reviews the credentials of the person requesting access and grants or denies access based on its assessment. The system then logs the transaction and returns to its original state. The remote system generally has some mechanism to alert the monitor when an alarm condition occurs. When an alarm does occur, the monitor should take appropriate action.

- It is important when selecting an electronic vehicle access control system that its architecture is flexible enough to use any commercially available communication network. This could be digital network, telephone, modem, satellite, microwave, or leased line. Depending on the type and format of data being used, bandwidth requirements will vary greatly from system to system.
- The manufacture of the system selected should be able to provide an accurate throughput performance estimate for a variety of networks.

5.3.5 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.

5.3.5.1 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.

5.3.5.2 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 Table 5-2, 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.

Table 5-2. Vehicle Barrier 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**
Usage	Create Standoff Distance	•	•	•	•	
	Protect Assets/Pedestrians	•	•	•	•	
	Slow Vehicles (speed control)		•		•	
	Stop Vehicles		•	•	•	
	Restrict Vehicle Entry		•	•	•	•
	Direct Traffic	•	•	•	•	•
	Revenue Collection		•			
	Theft Deterrent		•		•	

Design considerations **–** refer to Section 6.2.1

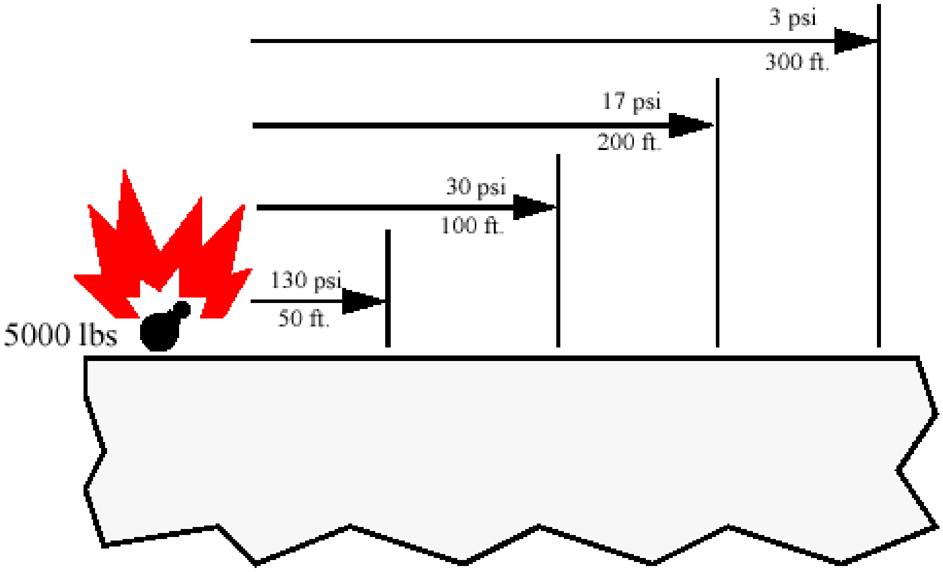
Security strategies – refer to Vehicle Access subsections in Section 6.3

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 (refer to Section 6.2.1.2 for further information on standoff distances).

Barriers can be placed to establish a standoff distance at a particular location or around the entire perimeter of a facility. Agencies should 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 5-7 shows blast overpressures at various distances for a 5,000 lb TNT equivalent blast.



Source: LLNL, undated

Figure 5-7. Blast Overpressures as a Function of Distance (For a Bomb Equivalent to 5,000 Pounds of TNT)

Blast overpressures can cause damage to structures and humans. Human blast injuries are primary (direct effect of blast); secondary (injuries caused by flying debris); tertiary (when people are thrown by the blast and strike other objects); and quaternary (all other injuries caused by explosions, e.g., burns or crush injuries). Although damages depend on the type/duration of the blast, Table 5-3 provides estimated damage thresholds:

Table 5-3. Blast Damage

Pressure (PSI)	Damage
0.5-1	Window breakage
>1	Knock down person
1-2	Damage to corrugated panels / wood siding
2-3	Collapse of non-reinforces cinder block
5-6	Push over wooden telephone poles
>5	Rupture eardrums
>15	Lung damage
>35	Threshold for fatal injuries
>50	About 50% fatality rate
>65	About 99% fatality rate

Source: [White, 1968], [DOD 1997], [Montgomery, 1993], [Kinney 1985]

As seen in Table 5-4, a blast of approximately this size could be delivered in a box truck.

Table 5-4. Blast Charge and Damage Distance

Device	Description	Charge Weight (TNT Equiv. lbs)	Distance for Specified Damage and Injury (ft)*				
			Minimal Damage	Minor Damage	Moderate Damage	Heavy Damage	Severe Damage
	Pipe Bomb	5					
	Suitcase	50					
	Compact Sedan	220					
	Full Size Sedan	500					
	Passenger / Cargo Van	1,000					
	Box Truck	4,000					
	Semi-Trailer	40,000					

Source: TSWG Damage and Injury Distance Card Set (available through the GPO (S/N: 064-000-00028-4)

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.

Vehicle Speed

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

Vehicle Stops

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

Vehicle Restriction

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

Traffic Direction

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

Revenue Collection

Barriers can enforce revenue collection at parking lots and garages.

Theft Deterrence

Barriers can deter theft at parking lots and garages.

5.3.5.3 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.

Refer to Appendix D, "Vehicle Barrier Types," for a list of all barrier types and a description of their effectiveness and use. For details on costs, advantages and disadvantages of vehicle barrier types, refer to the *TCRP Intrusion Detection for Public Transportation Facilities Handbook*[28] [TCRP 2003].

[28] *Intrusion Detection for Public Transportation Facilities Handbook*, Transit Cooperative Research Program (TCRP). March 2003.

5.3.5.4 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.

There are many issues to consider in developing requirements for barriers at a specific location and selecting the appropriate barrier. Refer to Appendix E, "Vehicle Barrier Selection and Implementation Considerations." This list can be helpful in selecting the appropriate barrier type and developing requirements for barriers.

5.3.6 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.

Agencies should follow these guidelines for critical operation areas and hazardous and security operating areas.

Design considerations – refer to Sections 6.2.2 and 6.2.5

Security strategies – refer to Critical Access subsections in Section 6.3

5.3.6.1 Critical Operating Areas

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

- The facility operator 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.

5.3.6.2 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.

5.3.7 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 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.

Agencies should follow these window security guidelines for construction, steel bars and grills, glass brick, glass and steel framework, and security glazing.

Design considerations – refer to Sections 6.2.3 and 6.2.4.3

5.3.7.1 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.

5.3.7.2 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.

5.3.7.3 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.

5.3.7.4 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.

5.3.7.5 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.

5.3.8 Wall Safeguards

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.

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

Design considerations – refer to Sections 6.2.3 and 6.2.4.1

5.3.8.1 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 (see Section 5.3.8.3).

5.3.8.2 Reinforced Wall

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

5.3.8.3 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.

5.3.9 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.

Design considerations – refer to Sections 6.2.5.8 (water and sewer)

Security strategies – refer to Human Access subsections in Section 6.3

5.3.9.1 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.

5.3.9.2 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.

5.3.9.3 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.

5.3.9.4 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.

5.3.9.5 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.

5.3.9.6 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[29].

- 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).

[29] 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.

- If relocation of outdoor air intakes is not feasible, construct intake extensions to place the intake out of 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.

These measures are not sufficiently secure for subway system tunnel, which require special considerations (refer to Section 6.3.6).

5.3.10 Personnel Security

Since it is possible for threats to come from within an agency (such as disgruntled employees) as well as from outside, transit mangers should follow hiring and employment termination practices that contribute to the security of their facilities.

Agencies should follow these guidelines relating to pre-employment screening and levels of screening. However, agencies should consider also adopting a policy of periodic ongoing employee screening.

5.3.10.1 Pre-Employment Screening

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.

5.3.10.2 Levels of Screening

Pre-employment screening can include many layers of investigation and types of screening.

- Identification check. Will confirm the identity of the person and typically includes a social security validation.
- Employment check. Will confirm the applicant's resume, and verifies their previous job history including: start date, end date, salary, reason for leaving, rehire status, and responsibilities, and comments from former employer.
- Education check. Will confirm attendance dates, degree/diploma/certificate received, grade point average (GPA), and area of study.
- Criminal history check. Will reveal felonies and misdemeanors (7-10 year history is typical), offense/disposition date and judgment.
- Motor Vehicle Records (MVR) search. Provides information contained in the applicant's driving record (verification of valid license and class/type, issue/expiration date, personal identifying information, violation points, and suspensions/revocations.
- Credit history. Will show the applicant's ability to manage their finances responsibly. This is useful in determining whether an employee is suitable for a fiduciary position.
- Military check. Confirms service dates, service branch, pay grade and termination status.
- Professional accreditation/license check. Will confirm whether an applicant has the required credentials or licenses, type of license, whether currently valid, dates issued, state and licensing authority, restrictions on the license, disciplinary actions or suspensions.
- Medical assessment. Ensures compliance with medical requirements of certain jobs.
- Immigration and Naturalization Service (INS) check. Verifies with the INS the status of the applicants.

Each transit agency should establish screening policies that specify the level of screening required of each position and employment circumstance. Table 5-5 shows a sample of a screening matrix that includes types of screening and the positions for which the screenings could apply. Agencies should consider whether the investigations will be done in-house or by a third-party vendor.

Table 5-5. Sample Pre-Employment Background Screening Matrix

	Type of Screening									
	Identification	Employment History	Education	Criminal Record	Motor Vehicle Record	Credit History	Military	Professional Accreditation	Medical Assessment	INS Form I-9
New hires	•	•	•	•	•	•	•	•	•	•
Re-hires	•	•	•	•	•	•	•	•	•	•
Contractors and vendors	•			•	•	•			•	•
Other non-employee/non contractor/vendor (e.g., street performer/ concession worker)	•			•						•

5.3.11 Key Control

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

Agencies should follow these guidelines relating to control of locks and keys, key control official responsibilities, records requirements, issue and control procedures, and lost keys.

5.3.11.1 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.

5.3.11.2 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.

5.3.11.3 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.

5.3.11.4 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.

5.3.11.5 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.

5.3.12 Security Force

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/uninformed; patrol/fixed post/random; mounted/K-9/cycle) can be tailored to the specific transit agency.

Agencies should evaluate the need for contract security guard support for existing facilities where guards are not already required. For facilities that have contract security guard service, the facility manager should ensure that the security guards are being employed in the most effective manner to accomplish facility security goals.

Security strategies – refer to Perimeter Security, Human Access, and Protecting Critical Assets subsections in Section 6.3

Contract guard requirements, responsibilities, and qualification criteria should be established and considered in the decision to employ a contract security guard force.

- Designated personnel should conduct roving safety and security patrols in facility areas with limited or irregular staff presence.

- Security patrols should, at a minimum, cover restricted areas, main power supply switch gear, lighting controls, perimeter access points, vehicle parking areas, communications and operations control centers and waterside access areas.
- Designated personnel must be able to respond immediately to a security alert signal in accordance with established procedures in the security plan.
- Records of unusual occurrences encountered during security patrols should be maintained in a log. Such records should be maintained and must be available for inspection.

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

6.0 Infrastructure

Generally, infrastructure is the set of underlying structural or institutional elements that provide the framework in which a structure or facility operates and functions. The components of infrastructure are the elements that enable and facilitate carrying out certain activities. Transit infrastructure in particular refers to all the stationary assets in a system, such as real estate, buildings, tunnels, and rail tracks.

Infrastructure design is only one element of a larger security program. The process begins with a TVA, which identifies potential threats and their severity, and estimates how vulnerable each asset is to these threats. Scenario and Consequence Analyses then evaluate the maximum extent of damage or injury in the event of an attack. Based on these evaluations, transit agency officials can then prioritize their concerns and determine the appropriate level of protection through countermeasures.

How is this chapter useful?

For **transit administrators** it is a resource for:

- Security design concepts to consider when procuring infrastructure assets
- Reviewing infrastructure design guidelines

For **operations or planning staff** it is a resource for:

- Identifying tools and techniques for hardening assets

For **engineers** it is a resource for:

- Reviewing current hardening practices and procedures

Agencies adopting any of the infrastructure design security measures described in this chapter should consider coordinating them with other transit system components, such as vehicles and emergency procedures, to develop a comprehensive security strategy.

Overlaps between access management and infrastructure protection are extensive. Many of the threats facing infrastructure can be greatly reduced by instituting appropriate access management measures. Since no transit security program can be completely effective at eliminating risk while still providing convenient and high quality service, infrastructure design should also include measures to prevent attacks or reduce their effects in the event that perpetrators are able to gain access. Refer to **Chapter 5: Access Management** for additional information. Note also that this chapter is specific to infrastructure; design-related security measures for other transit assets are covered in **Chapter 7: Vehicles** and **Chapter 8: Communications**.

This chapter provides further details on the concept of CPTED[30] by showing how agencies can use the physical design of infrastructure components to help detect and prevent attempted terrorist

[30] CPTED is a branch of situational crime prevention 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 differs from other crime prevention strategies by using environmental factors, such as site plan, building layout, and other physical characteristics, to bring about behavioral effects that reduce the fear and incidence of crime. Refer to **www.cpted.com.au** and **www.cpted-watch.com** and to the *Security-Oriented Design Considerations for Transit Infrastructure"* section of the 1998 *FTA Transit Security Handbook* at **http://transit-safety.volpe.dot.gov/Publications/Default.asp** for additional information.

attacks in their systems, and minimize the damage from attacks that do occur. This chapter begins with an overview of the various categories of transit infrastructure, then continues with a description of:

- Infrastructure Characteristics
- Security Approaches for Types of Transit Infrastructure

6.1 Introduction to Security Design for Transit Infrastructure

6.1.1 Categories of Infrastructure

Infrastructure categories relating to all of the fixed sites and facilities within a system are summarized below and described in more detail in Section 6.3.

- Transit Stations are facilities used for boarding and alighting of transit passengers, and fare collection; they can be below-grade, at-grade, or elevated. Their high profile, large volumes of pedestrian traffic, and central locations integrated with surrounding uses, make them likely targets for terrorist attack.
- Transit Stops are usually smaller and more open than transit stations. They are typically on public land, where passengers can board buses and light rail vehicles; these include everything from elaborate shelters to mere signposts. Transit agencies often lack control over these sites, which, combined with their high level of accessibility, makes them difficult to secure against attack.
- Administrative Facilities and Operations Control Centers (OCCs) are used for the operations and administration of the transit system and may be co-located on a site with non-transit uses. Although most administrative facilities are not open to the public and can therefore maintain stricter access control, they have a critical role in the transit system and have value as strategic targets.
- Vehicle Maintenance Facilities are used for the repair and storage of transit vehicles; they include vehicle garages, yards, and repair facilities. They often contain a large number of assets to be protected, including some high-risk elements such as fuel storage areas or containers. Maintenance facilities can be designed to allow transit vehicles and maintenance staff to enter and exit freely, while preventing access by unauthorized vehicles and people.
- Elevated Structures refer to all above-grade bridges and track structures, including pedestrian bridges and overpasses. Their high visibility and structural complexity present particular challenges to securing them against terrorist attack.
- Tunnels are used for the passage of transit vehicles underground and, in limited cases, underwater. They are more secure when designed to prevent unauthorized access from

passenger platforms and at-grade entrances, while allowing transit vehicles to pass freely. Proper design can also facilitate evacuation in an emergency.

- Right-of-Way, Track, and Signals include all land and equipment dedicated to the movement of transit vehicles between stations. Like tunnels, a design goal is to allow transit vehicle movement while preventing access by unauthorized people or vehicles.
- Remote and Unmanned Structures capture all other physical assets. This category includes power substations and communications relays, and the like, which are not necessarily located on rights-of-way or in stations. These may be owned or controlled by other agencies or companies. Design features that take into account their remote locations and lack of consistent or continuous staff presence can improve their security.

6.2 Infrastructure Characteristics

This section describes transit property design elements that planners, designers, and administrators should consider when selecting a facility location and/or designing a new or renovating existing facilities to protect them against potential terrorist attacks. Characteristics include:

- Site layout
- **Interior layout**
- **Structural engineering**
- **Architectural features**
- **Systems and services**

6.2.1 Site Layout

The physical characteristics of a site have a major impact on which security measures are possible and appropriate in safeguarding a facility. Some of these elements, such as building location, landscaping, and site circulation are under the control of the transit agency; while off-site features, such as topography and abutting uses, are not. Some on-site characteristics such as topography and vegetation are under limited control of the transit agency.

This section describes the factors a transit agency might consider when determining where to locate a facility and how to design the site. These include site selection, building placement, access points to the site, on-site vehicle circulation, and relevant factors to mixed-use facilities.

Site layout can be conducive to incorporating measures that protect personnel, riders, and other assets from attacks, and to limiting unauthorized access to the property. In addition, a facility's site design should enable security measures to be scaled and adapted in response to changing threat levels over time.

6.2.1.1 Site Selection

The unique characteristics of a site influence their appropriateness for different types of transit facilities, and have a direct effect on security. Relevant security issues for agencies include obstacles hindering outward surveillance, amount of available land, natural buffers, and the existence of nearby elevated vantage points.

Planners should consider the impact of the following site elements on site security when evaluating a property:

- Natural features (such as a stream or swamp)
- Manmade features (such as a pipeline or neighboring building)
- Existing easements
- General characteristics of abutting properties and access control
- Access to public roads
- Proximity to private roads

Natural Features

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. Refer to Section **6.2.1.2** for details on using unobstructed space as a strategy and Section **6.2.1.3** for access management strategies.

Some natural features benefit site security. For example a stream, especially one with a sunken bed, can be an effective barrier against vehicles trying to gain unauthorized access to the property. When incorporated strategically into site layout, these features can supplement access management strategies, however, agencies must be careful not to create security gaps where such features intersect with perimeter fences and other security measures (i.e., a person might use a streambed to crawl under a fence or wall where they intersect).

Manmade Features

Manmade features may present challenges to security. For example, storm drains and utility tunnels could enable someone to gain covert access to the property.

Existing Easements

Existing easements on the property might grant non-transit personnel the right to enter the property without prior approval from the transit agency. Agencies should make efforts to be familiar with the location of existing easements, especially in relationship to the location of critical assets.

Abutting Properties

While a transit agency may be able to design its property to meet agency security needs, it may have little or no control over neighboring properties. Site planners should therefore consider the characteristics of all nearby properties in the site selection process and layout of the transit property to avoid undermining even the best on-site security precautions.

Factors to take into account include topography, vegetation, buildings, and rooftops that can provide vantage points for aggressors. An additional consideration is what access controls, if any, exist on abutting properties. For example, if an adjacent building is a federal agency with tight security and access controls, this fact may mitigate concerns about the proximity of the building to the transit site. In contrast, an abutting public park, for instance, could be seen as a legitimate security concern—both for positive reasons (open areas provide clear views of approaching persons or vehicles) and negative reasons (open, public access is offered to a wide range of individuals). Agencies should consider these issues in addition to other non-security issues when acquiring property for transit agencies. Purchasing the abutting properties outright as a buffer or for less critical uses is also an option.

Access to Public Roads

Avoid siting critical facilities in such a way that vehicles may have direct routes between public roads and critical facilities. However, the site layout should neither preclude nor complicate access via public roads for emergency vehicles, nor should it inhibit emergency egress for passengers and/or employees.

Proximity to Private Roads

Agencies should be aware of any private roads close to the property that might introduce threats to the facility, the types of traffic attracted by adjacent uses and facilities, and traffic use of private roads near the facility.

6.2.1.2 Building Placement

Appropriate placement and orientation of buildings and other structures on the site is a major component of an effective security strategy to protect against damage from terrorist attacks. Agencies should consider the impact of the following building elements on site security: unobstructed space, standoff distances, and building orientation.

Unobstructed Space

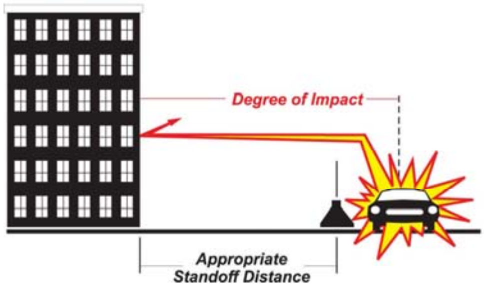
Unobstructed space is an area around an asset, usually a building, which provides clear visibility around the asset.

Agencies should consider surrounding buildings and equipment by unobstructed space to facilitate surveillance of the property and prevent the concealment of explosives and other harmful devices next to structures. For buildings, federal standards for unobstructed space call for an area 10 meters (33 feet) wide adjacent to a building.[31] This may not always be possible, particularly in dense urban areas, calling for alternate measures to accommodate existing conditions.

Standoff Distances

Standoff distances are minimum distances between a building, or other asset, and a secured perimeter barrier established to protect the asset from blast damage. Standoff distances limit the proximity of a terrorist or explosive to the asset. The appropriate standoff distances are determined by the size of a potential explosive and the critical value of the asset. Standoff distances help minimize damage from an explosive attack.

Figure 6-1 illustrates the impact of standoff distances on building security.



Standoff distances help minimize damage from an explosive attack.

Figure 6-1. Standoff Distance

The area within the standoff distance, excluding unobstructed space, can be landscaped with trees, shrubbery and other features. If agencies use this area, wherever possible they should avoid inhibiting the security function of the space; activities such as parking should be avoided. If parking within the standoff distance is needed, agencies should consider parking access control measures. If threat levels increase, they should consider temporarily prohibiting parking. Agencies should also consider restricting bicycle parking within standoff distances as threat levels rise, especially where bicycle lockers are used since they might conceal bombs or weapons.

Building Orientation

Building orientation can be used to protect or shield external vulnerable features of a building from an attack. Vulnerable features include entrances, windows, lobby areas, drop-off areas, loading docks, and other miscellaneous openings.

Agencies should consider orienting buildings and other critical assets so that clear lines of sight between their vulnerabilities and uncontrolled areas or vantage points is avoided. On-site vantage points include publicly accessible areas such as lobbies and parking lots, which may have less

[31] UFC 4-101-01, Department of Defense, *Minimum Antiterrorism Standards for Buildings*, (31 July 2002).

stringent security measures. For example, entrances to critical buildings should not directly face a public street from which an aggressor could fire a weapon at the lobby. When orienting assets, the site planner should keep in mind that the aggressor does not have to be in the secured area to attack a person or asset within the secured area; likely origins of attacks from which a terrorist could fire a weapon or detonate an explosive include nearby buildings, hilltops, roadways, or other uncontrolled areas outside the transit property perimeter.

6.2.1.3 Access Points to the Site

Control over how and where vehicles and pedestrians approach and enter a transit property is a crucial factor in site security.

Key concerns include number and location of access points, dedicated entrances or areas, and speed-control approaches.

Number and Location of Access Points

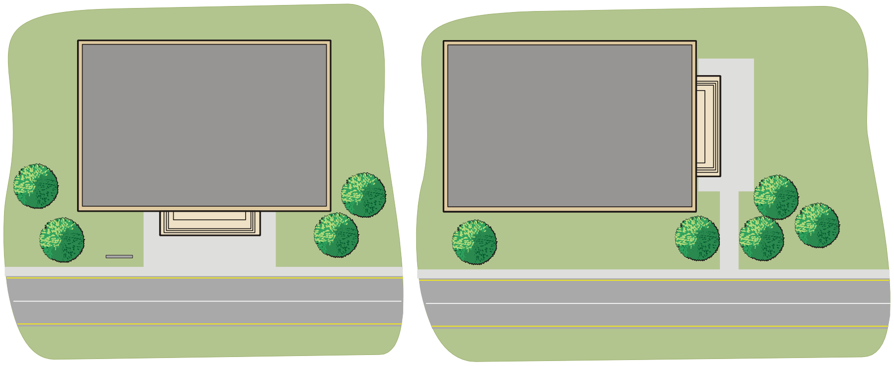
Access points are the means by which people enter and exit a site. The quantity and location of access points depends on a number of factors, including directions from which people will be approaching the site, method of approach (car, on foot, etc.), and the volume and timing of people or vehicles the entrances must accommodate. The type of facility plays a role as well; a large transit station, for example, may need several entrances to function smoothly, while a maintenance yard may have only one entrance for vehicles and pedestrians.

A facility with fewer entrances is generally easier to secure. Agencies should consider designing a site with the minimum number of entrances needed to satisfy the requirements of its daily operations. In areas where local safety regulations require emergency entrances and exits, these points should be secured in a manner that prevents unauthorized everyday access while still meeting safety criteria; this often requires advanced coordination with emergency responders to ensure they will have access to the property through all entrances. As threat levels vary, some access points to sites or buildings can be closed off, to channel movement by less vulnerable assets.

Agencies should consider locating facility entrances at points that reflect their user population, while facilitating security. Facilities with heavy public use, such as transit stations, should have access points that maximize convenience and capacity, while facilities used less frequently by the public can have less convenient entrances without generating a significant negative impact on facility operations (see Figure 6-2).

Dedicated Entrances or Areas

At facilities with different types of users accessing the site, it may be appropriate to have specific entrances and areas within the site dedicated to particular users. The goal of this strategy is to segregate traffic that presents different security threats, and therefore requires different degrees of access management. Transit staff, for example, pose less of a threat than anonymous transit riders or delivery vehicles, and agencies should consider allowing their staff to access a site more easily and park their vehicles nearer to sensitive assets.



Entrances should be oriented away from (right) rather than facing (left) uncontrolled areas such as roadways, provided that such orientation does not impinge on access by disabled persons and maintains safe, convenient pedestrian access.

Figure 6-2. Building Entrance Location

Delivery vehicles pose a particularly high threat to at-risk facilities, because of their large payload and authorization to enter sites. For these reasons, agencies should consider separate delivery entrances with a dedicated access road that admits vehicles directly to receiving areas or loading docks (and away from vulnerable assets) wherever possible. If a dedicated roadway is not practical, a designated route through the site could serve the same purpose. Any delivery vehicle parked inappropriately, or seen driving outside the designated route, would be noticed more easily and generate the appropriate response from security personnel.

Many facilities may already have segregated entrances. Commercial and industrial facilities typically segregate entrances to satisfy a variety of needs such as maneuverability, aesthetics, and traffic flow. If existing facilities have segregated access routes, they should be evaluated and upgraded to address the concerns discussed in this chapter. When initiating or reconfiguring access points, planners and designers should also maintain safe, convenient access routes for pedestrians, persons with disabilities, and cyclists as well.

Speed-Control Approaches

Agencies should consider designing roadway alignments to impede high-speed vehicle approaches to site access points and assets such as buildings. This prevents an attacker from using a fast moving vehicle to ram through perimeter security or destroy an asset in a collision. Roadways approaching gates or assets can force a vehicle to pass through sharp curves that can only be negotiated at low speed. Staggered concrete or water-filled barriers or indirect roadway alignment lined with dense low shrubbery or other barriers are examples of obstacles to high-speed approaches. These methods limit the approach speed, while preserving clear views of the roadway from security checkpoints and building lobbies.

Approaches that allow a vehicle to approach a gate or checkpoint unseen can be avoided using speed bumps, speed tables, and similar traffic-calming techniques as speed controls, although they are less effective because they still allow a vehicle to accelerate. Similarly, agencies should consider avoiding clear straight approaches that allow high-speed acceleration toward lobby entrances, fuel storage, or other sensitive areas.

Vehicle barriers such as this and other access control measures assist in managing vehicles approaching a submerged access point.

6.2.1.4 On-Site Vehicle Circulation

Controlling how vehicles and pedestrians move about within a transit property may also be a useful security measure. Designers might consider dedicated circulation routes for certain users and routes that limit high-speed approaches to assets on the site. The sophistication of a circulation plan depends on the size of the site, the diversity of activities, and the types of users at the site.[32] This should include drivers, pedestrians, cyclists, etc. When selecting a facility site, an agency should consider how the property accommodates the circulation needs of both its everyday functions as well as its security concerns.

Key concerns include parking areas and drop-off areas.

Parking Areas

Agencies should consider locating general parking in open lots or dedicated garages with access control systems. Vehicles should be parked beyond standoff distances that are sufficient to protect vital structures. Agencies should avoid locating parking under a transit building or on its rooftop. If this is unavoidable, agencies should consider stricter access controls, surveillance, or detection measures.

Depending on the type of facility, planners may segregate visitor or commuter parking from that of authorized personnel, especially at sites with substantial public activity. A separate visitor parking lot may be located near the visitors' entrance to buildings, but design measures (discussed above) can be used to protect the entrance from high-speed approaches or attacks from the parking lot.

Drop-Off Areas

Passenger drop-off areas should be located where vehicles pose a minimal threat to assets. If possible, they should be outside the required standoff distance, and should not provide clear lines of sight to openings, windows, lobbies, HVAC intakes, or other external building vulnerabilities. When

[32] For information about access control concerns such as perimeter vehicle inspection, access to parking, parking and traffic controls, vehicle registration, towage and access control systems, refer to *Chapter 5: Access Management*.

it is impractical to have the drop-off area outside the standoff distance, designers may consider monitoring the drop-off area for suspicious activity or devices with additional surveillance.

Agencies should consider locating drop off areas away from areas of concern, such as a station platform, especially when the drop-off area is within the standoff distance. Depending on passenger volumes, the agency can also consider providing a shuttle bus to bring passengers or visitors from remote parking areas to a closer point. All drop-off areas should be in an open space, not under a covered entryway or building overhang, and they should not be in areas that would concentrate a blast toward a building or other sensitive assets.

6.2.1.5 Particular Considerations for Mixed-Use and Intermodal Facilities

Mixed-use facilities are buildings or parcels of land that incorporate more than one use. They are addressed in this chapter because mixed-use transit stations – those that combine transit facilities with residential, commercial or other space – are becoming a popular model in the United States. In addition, transit agencies' administrative offices are often located in buildings shared with other tenants.

Intermodal facilities are characterized by the multiple modes that meet at the location. They enable transfers or connections between bus, rail, or light rail and/or ferry lines. These facilities enable seamless transportation throughout one's journey by facilitating movement between the modes at the site.

Challenges

Securing mixed-use facilities presents unique problems because other uses will be in close proximity to transit facilities, and the transit agency's control over the entire site is typically limited. The result is that traditional access management techniques and security-oriented site design may not be possible. This is especially true for retail facilities and historic sites that integrate transit space, because of the abundance of non-secure public space surrounding the station.

Strategies

Options for addressing security concerns in mixed-use facilities vary depending on the included uses. When administrative offices share space with other tenants, security options are usually limited to access control and intrusion detection. Many office buildings have a security system for the entire building that incorporates access control, intrusion detection, and surveillance. Standoff distances for blast protection and vehicle barriers (other than for parking control) are not commonly found at commercial office properties.

Transit stations integrated into commercial, recreational, or historic facilities should focus on strategies for detection of attempted attacks. Security options for these sites include:

- CCTV and other surveillance methods
- Attack detection (fire, chemical release, explosion)

- Intrusion detections (intrusion into restricted areas such as mechanical rooms)
- Evacuation plans

A transit agency should work with the owners of the surrounding spaces to develop a security plan that meets all parties' needs. If such cooperation fails, and if the facility is judged to be at a high risk for attack, the transit agency may want to evaluate relocating to another facility.

Intermodal facilities can be somewhat easier to protect than mixed-use facilities because they are under the control of a transit agency or multiple transport agencies. The advantage is that all transit agencies have similar security concerns, making it easier to implement a comprehensive security plan. The high level of transient pedestrian traffic through intermodal stations, however, creates increased risk because it is easier for an attacker to access the site and the large amount of people make it an attractive target for an attack.

In order for the facility to work efficiently, agencies should consider balancing the need to accommodate the large numbers of people smoothly with the impositions created by security measures.

6.2.2 Interior Layout

The interior layouts of the buildings and other structures on the site may also support the detection and deterrence of harmful activity by establishing protective barriers around sensitive assets and by enabling effective surveillance within the structure. In addition, providing the necessary access routes and emergency equipment enables successful facility evacuation and emergency response.

This section describes the factors a transit agency might consider when designing the interior layout of the site. These include asset shielding, surveillance, and emergency routes.

6.2.2.1 Asset Shielding

A building's layout can be used to shield critical areas such as a central-control room, or vulnerable areas such as a station platform packed with people, from an attack at the outer edge of the site.

Agencies should consider using special reinforced materials between valuable features and easily accessible areas, such as lobbies, mailrooms, and loading docks, or locating these areas at a distance from each other. For example, designers may consider positioning a control room at the center of a building, behind layers of other non-public areas, and at a distance from a likely detonation point in case of an attack. Within a room, planners may be able to reduce the vulnerability of personnel and critical equipment by positioning them away from windows and doors. Critical assets might be dispersed so that they cannot be disabled by a single attack, and locate redundant or back-up systems in a different building, or even at a different site, if possible.

Agencies should consider using a facility's layout to help enforce zones for each type of activity taking place, to safeguard the nonpublic areas of a site. Public areas such as train platforms or lobbies can be separated from non-public spaces intended only for staff; and access management elements (such locked doors, checkpoints, etc.) may help prevent unauthorized movement between the zones. Agencies can insulate particularly sensitive non-public facilities from the public using other, less critical non-public spaces.

Agencies should also consider making pedestrian movement within the facility consistent with the access management tools in place. Signage and other pedestrian flow controls can direct public users away from non-public spaces. Separate entrances and routes can be used for the public and staff within the building wherever possible; this minimizes the opportunity for someone to gain unauthorized access to secure areas of the facility.

6.2.2.2 Surveillance

Public spaces can be designed to facilitate surveillance—a key CPTED principle—with large fields of vision and no blind spots or hiding spaces.

With clearly identified and understood zones of activity, staff and the public can more easily identify unauthorized people and suspicious behavior. Designers should try to avoid creating blind corners, isolated passageways, as well as columns and other sightline obstructions.

6.2.2.3 Emergency Routes

Emergency routes within, to, and from all areas of the building serve two purposes: evacuation of staff and the public, and access by responding agencies. Appropriate emergency routing is critical to safety and can vastly reduce the impact of an unexpected event.

Agencies should consider making emergency routes an integral element of a building's design and factor in the following principles:

- Locating corridors and stairways making up the routes away from likely areas of attack and reinforcing them to resist damage in an explosion or fire.
- Devising evacuation routes that are clearly marked, unobstructed, and adequately sized for the occupancy level of the building.
- Designing routes and protected "safe areas" to accommodate wheelchair users and other occupants with special needs.
- Providing multiple evacuation routes, in case the primary exit becomes damaged or blocked.
- Locating critical routes and systems that are logical and consistent with other buildings and the surrounding area, since during an emergency, authorities must be able to quickly access to the building and the on-site emergency equipment.

6.2.3 Structural Engineering

Structural engineering, or structural design, is the design of a building's internal support system. Structural design includes the selection of a framing method or structural system, as well as the selection and sizing of structural members, based on loading and architectural requirements. Structural members include beams, columns, the foundation, floor slabs, connections of these elements to each other, and other ancillary components.

Building design (structural and architectural) can contribute to infrastructure security by minimizing the extent and depth of damage in an attack. Structural integrity can help mitigate blast and fire damage to the building; protect inhabitants; protect equipment, property, and records; allow critical operations to function immediately after an attack; and allow rescue operations in and around the building preserved after an attack.

This section focuses on blasts and fires, describing engineering concepts for structural integrity and strategies for minimizing damage. The concepts discussed include:

- Blast loads
- Blast damage
- Progressive collapse
- Blast mitigation
- Fire damage

The sections of most building codes relating to structural components address service loads and methods to determine the proper size of structural members and their connections. Service loads specified in building codes are based on the location and intended use of the proposed structure, and include:

- *Minimum dead load*: the weight of the structure
- *Live load*: variable loads such as people, cars, furniture, etc.
- *Earth load*: earth pressure on buried structures, retaining walls, foundations, etc.
- *Wind load*: pressure applied to the structure by wind
- *Snow load*: the weight of snow on a building
- *Seismic load*: loads induced on structural members during an earthquake

Building codes do not usually address "blast loads"; the force exerted on a building from the detonation of an explosive device.

Blast loads are different from the usual types of service loads considered by a structural engineer when designing a building. Service loads are relatively predictable in their magnitude and placement on the structure. In contrast, blast loads are much greater in magnitude, are unpredictable in size and placement. However, there are certain engineering strategies that agencies can use to enable a building to maintain its structural integrity after some of its components have been compromised or completely destroyed in a blast.

6.2.3.1 Blast Management

Blast Loads

A bomb exploding at ground level produces a hemispherical shock wave. As with other waves, such as sound waves, the shock wave can reflect off objects, concentrate in confined areas such as tunnels, or change direction. This is important to understand because once the skin of a building is breached, the shock wave can travel or ripple through a building's corridors as the energy in the wave dissipates.

Table 6-1. Bomb Size and Blast Range

Type of Explosive	Explosive Capacity in TNT Equivalents	Lethal Air Blast Range
Pipe Bomb	5 lbs. (2.3 kg)	
Briefcase, Backpack, or Suitcase Bomb	50 lbs. (23 kg)	
Compact Sedan (in trunk)	500 lbs. (227 kg)	100 ft. (30 m)
Full Size Sedan (in trunk)	1,000 lbs. (454 kg)	125 ft. (38 m)
Passenger or Cargo Van	4,000 lbs. (1,814 kg)	200 ft. (61m)
Small Box Van (14 ft box)	10,000 lbs. (4,536 kg)	300 ft. (91 m)
Box Van or Water/Fuel Truck	30,000 lbs. (13,608 kg)	450 ft. (137 m)
Semi-trailer	60,000 lbs. (27,216 kg)	600 ft. (183 m)

Source: Transportation Security Working Group, "Terrorist Bomb Threat Standoff (Card)," Government Printing Office (1999).

A bomb or other explosive device produces a blast that creates a blast load. Explosions cause damage by the generation and propagation of heat, pressure, and flying debris (shrapnel). An explosion is a rapid, often violent, release of energy that produces a rapid release of gases and heat. The rapid release of gases compresses the air immediately around the bomb, creating a shock wave. This shock wave, or pressure wave, propagates through the air outwards from the explosion. When this shock wave encounters an object, such as a building or a trash receptacle, it exerts a force on that object. The magnitude of these forces can be tremendous: a 74 mph wind (threshold hurricane wind speed) produces a pressure of approximately 21 psf (0.1480 psi); in contrast, according to Tod Rittenhouse, "the blast pressures exerted on the building façade in the Oklahoma City bombing were on the order of 4,000 psi."[33] Ranges for various types of explosives are further described in Table 6-1.

The blast load striking a building or other object depends on the amount and quality of explosive detonated and the distance of the explosion from the building. Maximizing standoff distances is important; the farther away an explosion, the weaker its effects. As the shockwave radiates away from the explosion, the magnitude of the shockwave decreases and the duration of the shockwave increases. (See Figure 6-3.)

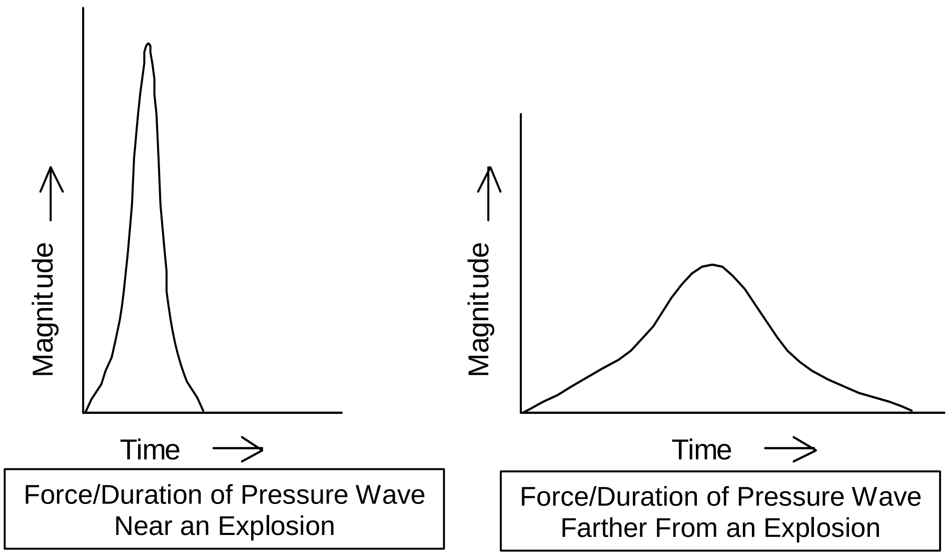
[33] "Designing Terrorist-Resistant Buildings," Tod Rittenhouse, *Fire Engineering* (November 1995).

The peak magnitude of the shockwave increases by a reflection factor as it encounters the face of a building. This increase in magnitude is analogous to ocean waves rising as they strike a sea wall and the water "piles up" against the wall. The reflection factor varies with the incident angle (the angle at which the shockwave hits the building). The increase is maximized when the direction of wave travel is perpendicular to the building. This can increase the pressures by an order of magnitude.

Explosive materials vary in their efficiency (energy released per pound of material). In calculating blast loads, current practice expresses all explosives in terms of an equivalent weight of TNT, regardless of the actual explosive material used. Information for determining blast load magnitudes in relation to building hardening design is available through the Department of Defense, General Services Administration, and in other security-related publications.

Damage from Blasts

The main threat to the structural integrity of a building is blast force, regardless of whether the explosion occurs inside or outside the building. The primary vulnerability is the overloading of the structural system by blast loads that cause the system to fail and the building to collapse.



Force/Duration of Pressure Wave Near an Explosion

Force/Duration of Pressure Wave Farther From an Explosion

Figure 6-3. Variation of Explosive Pressure and Duration with Distance from Explosion

Blast damages are classified as either direct (those that occur in the explosion) or indirect (those that occur as a subsequent consequence of direct damage).

- Direct Damage
  - A hole in the ground or foundation.
  - Localized damage to the building's façade (bricks, windows, signs, etc.).

  - Damage or removal of a structural member or members (a beam, column or other structural element) directly caused by the blast.
- Indirect Damage
  - Flying shards of glass: Glass shards thrown from a window can cause serious injury to people, even if they are several feet from the window that shattered.
  - Flying debris: If the force of the explosion breaches the building's façade (building skin, curtain wall), the energy not absorbed by the façade can hurl furniture and other light objects. These "missiles" can cause injury, damage property, and rupture service systems such a gas, water, electric and communications.
  - Progressive collapse: If a blast directly destroys a column or beam locally, other structural members may fail. This can start a chain reaction of failures that results in damage disproportionate to the blast and collapse of the entire building.

Progressive Collapse

The worst-case consequence of blast damage related to structural engineering is progressive collapse. This is the disproportionately large collapse of a building or structure from an explosion, caused by the loss of one or more structural members, resulting in only localized damage. Progressive collapse occurs because most buildings are designed to carry the required loads, based on the assumption that all structural members are in place.

Two types of progressive collapse are possible:

- Pancaking is the stacking of floors on top of each other. It occurs when an explosion destroys a structural member or members, causing the floor directly above the destroyed members to collapse, which causes the next floor above it to collapse, and so on.
- Cascading is the collapsing of a series of bays (the section of a building between two rows of columns) from the destruction of one or a few bays. Cascading occurs when an explosion destroys a bay, or bays, causing the adjacent bay or bays to collapse in succession.

Progressive collapse occurs in stages, as summarized below. A complete discussion of progressive collapse is beyond the scope of this report; for more details refer to the latest edition of ASCE Standard ANSI/ASCE 7, *Minimum Design Loads for Building Structures.*

Beams (Including Girders)

Beams are horizontal structural members that support the floor slab. They carry gravity loads and are typically supported by columns or girders. Transfer beams or girders can support floor slabs, other beams and other columns. Beams and girders also provide lateral support to columns to prevent the columns from buckling.

When an explosion destroys a column, the supported beams lose their support at the destroyed column and become cantilever beams. If the beams are connected to the remaining columns with non-rigid connections (connections unable to transfer bending loads from a beam to a column), all beams previously supported by the destroyed column will collapse along with the floor slabs those beams support. This can extend through several stories. The loss of these beams can also reduce the lateral stability of the adjacent columns not damaged by the initial blast, causing those columns to fail, followed by more beams, and so on.

Floor Slabs

Floor slabs are typically designed to carry gravity loads. Sometimes the slabs are designed as diaphragms and are part of the lateral support system.

When the shockwave enters the building through an open window or breached curtain wall, it can exert an upward load on the bottom of the slab, causing the slab to fail. The loss of the slab can increase the unbraced length of the adjacent columns, potentially causing the columns to buckle. Failed columns can result in collapsed beams and the other consequences discussed above.

Columns

Columns typically carry axial gravity loads and are usually not designed to bend. When columns are part of the lateral resisting system, bending is taken into account. The strength of a column is limited by its length and by the size and shape of its cross section. If the unbraced length of a column (the distance along the column between horizontal members) increases due to the loss of a beam or slab, the strength of the column is reduced.

If an explosion destroys a perimeter column or columns, the girders and beams supported by those columns lose their support. This may increase the unbraced length of the adjacent columns due to the failures described above.

Blast Mitigation

The best methods of protecting a building from blast damage are effective access management techniques and appropriate standoff distances. Since no security system is foolproof; however structural engineers need to anticipate that buildings may be subjected to blast forces. Structures designed to resist catastrophic effects from blast forces are referred to as "hardened" buildings; these use a combination of structural design, architectural design, and mechanical design to minimize the consequences of a blast.

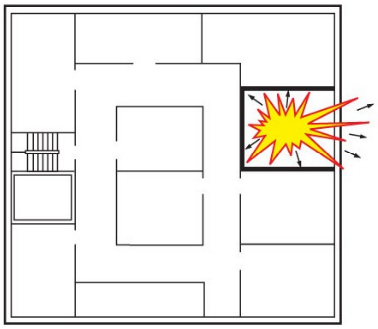
Constructing hardened structures can be expensive and time consuming, particularly when retrofitting an existing building. One possible alternative is to add redundant structural components to a building, although this approach can be just as expensive. Before hardening a structure, a transit agency should consider whether such an approach is necessary.

Avoiding Progressive Collapse

Agencies should consider designing buildings to sustain localized damage, including the total loss of multiple structural members, and still remain standing. Designs should take into account the stability of a structure if the structure loses a column or columns, a bearing wall, a beam or a combination of structural elements. Design techniques that help prevent progressive collapse include:

- Stiffening the perimeter frame by designing it as a rigid frame.
- Strengthening floor slab systems to distribute and sustain a load by catenary action to account for the loss of a column.
- Designing floor slabs to span in a direction in other than normal conditions (a lower factor of safety may be used for the secondary span condition).
- Designing load-bearing partitions to accept loading when slab spans change direction.
- Increasing the load capacity and ductility (ability to deform without breaking) of beam-to-column connections.
- Building returns (an angled section of wall at the free-standing end of a wall) on walls to increase their stability under suddenly increased loads.
- Reinforcing and tying walls and slabs together, allowing them to act respectively as the web and flanges of a beam to compensate for the loss of other structural members.

Underground parking presents an opportunity for a car bomb or other similar device to be placed under a building, and agencies should consider avoiding this design feature. When underground parking facilities are warranted, agencies can use structural design modifications. For example, columns in the garage can be designed for a greater unbraced length: double the unbraced length for one level of parking, triple it for two levels of parking, and so on.



Hardening vulnerable areas, such as a lobby, can protect other parts of the building from an attack.

Figure 6-4. Isolation of Vulnerable Areas

Agencies should consider structurally isolating sections of the building from each other, to prevent substantial damage in one area from causing a progressive collapse in other areas (see Figure 6-4). This compartmentalization serves two purposes. It can buffer high-risk areas (mailrooms, public lobbies, chemical storage areas, or other areas where an explosion is more likely to occur), from the rest of the building, so the destruction of such an area does not result in the total collapse of the building. It can also provide extra protection for critical rooms and equipment, such as control rooms, communications rooms, and staffed areas, so these remain structurally sound if a blast occurs elsewhere in the building.

6.2.3.2 Fire Management

While accidental fires may occur, fires resulting from an attack may have a different kind of impact. For example, an accidental fire usually starts at one location and often, but not always, spreads relatively slowly. On the other hand, a fire from arson is often strategically set in multiple locations to maximize the rate of spread and damage. An arsonist may also sabotage the fire protection system. An incendiary bomb that produces a fireball or intense heat (as opposed to a bomb that produces only a shock wave) ignites a large area and can cause substantial damage, including local damage to the fire suppression system.

Well-established design and construction practices for protecting structural members from fire are particularly important in case of an attack. Although not all structural materials will "burn," all structural members, regardless of their material composition, will lose a percentage of their original strength when subjected to intense heat. Excessive heat is the principal cause of a fire's detrimental effects on a structure. Therefore, upgrading or hardening the automatic sprinkler system is of tremendous benefit in mitigating the effects of fire on a structure. Additionally, many of the mitigation measures for blast impacts apply to fire management as well, such as isolating vulnerable areas to prevent the spread of fire and avoiding progressive collapse (see **Figure 6-4**).

This section discusses the effects of fire on four major structural construction materials: steel (structural steel), reinforced concrete, pre-stressed concrete, and timber.

Steel

At high temperatures, unprotected steel looses its strength. For this reason structural steel members used in building construction are protected (fireproofed). Fireproofing methods to protect steel members from heat insulate the steel from the fire. This increases the time required for heat to transfer from the fire to the steel.

There are several insulating methods for steel members:

- *Concrete encasement.* Encasing steel members in concrete provides excellent insulation to the steel. Lightweight concrete (see the About Concrete illustration on the next page) provides better insulation than standard concrete. The selection of concrete type depends on several design factors that are beyond the scope of this document. This method is well suited to insulating columns. It may also be used to insulate floor beams supporting a concrete floor slab. However this can be expensive due to complicated forming and increased dead load.
- *Sprayed on mineral fiber coatings.* Mineral fiber coatings are easy to apply, and they provide excellent protection when applied correctly. However, these coatings are easy to scrape off, and explosive blasts may damage portions of the insulation. Protection of the insulation is discussed at the end of this section.

- *Cementitious material coatings.* Cementitious coatings form a continuous coating around the steel. However, during a fire, they can spall (chip or flake on the surface), and there is a history of problems with lack of adhesion to the steel.
- *Intumescent paints and coatings.* Intumescent coatings swell when heated, thereby insulating the steel and retarding the effects of the flames and high temperatures. These coatings work well to protect the steel from heat. Exposure to flames can damage or destroy this type of coating and therefore should only be applied to components unlikely to be directly exposed to flames.

There are several concerns when selecting a method to fireproof steel, including method of building construction, and installation and maintenance costs. During a blast, it is likely that the fire proofing on the steel in the immediate vicinity of the blast will be damaged. However, the fire that may result (and spread) will have an effect similar to conventional fires. Assuming the progressive collapse considerations were used in design, protection of the remaining steel members will be effective.

About Concrete…

Concrete is a mixture of portland cement, coarse aggregate (stone), fine aggregate (sand) and water. Portland cement reacts with the water (hydrates) and hardens. The aggregate is basically used as filler (obviously the proportions determine the concrete's strength). The types of aggregate affect the properties of the mix. Lightweight aggregates such as vermiculite and perlite are used to create lightweight mixes as described above. Several other "admixtures" are available to modify the concrete's properties and even color. Admixtures include plasticizers to temporarily decrease the mix viscosity, agents to increase/decrease setting time, foaming agents and air entrainment.

Reinforced concrete is concrete embedded with steel rods to increase the member's strength (as distinguished from the material's strength). The steel reinforcement is usually placed were tensile stresses (tension) develop in the concrete member, although sometimes the steel is also used to reinforce compression zones.

Pre-stressed concrete is similar to reinforced concrete, except that the steel reinforcement are usually wire cables that are pre-tensioned *before* the members are loaded.

Reinforced Concrete

Concrete is often used as an insulating material. Although concrete structures rarely collapse from fire damage, the strength of concrete and reinforced concrete members is reduced by exposure to high temperatures. Type of aggregate and moisture content are the principal factors that determine concrete's sensitivity to heat.

Type of aggregate is the most significant factor. Lightweight aggregates such as vermiculite and perlite are used in lightweight concrete. Lightweight concrete, in addition to having better insulating characteristics, has better strength retention when exposed to intense heat.

The amount of moisture in a concrete affects the member's resistance to heat. The moisture is trapped in the small capillaries within the concrete. As heat energy is absorbed, the water in the concrete vaporizes, which locally helps maintain the concrete's strength until the moisture is burned off. However, voids left by the vaporized moisture weakens the area. Structural engineers should consider this when fire is a concern for concrete members.

Pre-Stressed Concrete

The relevance of aggregates and moisture content for pre-stressed concrete are similar to those for reinforced concrete. The concrete used for pre-stressed concrete members is usually stronger than the concrete used for reinforced concrete members and has better fire resistance, but tends to spall and expose the reinforcement.

Pre-stressing steel is the principal concern when exposing pre-stressed members to intense heat. High carbon-cold drawn steel used in pre-stressing is more sensitive to intense heat than low carbon, hot rolled steel used in reinforced concrete. Also, the loss of strength in pre-stressing steel is permanent and not regained upon cooling. For example, the pre-stressing steel is initially under great tension. Over time this tension decreases, as the steel tends to creep (continually deform or lengthen). This is taken into account during the design process; however exposure to high temperatures, exacerbated by the spalling concrete, accelerates this "creeping" process. Engineers should consider this when considering fire effects on building hardening.

Timber

Unlike steel and concrete, wood will burn. The principal factors that determine how timber responds during a fire are the size of the timber member and its moisture content.

As wood burns, a charcoal layer forms on the wood's exterior. This char layer is an insulator and as the layer thickens, it slows down the rate of burning. The unburned interior wood retains its strength. Buildings constructed with large timber members can maintain their integrity for a long time during a fire, providing an opportunity for the fire to be extinguished before structural failure occurs. As is in all cases, but especially for timber construction, a hardened sprinkler system is important. Fire retardants can slow combustion and delay ignition of wooden members.

6.2.4 Architectural Features

The design of architectural features on a site can aid in surveillance, help deny an opportunity for an attack, and reduce injuries and property damage in case of an event.

This section describes the factors a transit agency might consider when designing security features into a site. These include:

- Façade
- Entrances
- Fenestration
- Small architectural features
- Utility openings

- Signage

6.2.4.1 Façade

A façade is the outside face of a building or wall. It can refer to just the outer surface, or more generally to all construction between the exposed surface and the structural frame. In some instances, the structural frame is visible as an integral part of the façade.

Materials

Façade design affects a building's resilience to terrorist attacks and other incidents. Designers can construct a building façade with materials that resist fire and produce little or no toxic fumes or minimal debris in an attack. Materials that ignite and spread fire quickly or produce toxic fumes, such as plastics, paints, and other finishes can trap building occupants and cause suffocation or other consequences.

Façade materials can be attached in a manner that will reduce the amount of secondary debris. Masonry or pre-cast concrete panels can be reinforced and securely fastened to the building frame. Bricks or other face materials that come loose in a blast may become projectiles and cause secondary damage. As with progressive structural collapse (refer to the subsection on progressive collapse in Section 6.2.3.1), façade design should prevent indirect damage that destroys the entire facade. On sides of the building that face likely directions of attack (such as public streets or nearby buildings), agencies should consider minimizing the use of weaker materials and/or openings. Overhanging design features should also be avoided where they could receive a blast load from underneath.

Façade features can also impact visibility; elements such as light color schemes, translucent canopy materials, and skylights provide more light in interior spaces. Transparent materials like glass may provide added opportunities for surveillance, allowing transit employees and passengers to see from one zone of a facility to another and to share light from one area to the next. Conversely, solid materials such as concrete block walls may prevent potential attackers from observing facility activity patterns at non-public locations such as maintenance facilities, compared to chain link fences, which allow unhindered observation.

Decontamination

Incident recovery may also be relevant to consider when choosing materials. Weapons of mass destruction, such as chemical or radiological agents, can be absorbed into materials such as concrete and plastics. Non-porous coatings may be able to minimize absorption of chemical contaminants when applied to porous materials like concrete or brick. Agencies should consider decontamination efforts—whether cleaning or removal—when choosing façade materials, and perhaps even consider comparing the extent of the decontamination effort required for the material options before settling on a selection.

In response to the anthrax attacks at the Hart Senate Office Building and Brentwood Post Office, gaseous chlorine dioxide gas was pumped through the buildings' heating and ventilation systems and kept inside the buildings for 9 to 12 hours to ensure that all spores were killed. Liquid chlorine dioxide and other antibacterial gels were also used and potentially contaminated mail was irradiated before being sent to its destination. The Hart building was closed for three months while cleanup and testing was completed. The estimated costs for cleaning the 700,000 square foot Brentwood postal facility were $22 million.

6.2.4.2 Entrances

Agencies should consider locating entrances to the building, including main lobbies, service entrances, and loading docks, away from uncontrolled public spaces whenever possible. This reduces the opportunity for a direct attack on an entrance. Agencies should also consider locating exterior entrances where there is no direct access to key assets (such as OCCs) within a building.

The sizes of doorways and lobbies should be appropriate for the access management techniques used on-site. For example, at security checkpoints that span entryways it is extremely difficult to bypass them without detection, and in larger lobbies additional security staff may be required.

6.2.4.3 Fenestration

Fenestration is the design and arrangement of windows and other glass features on a building, including glass façade panels and openings. The location and construction of windows will likely vary, based on the location and contents of a building.

Designers may reduce the number of windows around sensitive or valuable assets, to make those assets less visible to the public and to minimize damage in the event of an attack. For facilities with large fenestrated areas, designers may compensate by incorporating standoff distances and orienting the windows away from unsecured areas. Where possible, agencies should consider locating windows out of convenient reach and use security screens or wire mesh to prevent unauthorized access through the opening.

Agencies should consider using windows and frames constructed of materials that resist tampering and easy destruction, and that prevent flying glass shards in an explosion. For example, tempered glass or polycarbonate composites that shatter cleanly (such as those found in automobile windows) may prove safer than conventional annealed glass that breaks into dangerous shards. Planners might also consider window treatments, including adhesive films, coatings, and blast curtains that limit the depth of in-room damage from shattering window glass.

6.2.4.4 Small Architectural Features

Agencies should incorporate small architectural features or amenities, such as planters, benches, and trashcans, in the facility design in such a way as to prevent them from causing damage in a blast. Anchoring objects made of blast resistant, reinforced materials to the ground will make them less likely to act as projectiles and cause secondary damage.

Agencies can also incorporate these design elements into access management techniques, such as barriers for vehicles, but should also be cognizant of not placing them in a location that could provide hiding spaces or shielding for potential attackers, especially near entrances or critical assets.

6.2.4.5 Utility Openings

Many buildings require numerous functional openings, such as utility tunnels, sewers, and HVAC vents, which provide the potential for unauthorized access or the introduction of harmful substances into a structure or tunnel.

Agencies should consider locating openings in inaccessible locations or where any suspicious activity would be easily observed to protect the openings. Security doors, hatches and grilles should resist tampering or damage and can be sized to prevent entry by a person or the introduction of harmful substances. In some cases, additional monitoring or surveillance equipment may be justified.

6.2.4.6 Signage

Signs are effective tools for access management and for assisting people unfamiliar with the building. They can direct public users to proper areas of the building, warn against unauthorized entry into nonpublic spaces, and indicate emergency evacuation routes.

Signs can also inform and instruct visitors on proper and improper activities within the building or facility. In some cases, transit agencies may consider reducing or eliminating signage for key assets, to hinder their discovery by potential aggressors. All signs should be legible and easily discernable to all passengers, including those with disabilities.[34] Emergency exit signs can also be designed with lighting elements, to make them visible in the dark. Agencies should consider designing signs in public areas to resist tampering or destruction, and, when placing signs on walls or other surfaces, should avoid adhering them in a way that allows items to be hidden on, in, or between the sign and the surface.

6.2.5 Systems and Services

Building services create a safe and comfortable environment for occupants and enhance a building's functionality. Individual systems have many similarities and may rely on shared or auxiliary systems for part of all of their service. In addition to having similar attributes, they also have many parallel vulnerabilities and countermeasures.

This section describes the principal systems and services in a transit building. These include:

- Public utilities

[34] All signs, emergency facilities, and any security measures should be compliant with the American with Disabilities Act (ADA).

- Electrical system
- Functional components[35]
- Heating, ventilation and air conditioning (HVAC)
- Lighting
- Communications
- Security systems
- Water and sewer
- Fire protection

Many of these services are vital to emergency response and may be targets of terrorism themselves. Consequences of building service disruptions can range from inconveniences to the public and the transit agency to a total shutdown of the system and potentially dangerous conditions. If the building services and utilities are required for emergency response, then willful disruption of these services may supplement the primary attack.

6.2.5.1 Public Utilities

Most transit systems receive electric power from public/private utility companies through the normal public transmission system. Transit agencies also rely on public gas and water supplies. The location of these utilities is public information that can be easily obtained by anyone.

Damage to power and gas lines can cause major disruptions at transit facilities. External utility lines for all services and systems need to be protected and monitored to prevent tampering. Natural gas lines are of particular concern because of the explosive nature of their contents.

Utility lines within transit buildings may also be targets of terrorists and agencies should consider their placement as part of the building design. Perimeters and parking garages are vulnerable to large explosions and vehicle ramming. Keeping utilities away from these areas reduces the risk of additional destruction or loss of critical emergency systems. Agencies should consider concealing and protecting all utilities to the greatest extent possible.

6.2.5.2 Electrical System

Agencies should consider facility backup power sources in case of a local or regional power failure, and identify those systems requiring emergency power in the event there is an outage.

Backup power can consist of a generator that uses fuel to create electricity or a battery that can store enough power to act as a supply in an emergency. Agencies should consider regular maintenance

[35] Building services use functional components such as wiring, mechanical equipment, switchgears and alarms that manipulate system inputs to produce the desired outputs. The only human interaction with functional components should be by maintenance or operational staff as these components are not part of the public interface.

checks to ensure backup power is operational. It is important to locate backup systems far away from the primary systems so that they are not damaged by incidents affecting the primary systems.

6.2.5.3 Functional Components

Control systems include electrical and mechanical equipment such as switchgears, alarms, sensors, meters, and other associated equipment used to coordinate other systems' functions and monitor their performance. Tampering with these controls can halt operations and compromise emergency response and evacuation.

Distributed control systems (DCS) are used to monitor whether the system is working properly, make system adjustments when necessary, and shut down the system if problems are identified. DCS can be integrated into ventilation, communication, and security systems, and located adjacent to other control components. They can be connected to an integrated facility communications system as an alarm system to notify system monitors of malfunctions or unusual activity.

Access to the control components is needed for maintenance but agencies should consider using appropriate access management controls to protect these components, and not leave them out in the open. They should also consider locating mechanical rooms away from the building perimeter, loading docks, and parking garages that are vulnerable to attack.

6.2.5.4 Heating, Ventilation and Air Conditioning (HVAC)

HVAC systems create a climactically comfortable environment and ensure air quality is adequate by regulating temperature and humidity, and filtering and replacing stale inside air with fresh outside air.

Miscellaneous Openings - refer to Section 5.3.9

While some buildings provide sufficient natural ventilation to remove carbon dioxide and other pollutants generated indoors, many buildings require mechanical ventilation systems to provide conditioned air by filtering, exchanging with outside air, and temperature and humidity control. Air vents collect air from outside; fans and ducts distribute it throughout the building and vent the "used" air out of the building.

Ventilation

Heating and cooling systems may be used in conjunction with ventilation systems to keep indoor temperatures comfortable. Transit buildings, such as open garages and above-grade stations, may not have mechanical HVAC systems since they have sufficient natural air transfer, while ventilation systems are a key component of tunnels and underground facilities.

Air vents may be used to gain access to the building if not properly located and secured. A terrorist could enter a facility through the vent shaft or use the opening to disperse weapons of mass destruction throughout the facility.

Agencies should consider designing HVAC systems to reduce the potential for break-in. Some techniques that can be used include:

- Designing vent shafts to have minimally sized openings.
- Securing doors and grates on ventilation systems accessed for maintenance.
- Locating vents away from areas with public access, such as sidewalks or medians, wherever possible. It is especially important they are not located on roadway gutters or other low spots, where oil spills or floodwaters could enter.
- Locating vent openings high up where they are out of reach.
- Installing actuated louvers over vent openings that open only while the fans are running.
- Monitoring vent openings with alarms and intrusion/tamper detectors to alert officials of the presence of humans or chemical substances.
- Installing sensors in vents to detect foreign substances in the ventilation systems.

Smoke and Fume Control

In addition to the vulnerabilities the HVAC system creates, it can also play an important role in smoke and toxic fume removal, especially for large or underground facilities. Agencies may use separate or auxiliary ventilation systems for smoke and fume control.

HVAC systems can create "safe zones" in buildings for occupants who cannot leave via emergency routes. Safe zones work by creating areas of higher pressure to keep fumes and smoke out until properly equipped rescue workers can assist the trapped occupants. It is important that these systems have backup power supply and can be manually controlled safely during emergency situations.

Fuel Oil/Propane

Some facilities, generally smaller ones and those in the northeastern United States, use fuel oil or propane for heating. Agencies should take into account that fuel storage locations and methods at these sites may cause security vulnerabilities.

6.2.5.5 Lighting

Lighting is an essential facility requirement, especially where buildings do not have adequate natural light or are used at night.

Surveillance

In addition to making buildings functional, lighting has a pivotal role in helping a facility prevent and recover from a terrorist attack. Appropriate lighting also creates a sense of security for people in the building. Without adequate light, surveillance, either human or mechanical, is limited in scope. Security and other personnel require light to clearly see what is going on around them and, more importantly, beyond their immediate area. CCTV and motion detectors also require adequate levels of illumination in order to detect suspicious activity.

Lighting should provide illumination of pedestrian walkways and eliminate shadowed areas where attackers could hide. The selected type of exterior lighting should cast consistent color throughout the site, so the video surveillance quality is clear. The lighting intensity (foot-candles/square foot) should be greater around critical assets.[36] Lighting should be compatible with the particular camera systems in use, and should be designed to provide a bright, even distribution of light to eliminates hiding spots.

Lighting can also be faced outward away from a building entrance, to produce "glare" that reduces the visibility of anyone approaching a site or building checkpoint at night and providing an advantage to security personnel on duty. However, when selecting and positioning fixtures agencies should consider the possibility of concealed injurious devices within fixtures or between fixtures and the surface to which they are attached.

Evacuation

Lighting also plays a key role in the evacuation of a facility when an emergency occurs. Building occupants need sufficient light to safely exit the building without tripping or falling into others. Backup power is important for ensuring a safe evacuation if the main power source has been affected.

Security lighting installation - refer to Section 5.3.2

6.2.5.6 Communications

Communications systems interconnect various areas of transit facilities, connect to other transit facilities, and link to outside connections, such as emergency responders and the local phone network. In addition to facility and passenger communications systems, security systems and DCS should be connected to a central location to quickly identify and set in motion the response to emergency situations. Agencies should consider backups of vital communications systems, preferably through a secondary type of network. Wire-based communications should be backed up by radio or cellular systems and vice versa.

Agencies should consider all of the following communications systems when building a new facility or when updating existing communications systems.

Pubic Address Systems

Public address systems play a vital role in providing information to facility occupants in the event of an emergency, especially when on-going emergency egress training is impossible, such as at public

[36] Site lighting levels must satisfy the established minimum recommended levels outlined by the Illuminating Engineering Society of North America (IESNA) and other applicable codes.

facilities like transit stations. Where feasible, agencies should provide clear audio and visual directions in an emergency situation to direct patrons to safe locations. Agencies can also connect fire alarms to public address systems to alert all building occupants of an emergency situation.

Call Boxes

Call boxes provide a direct communication, linking isolated parts of a facility to either on-site personnel or a remote security service. They are commonly sited where they can be easily found at stations and stops on the platform, outside the station building and/or in parking lots. These systems allow citizens to report incidents quickly without leaving the site.

Agencies should keep public call boxes in working order, even if they are rarely used, and should design and locate call boxes that are accessible to persons with disabilities. They should also consider providing training for all staff responding to these calls so that emergency calls are responded to promptly and helpfully. It is important that the public is aware there are public call boxes available for reporting incidents and that they feel confident they will receive an appropriate response from the agency.

Emergency Response

Communications systems not only provide on-site communications, but also connect facilities to transit administrators and emergency response teams. Agencies should consider providing field employees with direct lines of communication between supervisors, control centers and/or emergency response personnel. Customer service booths and building reception desks can also be outfitted with silent emergency alarm buttons to inconspicuously activate an emergency response if required.

Agencies can also network monitors and alarms connected to building services, operations and surveillance equipment into the security system. Streamlining the communications networks can ensure they are all being monitored so that a response can be implemented rapidly when an incident occurs.

Communications technology overview - refer to Section 8.3

6.2.5.7 Security Systems

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 for most agencies, the practice must be supplement 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, an agency 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.

***Surveillance systems overview* –** refer to Section 5.2.5

***Intrusion detection overview* –** refer to Section 5.2.6

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, theses 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. Agencies should consider how emergency responders can plug in locally to video feeds for on-site cameras.

When designing a remote surveillance system, it is important agencies 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. Agencies should 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.

Agencies can use these security measures 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 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.

6.2.5.8 Water and Sewer

Transit facilities typically receive their water supply from the public network. This water supply is critical for fire suppression, but localized sections of the fire sprinkler system may be damaged in a blast or other violent event. Agencies should consider designing the on-site water distribution system with reinforcements and redundancies, to ensure there is a continuous supply of water throughout a facility and that damage to one section does not incapacitate the entire system. Agencies should consider providing access to water gates, manholes, and control valves only within a secured perimeter, to prevent someone from cutting off the water supply to the facility. Likewise, storm water culverts and other drainage facilities should be within a secure perimeter, to prevent them from being used to access the site.

6.2.5.9 Fire Protection

Fire protection systems are designed to minimize harm to people and the structure in the event of a fire. Fire detection systems include smoke detectors and alarms. Sprinkler systems, standpipes, and chemical fire extinguishers are used to minimize fire damage while emergency ventilation systems and emergency exit routes allow inhabitants to exit the building. Flammability of construction materials, furnishings, and other materials stored on-site are also regulated to minimize the risk of a major fire. A compartmentalized structure that allows fire or contaminants to be isolated can also minimize risk. Such compartmentalization might be accomplished through various measures, including movable barriers or partition walls, fire doors, etc.

This information is intended to supplement existing codes and considerations on fire protection, rather than to replace such information. States and municipalities regulate minimum fire protection for different types of structures and facilities. Many of these regulations are based on National Fire Protection Agency codes and standards, which can be viewed in NFPA 130, Standard for Fixed Guideway Transit and Passenger Rail System.

6.3 Security Approaches for Types of Transit Infrastructure

This section describes different types of transit infrastructure and facilities that agencies maintain and operate as part of the normal functions of a transit system, from the most obvious and visible to the most remote. They include:

- Transit stations
- Transit stops
- Administrative buildings and OCCs
- Maintenance and storage facilities for transit vehicles
- Elevated structures
- Tunnels

- **Right of way, track, and signals**
- **Remote equipment and unmanned structures**

For each type of transit infrastructure, where applicable there are subsections that describe: potential threats, site analysis, access management, emergency response and egress, protecting critical assets, protecting vulnerable assets, structural engineering, facility services, and systems and services

6.3.1 Transit Stations

Transit stations are facilities where passengers board and alight from transit vehicles. They vary greatly in size and design, both across systems and within a given system.

This section focuses on the more elaborate stations that typically include enclosed structures, full-time personnel, and separate paid waiting area, such as underground subway stations and off-street bus terminals. Since transit stations are prone to a different set of threats than less elaborate "transit stops," the two facility types are discussed separately. (See Section **6.3.2** for security approaches for transit stops.)

A major security challenge at stations lies in **balancing the need for openness and convenience with the need to control the environment** in order to protect its users and system operations.

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. They may also have components that are underground or elevated, depending on the system. Since stations are designed for optimum passenger convenience and efficient traffic flow, they must be fully accessible and open as well as centrally located, often tightly integrated within a complex urban landscape.

Stations are typically divided into three 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 stalls).

Subsections describe:

- Potential threats
- Site analysis
- Access management

- Protecting critical assets
- Structural engineering
- Systems and services

6.3.1.1 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 are centrally located.

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. Fires may be particularly dangerous in those stations that are enclosed or underground, where people may become trapped and exposed to fumes and heavy smoke.

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.

Weapons of Mass Destruction

Stations that are enclosed or underground may be particularly vulnerable to a WMD attack, and may serve as an access point for an attack on an entire underground network. 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.

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.

6.3.1.2 Site Analysis

Since stations are situated in areas where large numbers of people live, work, and travel, they are often adjacent to public space, dense development, and other facilities that might not otherwise be considered security threats. However, site planners may be able to make some choices that improve security without compromising nearby facilities.

Facilities located above, below, or adjacent to the station deserve special attention, especially roadways, loading areas, vehicle-service areas, offices, and parking lots, all of which may serve as access points for explosive-laden vehicles or as vantage points. Surveillance by transit personnel and the general public and the ability to identify and respond to an emergency situation are key components of safety within the station setting; open layouts with wide fields of vision support this goal.

6.3.1.3 Access Management

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.

The following sub-sections present an overview of access management at transit stations for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management.*

Admissions Control overview – refer to Section 5.3.3

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, 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.

Perimeter Protection and Barriers overview – refer to Section 5.2.2

Vehicle Access

Agencies should consider how to minimize the potential for unauthorized vehicles to gain proximity to the station, crash into the station at a high speed, or enter the station through one of its entrances. Barriers to vehicle access need not be brick or concrete structures; natural elements such as trees and shrubs may also be appropriate depending on the location and configuration of the area.

Planners should consider locating key load-bearing structural components, as well as densely populated passenger waiting areas, away from areas that unauthorized vehicles can access. Design choices (the depth or height of the station, the dimensions of passageways between the street and the core of the station, and shielding passenger-waiting areas behind other structural elements) can mitigate the risk of a successful attack.

Transit vehicle entrances to the station can be limited to a small number of controllable access points. These entrances should be separate and clearly distinguishable from any public right-of-way or entrances, through the use of signs and/or channeling circulation. In addition, designers can use access controls, such as bollards, to limit the type of vehicle that may easily enter. Pedestrian entrances should be constructed in a manner that bars vehicles altogether or prevents access by vehicles other than maintenance or emergency responders.

In vehicle areas that must be close to the station, such as passenger drop-off areas, agencies should consider using traffic circulation tools to slow traffic, such as S-route curves, to minimize the opportunity for ramming (refer to Section 6.2.1).

Both passenger access and vehicular security are easier to manage when vehicle loading areas are segregated from passenger drop-off areas.

Vehicle Access Control and Parking overview - refer to Section 5.3.4

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.

Credentialing overview: refer to Section 5.2.4

Surveillance Systems overview: refer to Section 5.2.5

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.

Agencies 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. Stations should be equipped with emergency lighting, sprinkler systems and safe rooms, especially if there are subway or elevated platforms.

6.3.1.4 Protecting Critical Assets

Agencies should consider locating critical assets in transit stations, such as building systems and operations equipment, in secure locations with adequate surveillance. For example, mechanical rooms should be within a secure perimeter, and, where feasible within sight of station attendants or monitored by surveillance systems. Agencies should also protect the assets from attack by explosives by locating them away from the site perimeter, where explosions are more likely to occur, and should protect station platforms against access by non-transit vehicles, using different types of barriers.

The location of entrance controls and station attendants is important in protecting the facility. Locating controls and attendants at the outer edge of a building may enhance security of the entire site if these attendants have views of the surroundings. This may mean there are other areas within the station that do not have constant surveillance. If the station attendant is located at platform level, they can observe activity in this area, although this may leave stairways and corridors leading to the platform vulnerable.

If bicycle lockers are on-site, agencies should try to locate them away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials.

Building materials are critical in minimizing the impact of an attack. Qualities such as fire resistance and resistance to absorption of toxic materials can greatly reduce the work needed to recover from an attack. For more information on building materials, see Section 6.2.3.

6.3.1.5 Structural Engineering

Structural considerations for the station depend on the station design: elevated stations will have very different concerns than underground stations. The primary consideration for agencies should be to protect the lives of staff and riders during an attack. A design that has redundant structural elements to prevent progressive collapse in the event of an explosive blast, vehicle ramming, or fire can greatly improve the security of people in the building. (See Section 6.2.3)

Table 6-2. Security-Oriented Design Strategies for Transit Stations

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Structures set back from roads and parking areas, if applicable	Deter/Minimize	
Physical barriers such as bollards, road spikes, and fencing to enforce setbacks and/or prevent ramming	Deter/Minimize	X
Minimum number of vehicle entrances	Deter/Detect	X
Unobstructed sightlines surrounding the station	Deter/Detect	X
Interior Layout		
Interior station layout provides unobstructed sightlines, minimizing hidden areas or remote passageways	Deter/Detect	
Kiosks, ads, and information positioned to not disrupt sightlines	Deter/Detect	X
Minimum use of columns and blind corners	Deter/Detect	
Security mirrors on columns and corners	Deter/Detect	X
Operator booth positioned for maximum presence and visibility within station	Deter/Detect	
Critical assets buffered from public or vulnerable areas	Deter	
Non-public facilities hidden and not identified	Deter	X
ADA-complaint emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Critical equipment secured with gates, locks, or other access control measures	Deter/Detect	X

Design Feature	**Goal (Detect/ Deter/Minimize)**	**Able to Retrofit**
Dimensions of station entrances limit permissible vehicle size	Deter	X
"No Trespassing" signage	Deter	X
Posted or broadcasted instructions on how to report suspicious activity	Deter/Detect	X
Bright paint colors to increase ambient lighting	Deter/Detect	X
Vulnerable features designed to channel blasts	Minimize	
Shatter-proof glazing	Minimize	X
Façade materials that resist explosive blasts	Minimize	
Materials that do not absorb toxic substances when exposed	Minimize	Maybe
Fire-retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		
Appropriate surveillance at entrances, at access points to non-public areas, and throughout the station	Deter/Detect	X
Sufficient lighting for nighttime surveillance	Detect	X
Motion detectors or intrusion alarms on vehicle entrances	Detect	X
Intrusion alarms at access points to non-public areas	Detect	X
Communication links from remote station areas to station personnel (such as call boxes and a public address system)	Detect/Deter	X
Communication links to administrative and emergency response centers	Detect/Deter/ Minimize	X
Backup emergency lighting	Minimize	
Fire detection and suppression system	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

6.3.1.6 Systems and Services

Building systems play a critical role in transit stations because of the large numbers of people present, especially in enclosed facilities, such as underground stations. 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. Agencies should consider 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.

6.3.2 Transit Stops

For the purposes of this report, transit stops are considered separately from transit stations and more elaborate transit facilities. (See Section **6.3.1** for security approaches at transit stations).

Transit stops are facilities where riders board and alight from buses or light rail transit vehicles. These sites range from a simple signpost in the sidewalk indicating where a vehicle stops, to an elaborate transit plaza with sheltered waiting areas serving multiple bus routes or light rail lines. They are almost always at-grade, and may be located either right at the street curb or, in the case of larger sites, set back from the street on a dedicated parcel of property. Transit stops are often on public land, and have minimal facilities: signage, open shelters, lighting, and occasionally heating elements in colder locales. Although some transit stops have staffed information or fare-collection kiosks, most have no consistent on-site personnel.

The public nature of transit stops makes such sites easy targets for terrorist attacks. Worldwide, buses are the most frequently attacked transit vehicles,[37] and the sites that serve them are at risk by association. Although their high level of accessibility and lack of opportunities for security elements mean many of the techniques in this report cannot be implemented at transit stops, certain measures can be used to increase their level of security. These include improving visibility in and around transit stops, and using construction materials that resist damage in an explosion or collision.

There are three categories of transit stops referenced in this section:

- Curbside stops are waiting sites located on public streets. These typically have a signpost indicating the transit route, and may have some combination of lighting, a bench, or a partially enclosed shelter on the sidewalk.
- Transit plazas are separate parcels of land typically dedicated to light transit service, although transit vehicles access these sites from public roadways. These include off-street bus plazas and light rail stops serving one or multiple routes.
- Light rail stops reached by dedicated rights-of-way are typically at-grade. They may or may not be isolated from public roadways, and are therefore less accessible to public vehicles. Transit plazas and light rail stations often have basic amenities, such as shelters, a small concession stand, or a fare collection/information booth—staffed or unstaffed.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets

[37] "Protecting Surface Transportation Systems and Patrons from Terrorist Activities," Brian Michael Jenkins, International Institute for Surface Transportation Policy Studies (December 1997): p. 106.

- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.2.1 Potential Threats

Since most transit stops have limited staff or facilities, transit riders are the primary targets at these sites since the death or injury of riders would receive substantial media attention and provide a strong opportunity for a political terrorist statement. Attacks on light transit vehicles, especially buses, are the most common transit-related terrorism events, and the stops that serve these vehicles should take this into account in their design.

The following principal threats to a transit stop are intended primarily to harm the greatest number of transit riders as possible, but also to cause damage to the facility.

Explosives/Fire

Transit stops are easy, high profile targets for an explosive device. Since people tend to congregate at stops, they are attractive targets for prospective terrorists. The small size and lightweight construction of most shelters would require a small amount of explosives to achieve a high level of damage, and few if any measures are in place to prevent a bomb from being detonated at a transit stop. Such facilities are typically in public places, so there is also the potential to spread the collateral damage from a blast to adjacent properties.

Vehicle Ramming

The small size of most transit stop facilities means they could be severely damaged or destroyed by a vehicle collision. This threat is exacerbated by their open layout and close proximity to public roadways. Transit riders and staff need to be protected against the possibility of a non-transit vehicle intentionally colliding with people or structures on the site.

Weapons of Mass Destruction

Transit stops present an opportunity to use biological or radiological agents to harm not only transit riders, but an entire region as well. Since riders have a wide geographic range of destinations, a toxic substance with delayed effects can be released at a transit stop and inadvertently carried by riders to different areas of a city. This dispersal would help to maximize the harmful effects of the attack on the region as a whole, rather than concentrating the effects in a small area that could be contained and treated. Transit stops are less likely to be a target for this type of weapon than subway stations, since the latter have higher numbers of riders and present a more attractive target to terrorists.

6.3.2.2 Site Analysis

Agencies should consider several aspects of a site when determining appropriate security precautions. Most important is the site's relationship to the road, since this is the most likely direction of an attack. Agencies should consider designing and orienting on-site facilities both to provide clear views of the road(s) and to shield occupants from attacks. In most cases, views of approaching traffic are already incorporated into the site design (so riders can see arriving transit vehicles), but views of opposing traffic and adjacent land should also be considered. Adjoining properties and nearby buildings may be evaluated for their potential as hazards or protective buffers in an attack, and factored into layout and design considerations.

6.3.2.3 Access Management

The following sub-sections present an overview of access management at transit stops for perimeter security, vehicle access, human access, and emergency response and egress. Cross-references provide more specific information in *Chapter 5: Access Management*.

Perimeter Security

Perimeter security is largely impractical at transit stops. The public function of these sites means that people should be able to access them easily; any features that hinder approach will ultimately be seen as counterproductive to the site's primary function.

A transit agency may choose to establish a perimeter with limited access points around a stop, especially at transit plazas and light rail stops. This not only limits people to moving through entry points that are under surveillance, but can serve a safety function by separating pedestrian and vehicle traffic. Some larger facilities may have non-public areas to be secured against unauthorized access; these can have barriers around them to establish a small-scale perimeter.

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access Control and Parking overview: refer to Section 5.3.4

Vehicle Access

Vehicle access issues vary for each type of transit stop. At curbside stops, the transit vehicles share the roadway with public vehicles, and all vehicles (transit and private) must be able to access the site. Design features such as bollards can prevent a vehicle from ramming benches or a shelter, but any vehicle can get close enough to a curbside stop to inflict extensive damage with explosives. Agencies may consider using blast-reducing measures, as described in Section 6.2.3.1.

For bus lanes and transit plazas, where private vehicles are not allowed in the lanes intended for transit vehicles, the challenge is providing easy access for transit vehicles from public roadways, while preventing access by unauthorized vehicles. It is possible to equip exclusive bus lanes with automated gates triggered by a transmitter in each transit vehicle as it approaches, but this technology may be cost-prohibitive for many agencies and reduces the overall operating speed of the transit vehicles.

Light rail stations, especially those with dedicated rights-of-way, are typically more isolated from roadways than other transit stops. Where possible, barriers can be installed to prevent vehicle access from public roads and parking lots to the transit stop and right-of-way. These barriers can be designed to withstand impacts from vehicles while still enabling pedestrians to pass through.

Human Access

Transit stops are meant to be accessible to all people, so it is virtually impossible to prevent specific people from gaining access. These considerations are intended to increase the security of riders and staff in the facilities by increasing their ability to detect potential threats, rather than through access management.

When constructing staff booths used for fare collection or providing information, agencies should consider using mechanical locks, pass codes or key cards, and other access controls to resist tampering and forced entry. Booth orientation and design should provide staff with clear views of as much of the site as possible, for both surveillance purposes and staff safety.

Agencies should consider situating shelters for waiting riders so the interiors are visible to either an electronic surveillance system or to transit staff, including the drivers of approaching vehicles. The shelter design should eliminate potential hiding spots for bombs or other devices. Windows and cutouts should be located to allow users to view approaching traffic (both transit vehicles and others), and reduce the possibility of anyone approaching the shelters undetected; this may affect an agency's policy regarding billboards and other forms of advertising incorporated into shelters. Some transit systems (such as BRT systems) have paid fare areas to secure, but access management in these situations addresses scofflaws more than it addresses security risks.

Emergency Response and Egress

Every transit facility design must enable easy evacuation and response by emergency personnel in the event of an attack.

Agencies should consider a facility layout that facilitates the detection of a serious problem, with traffic lanes that are wide enough to permit access by responding personnel and vehicles. However, agencies must balance these needs against the goal of preventing access by unauthorized vehicles.

The design of any on-site enclosed structures (attendant booth, paid fare secure area, etc.) should ensure easy evacuation by riders and staff. Emergency exits must be appropriately located and well marked. Agencies should consider installing an integrated emergency call box to the transit agency or local police, with the transit stop name/facility number clearly displayed to enable quick identification.

6.3.2.4 Protecting Critical Assets

The principal assets at transit stops are riders and on-site agency staff. Facility layout can contribute to their protection by providing a high degree of visibility from the site into the surrounding area, sufficient lighting to detect any potential threats, and structural elements (such as reinforced shelters or traffic bollards) that shield occupants from likely directions of attack. Where possible, waiting areas, staff facilities, and any other assets should be set back from public roadways as far as possible.

If bicycle lockers are on-site, they should be situated away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials.

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.2.5 Structural Engineering

Agencies should design all structures at transit stops to resist damage or destruction. Passenger shelters, staff kiosks, and utility housings can be reinforced against accidental or intentional ramming by a vehicle and construction materials selected that minimize the amount of flying debris in an explosion (especially window material, which is more easily dispersed). Any street furniture such as benches or trash cans can be anchored to prevent them from becoming projectiles in a blast, and designed to redirect blast force in a safe manner, whenever possible.

6.3.2.6 Facility Services

Mechanical Systems

Most transit stops are too small to have substantial mechanical systems. The main exceptions are facilities with fare machines or on-site staff, normally in small booths. Agencies should consider installing communications equipment and basic HVAC capability in booths. Most mechanical systems will be relatively easy to access, but since they serve more of an accessory function within the transit system, their vulnerability merits less concern than other elements of the infrastructure. Agencies should consider housings for any on-site equipment that are durable and tamper-resistant and locate equipment, where possible, in view of riders or on-site staff to assist the detection of tampering attempts.

Electrical Systems

Some transit stops have basic electrical systems for lighting and, in colder locales, heating elements in shelters for waiting riders. At curbside stops, the city power lines serving streetlights often supply the electricity, meaning they are not under the direct control of the transit agency. In most cases, the size and open layout of transit stops make on-site backup electrical systems unnecessary.

Agencies should consider installing emergency communication equipment in as many transit stops as possible. This enables transit staff and riders to notify the agency of any emergency as soon as it occurs, increasing both the safety and security of the site. Call boxes can be located in rider waiting areas and on-site staff booths can have direct communication capabilities with the transit OCC.

Table 6-3. Security-Oriented Design Strategies for Transit Stops

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Unobstructed sightlines surrounding the stop	Deter/Detect	X
Physical barriers such as bollards and fencing to prevent ramming, or to prevent unauthorized access if the stop has a segregated transitway	Deter/Minimize	X
Interior Layout		
Kiosks, ads, and information positioned to not disrupt sightlines	Deter/Detect	X
Architectural Features		
Signage to deter non-transit vehicles from the stop area	Deter	X
Structural Engineering		
Structures and street furniture anchored to prevent being dislodged	Minimize	
Materials chosen to minimize flying glass and debris	Minimize	
Systems and Services		
Emergency call boxes to report incidents	Minimize	X
Adequate lighting for surveillance	Detect	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

6.3.3 Administrative Buildings and Operations Control Centers

Administrative offices and operations control centers (OCCs) 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.

These functions and activities may or may not be integrated into a single, centralized facility. A larger transit system may conduct administrative functions in a conventional office building (either entirely dedicated to the transit agency or shared with other office tenants), while operations control occurs at a specialized facility in a

> Administrative buildings and operations control centers might be strategic targets because of their important role in system operations.

separate site. For smaller transit systems, all the activities are often integrated into a single facility, and may be co-located with another facility such as a maintenance yard.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.3.1 Potential Threats

OCCs 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.

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 an OCC 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.

Arson

A fire, especially one deliberately set in a critical area of an OCC 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.

Tampering

Critical operations control and computer systems at administrative buildings and OCCs 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.

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.

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.

6.3.3.2 Site Analysis

These 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. Agencies should 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.

6.3.3.3 Access Management

The following sub-sections present an overview of access management at administrative buildings and OCCs for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management*.

Perimeter Security

OCCs 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.

Perimeter Protection and Barriers: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access Control and Parking overview: refer to Section 5.3.4

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.

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.

Admissions Control overview: refer to Section 5.3.3

Credentials and Credentialing overview: refer to Section 5.2.4

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.3.4 Emergency Response and Egress

To protect the people inside an administrative or OCC facility, agencies should consider incorporating emergency-detection systems and egress routes. One consideration unique to this type of facility is how to maintain maximum operability, even during an emergency. Designers may consider ways to seal off certain areas of the building from other areas, for example to prevent a fire from spreading to important operations equipment areas.

6.3.3.5 Protecting Critical Assets

Not all assets in a facility share the same vulnerabilities, and therefore may require different security measures. One way to address this is to create areas of varying security, or "layers of security," within a facility. This can be particularly effective in administration buildings and OCCs because it locates critical or vulnerable assets behind tight security, while minimizing the impact on daily operations that require less security. For example, entry lobbies and conference rooms are less critical targets than control rooms and document vaults. Planners can locate control rooms and document storage at the core of several "rings of protection" within the building, so that any attacker would have to cross increasingly stringent controlled-access areas in order to reach a critical target. For more information refer to Section 5.1.5.4.

If bicycle lockers are on-site, agencies should try to locate them away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials.

6.3.3.6 Structural Engineering

Planners should consider the full effects of various blast loads, fire, and ramming when designing the building to protect employees, as well as the areas that are critical to operations. Critical facilities can be "hardened" (see Section 6.2.3) to resist these types of threats. Glazing materials are a particular concern, since an administrative office building may face adjacent unsecured buildings on multiple sides.

6.3.3.7 Facility Services

Administrative and OCC facilities provide a variety of services to make the building a comfortable workplace. While all of these services impact security, some services warrant special treatment because of the function of the facility and the associated security concerns.

Certain areas of a building may call for heightened fire protection measures, such as erecting fire doors to seal off an area or installing sophisticated detection and extinguishing systems. The ability to provide uninterrupted power to the facility after an attack is of critical importance. Power lines into the building should be secured and planners may consider redundant power sources as well as on-site generators. Communication equipment may also deserve special attention on OCC sites. Communication systems may be critical for security and for operability throughout the transit agency's network, and agencies should consider protecting any critical communication conduits or receivers from attack and incorporating redundancy.

Table 6-4. Security-Oriented Design Strategies for Administrative Buildings and OCCs

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Inconspicuous facility location	Deter	
Co-location with facilities having similar security needs	Deter	
Securable perimeter	Deter	
Structures set back from roads and parking areas	Deter/Minimize	
Physical barriers such as bollards, road spikes, and fencing to enforce setbacks and prevent ramming	Deter/Minimize	X
Minimum number of access points necessary	Deter	X
Building entrances facing away from unsecured areas	Deter/Minimize	
Unobstructed sightlines surrounding the building	Detect	X
Interior Layout		
Building layout provides unobstructed sightlines, minimizing hidden areas and blind corners	Deter/Detect	
Critical assets buffered from public or vulnerable areas	Deter	
Zones of activity segregate building uses	Deter/Detect	maybe
Ability to isolate critical areas and maintain operations	Minimize	maybe
ADA-compliant emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Critical equipment secured with gates, locks, or other access control measures	Deter/Detect	X
“No Trespassing” signage	Deter	X
Vulnerable features designed to channel blasts	Minimize	
Shatter-proof glazing	Minimize	X
Façade materials that resist explosive blasts	Minimize	
Fire retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Redundant OCC off-site	Minimize	X
Sufficient lighting for nighttime surveillance	Detect	X
Appropriate surveillance and access management system at entrances and throughout the facility	Detect/Detect	X
Backup power supply	Minimize	X
Backup communications system	Minimize	X
Backup emergency lighting	Minimize	X
Fire detection and suppression system	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

6.3.4 Maintenance and Storage Facilities for Transit Vehicles

At transit maintenance yards and storage facilities transit vehicles are serviced for cleaning, fueling, maintenance, and repair; and vehicles are stored when not in use. The site may include fleet vehicle parking areas; garages where vehicles receive regular inspections and service; maintenance yards where substantial vehicle repairs occur, and where partially assembled vehicles are housed; fuel-storage facilities (either underground or above-ground tanks); and administrative offices. There may be lounges for off-duty drivers and offices for supervisors whose work is based out of the maintenance yard rather than the transit system's operations and control center. Some sites may also house a secure fare-processing facility, as well as training facilities for operators and other field workers. Maintenance yard and storage facilities may be co-located with a station or operation and control center.

Thoughtful design of vehicle maintenance and storage facilities can help prevent unauthorized site access.

This section focuses on-site security for these facilities, including access to stored vehicles on the site, but does not address vehicle design. Refer to Section 7.4 for rail and bus vehicles security-oriented design considerations.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.4.1 Potential Threats

Maintenance and storage yards typically have few on-site staff, but house numerous vehicles, equipment, and stored fuel. Vehicles and fuel are the most likely targets for terrorist attack. Agencies should consider focusing security precautions on preventing unauthorized access to parked vehicles and fuel-storage areas to protect transit staff, riders as well as the transit vehicles.

These facilities are more vulnerable to attack by individuals with knowledge or expertise in yard operations. Agencies should consider a site layout and design that facilitates the detection of any improper behavior, regardless of whether the perpetrator is authorized to be in the facility.

Explosion/Fire

Fuel-storage sites are especially attractive targets at bus yards, where fuel tanks hold as much as 50,000 gallons—enough fuel to cause a major fire that could destroy the facility and the vehicle fleet stored there. Liquid fuel is more likely to spread out into a pool and burn for an extended period of time, while gaseous fuel can release under high pressure and cause an explosion. Fuels that ignite more readily than others must be kept farther away from potential ignition sources. Facilities with compressed natural gas, or other fuels stored under pressure, are at a particular risk for a major incident.

Maintenance facilities are also potential targets for attacks using explosives or arson, although other transit infrastructure assets might be more likely targets for this type of terrorist attack.

Tampering

Maintenance facilities provide the opportunity for terrorists to sabotage vehicles by tampering with the electrical and mechanical systems in a manner that would cause an accident when the vehicle is in service. Such an incident could result in as much damage as a direct attack on a vehicle or transit station. In addition, although maintenance sites might be unlikely targets for an attack with explosives or WMD, a terrorist could try to place a device on a stored vehicle for subsequent detonation or release while the vehicle is in service. For this reason, access to the vehicles should be a key concern at maintenance and storage facilities.

6.3.4.2 Site Analysis

When locating a new maintenance or storage facility, agencies should consider the ability to secure and isolate the site. Maintenance and storage facility sites can have a clear perimeter equipped with strict access control measures. Other important considerations might include the location of vulnerable assets such as fuel-storage tanks and maintaining divisions between any adjoining transit facilities that have different security goals.

6.3.4.3 Access Management

The following sub-sections present an overview of access management at transit vehicle maintenance and storage facilities for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management.*

Maintenance and storage facilities can be contained within a secured perimeter.

Perimeter Security

Because these sites are not public facilities, agencies can maintain a fairly strict perimeter without interfering with normal operations of the facility. Transit vehicles, transit employees, and employee vehicles need to cross the perimeter on a regular basis, and the site may also need to accommodate occasional visitors and their vehicles. Access control measures can help distinguish those authorized to access the site through its entrances and prevent and detect covert access elsewhere along the perimeter.

Agencies may need to consider additional access control measures if adjoining transit uses require public accessibility. For example, rail facilities need to be adjacent or connected to the rest of the rail system. This means that storage and maintenance facilities may be adjacent to stations, which have widespread public access. Planners may consider ways to monitor the division between the public and nonpublic zones of the site.

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access Control and Parking overview: refer to Section 5.3.4

Vehicle Access

Maintenance and storage vehicles require regular transit-vehicle access. Creating a limited number of carefully controlled access points reduces the opportunity for unauthorized vehicles to enter the site. Access control measures might be particularly important at bus yards, where transit vehicles enter directly from public streets into the yard.

Agencies should consider dedicated entrances for transit vehicles that can be monitored, either electronically or by on-site security staff, to ensure no unauthorized vehicles gain access. Placing tracks and driveways for transit vehicles adjacent to one another instead of intermittently around the site, can also provide more streamlined site control. Non-transit vehicles, including staff cars, visitors' cars, and delivery trucks can be directed to parking areas that are separate from the parking and maintenance areas for transit vehicles. This can make it more difficult for perpetrators to gain access to transit vehicles and equipment.

Human Access

A secure perimeter and access control measures at the entrance to the site can help prevent unauthorized access onto the site. Additional access control measures can further protect critical areas such as vehicle garages and repair buildings, where open vehicles might be found. Keys, locks, and credentialing, as well as surveillance using security guards or CCTV may help deter and detect an attacker from accessing the buildings on a site. Technology such as cameras and intrusion alarms can extend the reach of surveillance in those areas with a limited staff presence.

Admissions Control overview: refer to Section 5.3.3

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.4.4 Emergency Response and Egress

Agencies should consider the location of hazardous substances and equipment, such as fuel-storage tanks, when planning emergency routes and response equipment.

6.3.4.5 Protecting Critical Assets

Transit Vehicles

Vehicles in the maintenance barn may be in various stages of repair, with parts removed or components exposed, presenting an opportunity for tampering and sabotage. Agencies should consider a location out of public view, within secured buildings.

The exposed underbelly of a transit vehicle may be at risk for a tampering attack while undergoing repairs.

Sunken inspection bays or reflective mirrors can facilitate under-vehicle inspections, which ideally should be completed prior to returning a vehicle to service. Transit agencies might also utilize technologies such as sensor systems to evaluate whether a vehicle underbelly deviates from its expected design, triggering an alarm if anything unusual is detected.

Vehicle parking areas can be designed to provide clear sightlines between rows of vehicles to allow for easy surveillance and minimize places where a person might hide. For example, parking buses in either a parallel, perpendicular, or angled formation, rather than a chevron formation, allows a security guard to see between multiple vehicles at a time instead of having to walk by each vehicle to have a clear view. If space and maneuverability constraints require a chevron formation, stricter access controls may be required for the vehicle parking areas.

Fuel-Storage Tanks

Agencies should consider storing fuel tanks far enough away from structures to minimize damage to buildings in the event of an explosion or fire. Additional fencing and access controls can help limit access to authorized personnel. CCTV or other surveillance devices can be used to monitor the tank enclosure and a well-lit area can provide adequate surveillance.

6.3.4.6 Structural Engineering

Buildings should follow standard physical, mechanical, electrical and emergency requirements of other buildings, and agencies should consider designing them to maintain their structural integrity in fuel fires as described in Section 6.2.3. Facilities can also be locked when not in use.

6.3.4.7 Facility Services

Appropriate equipment must be on-site to handle fuel fires and any other hazardous materials stored on-site. Agencies should consider having backup systems in place to provide continuous power and communications in the event of an attack.

Table 6-5. Security-Oriented Design Strategies for Maintenance and Storage Facilities

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site layout		
Securable perimeter	Deter	X
Structures and vehicle-storage areas set back from roads and public parking areas	Deter/Minimize	
Physical barriers such as bollards, fencing, and grade changes to enforce setbacks and secure perimeter	Deter	X
Minimum number of access points necessary	Deter/Detect	X
Staffed security checkpoints at site access points	Deter/Detect	X
Unobstructed sightlines throughout site	Detect/Deter	X
Fuel storage site isolated from rest of facility with appropriate standoff distance	Minimize	Maybe
Parking areas segregated from transit vehicles and fuel storage	Deter/Minimize	X
Interior Layout		
Building layout provides unobstructed sightlines, minimizing hidden areas and blind corners	Detect	
Access management and layout used to segregate facility uses with different time-of-day and security needs	Deter/Detect	
Architectural Features		
Rolling doors to restrict view or access into maintenance barns	Deter	X
Critical equipment secured with gates, locks, or other access control measures	Deter	X
Underground fuel tanks (instead of aboveground)	Deter	
Fire-retardant construction materials	Minimize	
Structural Engineering		
Multi-hull fuel storage containers with secure openings	Deter	
Resistance to progressive collapse	Minimize	
Systems and services		
Remote surveillance and alarm systems	Detect	X
Sufficient lighting for nighttime surveillance	Detect	X
Backup emergency lighting	Minimize	
Fire detection and suppression system	Minimize	

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances

6.3.5 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. A bridge might serve multiple types of transit vehicles, and may also incorporate non-transit utility conduits. Example facility types include an elevated railway or a bus overpass.

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.

Elevated structures might span unusual natural features or navigate dense development.

This section focuses only on the elevated structure itself, and is limited to transit-only infrastructure. Multi-modal bridges and overpasses that serve the public right-of-way are beyond the scope of this report.

Rights-of-Way overview: refer to Section 6.3.7

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering

- Facility services
- Systems and services

6.3.5.1 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. Agencies should consider focusing security strategies on protecting components that are critical for structural integrity.

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.

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.

6.3.5.2 Site Analysis

The most important consideration for the location of elevated structures is an evaluation of adjoining land uses as points of access to structural elements of the bridge, particularly load-bearing columns or the deck itself. For elevated structures that do not inherently straddle a public roadway, agencies may consider avoiding placing the structure directly above a public roadway, parking area, or other land uses that cannot be secured by the transit agency. Given the amount of land required for elevated rights-of-way, it may be impossible to entirely prevent access to the bridge from nearby uses. In these cases, the agency should consider focusing on isolating crucial elements of the structure (such as foundations), and situating these vulnerable areas at a safe distance from uses that the agency cannot control. For existing structures, the agency may consider eliminating nearby uses that are incompatible, such as eliminating public parking from under the structure.

Planners should consider providing clear areas with adequate lighting around secured areas and avoid providing places that might conceal someone attempting to access or tamper with the facility.

They can also identify unusual topography that could provide a niche or concealed approach, as well as dense foliage or other landscaping that obstructs sightlines.

6.3.5.3 Access Management

The following sub-sections present an overview of access management at elevated structures for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management.*

Perimeter Security

Although the footprint of an elevated structure may overlap roadways, waterways and buildings, the structures themselves do not require frequent access, except by transit vehicles. Perimeter security might focus on reducing the risk of terrorists gaining access to the deck and the structural support columns. The ability to fully protect the structure will depend on the need for movement on adjacent public ways. One aspect of perimeter security that may be difficult to control, especially for bridges spanning water, is the risk of ramming by an aircraft, since there is likely to be minimal surrounding infrastructure that could act as a buffer.

Vehicle Access

Agencies should consider designing the site to prevent unauthorized vehicles from accessing the deck of the structure, gaining proximity, and being able to ram structural columns.

A vehicle could gain close proximity to this column or could ram it at high speed. However, the design may help inhibit an individual from attempting to climb the structure.

If possible, designers may attempt to seal the entire area around the structure from public access. However, for elevated structures that span areas with public access, such as roadways, parking lots, non-transit buildings, and waterways, designers should consider enforcing buffer zones around key structural elements using physical barriers, such as bollards, fenders, pile piers, abutments, fencing, landscaping, and deep shoulder widths. In addition, slowing the permissible speed of passing vehicles using speed limits and curved routes may help diminish the risk of damage by ramming. Appropriate controls can be implemented to keep unauthorized vehicles from accessing the structure's deck. Fencing and bollards may be used where they do not impede transit vehicles' access while monitoring systems should be use in locations that cannot be blocked off.

Perimeter Protection and Barriers overview: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Human Access

Since individuals on foot may also pose a threat by positioning explosives directly on the structure, agencies should consider a design that denies unauthorized pedestrian access onto or beneath the structure using physical barriers, monitoring, intrusion alarms, and surveillance.

If an essential pedestrian throughway is necessary in the vicinity of the structure, the focus can be on denying access to critical structural components. Buffer measures designed for vehicles can be difficult for people to climb. They can be secured with features such as signage, fencing, barbed wire, and intrusion alarms. Agencies should consider not including accessible ladders or other features that facilitate climbing the base of the structure and should lock and secure any access points intended for maintenance personnel.

6.3.5.4 Emergency Response and Egress

Placement and types of any physical barriers designed to keep people at a distance from the structure should be chosen so that they do not compromise needs for emergency egress from the structure and access to the site by emergency responders. Agencies should consider including space for maintenance and emergency evacuation that does not compromise the ability to keep human carriers (on foot) from accessing the structure.

6.3.5.5 Protecting Critical Assets

Elevated structures are themselves critical infrastructure links. Maintaining structural integrity is a primary concern. Designers might focus on hardening the structural engineering of the asset.

Though this may be a convenient location for bicycle parking, agencies should try to locate bicycle lockers away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials. However, this goal should be balanced with concerns for safety of cyclists and the overall number and type of parking locations provided on-site.

6.3.5.6 Structural Engineering

Since it can be difficult to prevent access to the load-bearing columns of a bridge or elevated track, designers might consider engineering the structure to withstand additional forces. Load-bearing columns can be reinforced and hardened with appropriate construction techniques to withstand attacks. Redundancy can help minimize failure and prevent progressive collapse. Refer to Section 6.2.3.1.

6.3.5.7 Systems and Services

Elevated structures have minimal building systems although conduits for transit and other services may share the right-of-way. Agencies should consider locating transit utilities in such a way as to allow adequate maintenance and provide as much protection from impacts and tampering as possible. Other utilities such as water and gas pipelines that are co-located with elevated structures can be placed to minimize interruptions and damage to the transit system if they are compromised.

Table 6-6. Security-Oriented Design Strategies for Elevated Structures

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site layout		
Restricted access to land below structure, where possible	Deter/Minimize	Maybe
Structure setback from roads, parking areas, and other buildings, if possible	Deter	
Physical barriers such as fences, bollards, and fenders enforce setbacks and prevent ramming	Deter/Minimize	X
Adjacent roadways designed to inhibit high-velocity ramming of columns	Minimize	
Clear sightlines under and around structure	Detect	X
Interior Layout		
Emergency and maintenance access points limited	Deter	
Protected locations provided for limited-mobility occupants to wait for emergency personnel	Minimize	
Architectural features		
Emergency and maintenance access points secured with gates, locks, or other access control measures	Deter	X
"No Trespassing" signage	Deter	X
Columns made difficult to climb (by choice of materials or dimensions, or by barriers such as fences)	Deter	X
Fire retardant construction materials	Minimize	
Structural engineering		
Columns and piers able to withstand the impact of ramming by a truck, boat, or other vehicle	Minimize	
Resistance to progressive collapse	Minimize	
Systems and Services		
Motion detectors or intrusion alarms at vehicle entrances and other restricted-access areas around the structure	Detect	X
Electrical conduits and utilities built into structure to reduce exposure to vandals and fire	Deter	

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances

6.3.6 Tunnels

Transit vehicles use rail and bus tunnels to move passengers from station to station underground or underwater. This section addresses design issues relating to the tunnel structure itself and assumes that private vehicles do not share the tunnel with transit vehicles. For information on transit stations, refer to Section 6.3.1 and for rights-of-way, refer to Section 6.3.7.

Tunnels are long underground or underwater structures that typically have few access points. Although public access to tunnels should be prevented, tunnels cannot be altogether closed systems, as authorized transit vehicles need regular access and ventilation shafts must be open to fresh air. Tunnel design must also accommodate maintenance and emergency personnel access. Designing a tunnel to minimize access by unauthorized persons is the best way to keep tunnels safe from many potential terror threats.

Tunnel access points may include:

- Portals, where transit vehicles enter and exit the tunnel, usually at the point where the right-of-way submerges below grade.
- Station platforms, where passengers in an underground station board a transit vehicle.
- Maintenance entrances, which may be separate access points or adjoined to a station platform or portal.
- Ventilation openings that connect tunnels to the surface for air exchange via a network of ducts.
- Emergency evacuation routes and access points for emergency responders.

Fencing and a grade change help segregate this portal from nearby public areas.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering

- Facility services
- Systems and services

6.3.6.1 Potential Threats

Because tunnels are enclosed spaces that have few access points and depend on ventilation systems, they are particularly vulnerable to attacks on their ventilation systems, and to attacks that might trap people in the tunnel while exposed to fire, smoke, chemicals, flooding, or air deprivation.

Explosives/Fire

Depending on the magnitude of the blast and materials surrounding the tunnel, consequences of a blast will vary. Tunnels in bedrock have additional support provided by the surrounding rock, while those built in soils or water bear the load of the surrounding material and are likely to have more catastrophic structural failures.

Fires resulting from explosions pose a particular threat in tunnels because there are few exits, and smoke and toxic fumes can build up quickly in the enclosed spaces. Smoke has a tendency to rise, making emergency exits to the surface excellent conduits for smoke to escape from tunnels, and making exit use potentially difficult.

Weapons of Mass Destruction

WMD such as chemical, biological, or radiological agents that are released into a transit tunnel could make them permanently unusable if the materials are able to be absorbed into the tunnel structure or façade. Tunnels can be good conduits for WMD because they can be delivered through the ventilation system and spread throughout the system and into stations. Depending on the vehicle design, passengers within transit vehicles will have different levels of exposure to these agents.

6.3.6.2 Site Analysis

In choosing where to situate tunnels, agencies should consider avoiding certain geographic peculiarities and land uses, such as sites adjacent to gas or chemical tanks or to major public works pipes. While it may seem advantageous to allow external utilities to use tunnel facilities, their need for access and consequences of their systems' failures need to be considered when making agreements.

From a security standpoint, carefully choosing the location of tunnel access points may be even more important than the location of the tunnel itself. Access- point locations can be chosen based on how easily they may be secured and made inconspicuous. Planners should consider how nearby roads, topography, and land uses impact these factors.

6.3.6.3 Access Management

The following sub-sections present an overview of access management in tunnels for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management*.

Perimeter Security

The "perimeter" of a tunnel may be thought of as the perimeter areas around each of its access points (such as portals and vents). Because tunnels must not be accessible to the public, this perimeter can be strictly protected without compromising the tunnel's intended use.

The types of tunnel access (when the perimeter must be crossed) include: use of the tunnel by transit vehicles, occasional access to the tunnel by maintenance personnel, and emergency access and egress routes. Planners should consider how to selectively allow appropriate access and prevent inappropriate access at these points.

Perimeter Protection and Barriers overview: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access

Site layout can be used to minimize how close a vehicle can be near a tunnel (above or below ground), its portal, or its affiliated network of air ducts. Wherever possible, agencies should consider positioning tunnel portals at a distance from public roadways, and oriented so that driving an unauthorized vehicle into the portal is difficult or impossible. In rail tunnels, the track and third rail may make the tunnel difficult to access for other vehicles. Designers can consider other ways to manipulate the size and design of openings to limit access by non-transit vehicles, or at least prevent the largest trucks from entering. In addition, ditches, bollards, and road-spikes can be used as additional protection against unauthorized vehicles. Air vents can be housed in secure structures and concealed. Although vents can be positioned off roadways and elevated to prevent accidental spillage from the street into the vent, designers might position vents even farther from roadways and elevated a number of feet above grade, making intentional spillage more difficult to perform.

Human Access

Agencies should consider keeping at-grade tunnel access points (portals, maintenance entrances, vents, and emergency exits) as inconspicuous as possible, but oriented for easy surveillance. Clearing brush and other visual obstructions, as well as supplying adequate lighting, can provide more effective surveillance. A transit agency may encourage passive surveillance by notifying neighboring property owners or local authorities about what to do if they observe suspicious activity in the vicinity of the access point.

Grates, manholes, and other entrances can be secured with locks, electronic keys, or biometrics, and those used for air intake elevated to prevent materials from easily pouring in. Fencing and warning signs may also play a role in deterring individuals. Remote monitoring techniques such as intrusion alarms, chemical sensors, and CCTV can be used to monitor access points.

Station platforms require particular attention as access points into tunnels. Tunnel walkways are of particular concern because they are often built adjacent to the platform. The tunnel-platform interface can be designed to discourage unauthorized passage. Uneven surfaces, electrified rails, and oncoming vehicles can act as deterrents for access via the road/rail bed. Vertical grade separation between the platform and the road/rail bed does not provide an actual barrier, but does create a psychological barrier that may make bystanders more responsive to a breach.

Physical barriers separating the platform from the tunnel can be used to prevent passengers from accessing the tunnel. Platform screen doors, which open on the platform simultaneously with those of the train car, can allow passengers to board and alight without providing continual access to the track and also increase passenger safety. Station walls can be extended to be flush with the platform edge. Locked doors or barrier gates can be used to provide access from the station to the walkway as long as they do not interfere with emergency evacuation routes. Personnel, remote surveillance, and intrusion alarms can also be used to observe activity at platform periphery/tunnel entrances to detect unauthorized passage or suspicious behavior. Appropriate lighting and clear sightlines to the platform edges may also help deter and expose attackers.

Agencies should provide passengers with general instructions on what to do if they see suspicious activity, such as a person walking into the tunnel. Providing on-platform emergency phones may result in faster response times than reported.

6.3.6.4 Emergency Response and Egress

Emergency exits must be provided to allow safe egress in case of an emergency. NFPA 130, 3-2.4 prescribes emergency exits every 1,250 feet.[38] Planners should also consider providing passages for emergency responders and invite them to participate in the tunnel design and emergency planning process. Since these passageways may double as access points for maintenance personnel, they must be secured at the street level to ensure only authorized entry, while allowing easy opening from the inside for emergency egress. Agencies should consider clearly labeling emergency passageways and not rely on power or other systems to display the labels, since these may fail in an emergency or should be served by systems with redundancy.

6.3.6.5 Protecting Critical Assets

Tunnels may contain assets such as power and communications lines that may be critical for operations and for emergency systems, and may also be dangerous if tampered with. Agencies

[38] See Appendix F for more information on codes and standards.

should consider embedding power and communications wiring into the tunnel, not attached to the surface, to help protect these systems from damage in case of an incident.

In addition, the tunnel itself may be considered a critical asset for the operation of the transit agency and for the safety of transit users. Planners may treat tunnel access points as critical and choose to implement heightened access control measures.

6.3.6.6 Structural Engineering

The primary structural purpose of a tunnel is to support the tunnel against pressures from the surrounding soil, water and other loads. Cut and cover and boring are the two main techniques used to build tunnels.

Bored tunnels are generally deeper underground and are not usually threatened by explosions at ground level. Cut and cover tunnels just below grade, may need to consider the effect of a major explosion at-grade. If the tunnel is designed to prevent unauthorized vehicle entrance through the portals, explosives are most likely to be brought in by hand.

6.3.6.7 Systems and Services

Heating, Ventilation, and Air Conditioning

Ventilation is crucial to people working and traveling through tunnels in transit vehicles. Ventilation in underground, electrified rail systems usually relies on the natural piston action of vehicles to draw air in and push air out of tunnels. Fans are required for emergency situations, such as fires and stalled trains. High-speed transit systems require air relief vents to minimize the blast effects of air ahead of the train entering a station. Ventilation shafts can also provide blast over-pressure relief in the case of an explosion.

While fans and vents play an important role in minimizing harm from explosions and fires, they can have unintentional consequences in a situation involving a WMD or other contaminant. The ventilation system should not be used to remove harmful substances from a station or tunnel; this would only spread the contaminants more. Instead, the ventilation system can be used to help limit the contamination by shutting down and sealing off openings. Other isolation techniques include inflatable dams in tunnels and reducing train speeds to 5 mph or less. Agencies should consider making available additional manual controls for the ventilation system at the tunnel opening for use by emergency responders.

NFPA 130, Chapter 4 mandates the performance standards for transit tunnel ventilation. FTA has developed the *Subway Environmental Simulation* software to accompany the *Subway Environmental Design Handbook* to provide guidance in determining ventilation needs.[39]

[39] *Subway Environmental Design Handbook*. FTA. [need complete reference]

Water Management

For tunnels located below the water table, portals and cracks produced by an attack may allow minor leaks through percolation or major leaks that lead to flooding. Water used in fire suppression may also flood a tunnel. Planners may consider installing water-monitoring devices, floodgates, water pumps, and drainage systems. These water management devices may be alarmed and connected to Central Control.

Fire Protection

Tunnels can be equipped with fire alarm and suppression systems connected to a central control panel. Planners may consider installing dry fire standpipes systems, and deluge systems that release large volumes of water at track level to quench fires beneath rail vehicles. This information is not exhaustive, however, and should only supplement existing guidelines and regulations, such as those contained in NFPA 130.

Lighting Systems

Since tunnels are naturally dark, tunnel lighting is important both for the operation of vehicles as well as the detection of unusual activity in the tunnel. Emergency lighting may be essential in a tunnel emergency when people may need to move around in unfamiliar and potentially hazardous conditions. Planners should consider supplying emergency exits and pathways with independent and/or redundant power sources.

Security Systems

Security systems such as door alarms, motion detectors, and surveillance cameras may be used to protect tunnels and their remote access points. Because many parts of a tunnel network are dispersed and remote, tunnel security systems may be particularly apt to link to Central Control.

Table 6-7. Security-Oriented Design Strategies for Tunnels

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Access points isolated from public roadways and parking areas	Deter	
Physical barriers such as ditches, bollards, road spikes, and fencing around portals and other access points	Deter	X
Unobstructed sightlines around access points	Deter/Detect	X
Vent ducts situated in self-contained secure buildings, locked, elevated, and hidden	Deter	
Interior Layout		
Tunnel-level enclosed areas for rescue assistance (AORA) with pressurized fresh air	Minimize	

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
No unnecessary niches in the tunnel that may conceal people or explosives	Deter/Detect	X
Physical barriers that shield tunnel walkway from platform or portal access	Deter	X
Emergency exit doors that lock from the outside but allow unimpeded egress during emergencies	Deter/Minimize	X
ADA-compliant emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Portal entrance that limits permissible vehicle dimensions, if possible	Deter	
Screen doors that seal platform from tunnel, only opening during vehicle boarding	Deter	X
Solid access doors to ventilation shafts whenever grating is unnecessary	Deter	X
“No Trespassing” signage	Deter	X
Ample freeboard that helps protect tunnel from flooding	Minimize	
Materials that do not absorb toxic substances when exposed	Minimize	Maybe
Fire-retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		
Electrical conduits built into structure to reduce exposure to vandals and fire	Deter	
Remote surveillance of portal entrances and other access points	Detect	X
Automated central control of ventilation system, with manual override available to emergency professionals	Minimize	X
Blast- and fire-resistant, rapid-startup ventilation system	Minimize	X
Backup communications system	Minimize	X
Backup emergency lighting	Minimize	X
Water detection system and pumps capable of removing accumulating water	Detect/Minimize	X
Fire detection and suppression system	Minimize	X
Actuated vent louvers that open only when fans are running	Minimize	X
Inflatable dam to seal tunnel, to prevent spread of contaminants	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances

6.3.7 Right-of-Way, Track, and Signals

A right-of-way (ROW) is the continuous stretch of land dedicated to transit vehicle movement. Although some bus systems (notably Bus Rapid Transit systems) use exclusive rights-of-way, this type of infrastructure is typically relevant only to rail vehicles. The focus of this subsection is rail alignments and equipment, even though many of the principles are transferable to bus rights-of-way. The transit agency may own, lease, or have a use easement for the land comprising the right-of-way, and may share use of the right-of-way with other agencies or companies. Elevated structures and tunnels, while typically considered elements of a right-of-way, due to their particular security concerns are covered separately in Sections 6.3.5 (Elevated Structures) and 6.3.6 (Tunnels).)

Assets within the right-of-way include track, signaling equipment, power conductors and ancillary assets. Track hardware supports and guides vehicles, and consists of rails, switches (used to guide vehicles at junction points), and ties, all resting on the "ballast," the base material (usually crushed stone) that holds the ties in place.

Switch and signal equipment provide essential functions for a rail line.

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 either an electrified third rail or through an overhead catenary wire, depending on vehicle type and right-of-way location. Auxiliary equipment along rights-of-way includes such items as fencing, signage, and barriers.

These assets typically do not receive as much public attention as other infrastructure assets such as stations or vehicles, but they are essential for the operation of the transit system. This section focuses on the vehicle support, collision avoidance and switching application of right-of-way assets, and how best to maintain their operation during attacks.

Subsections describe:

- Potential threats

- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.7.1 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.

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.

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. Such an attack, and the measures to defend against it, is beyond the scope of this report.

6.3.7.2 Site Analysis

Rights-of-way may pass through areas that make them difficult or even impossible to secure. In addition, their contiguous layouts mean that any access point compromises access management for the entire right-of-way.

Given their size, rights-of-way typically have a variety of surroundings. A single alignment may pass through dense urban development, natural environments, and a range of land uses. The right-of-way may have a substantial buffer space between it and adjacent property (with or without a fence or wall separating the two), or vehicles may travel within a few feet of adjacent, non-transit buildings. The type of border separating a right-of-way from adjacent property affects its accessibility: for a below-grade, open-cut right-of-way, a vertical 10-foot retaining wall is a much more effective barrier than a gradual slope covering the same grade change.

Likely entrance points to a right-of-way can be identified, and their locations factored into the placement of access management measures, critical system hardware, and remote surveillance equipment. Abutting structures, adjacent public space, and at-grade intersections all constitute potential entry points for attackers. Agencies should consider locating critical equipment, like signals and electronic relays, away from such sites, preferably at points along the right-of-way that are visible from farther along the alignment or from adjoining facilities; this makes them more difficult for terrorists to access, while increasing the odds of inappropriate activity being seen and reported.

6.3.7.3 Access Management

The following sub-sections present an overview of access management for right of way, track, and signals, relating to perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in **Chapter 5: Access Management**.

Perimeter Security

It is effectively impossible to establish an effective perimeter around an entire right-of-way; it passes through too many types of areas and has insufficient staff presence to secure it.

In many places, the perimeter is simply a fence, wall, or building. Fences, walls, and other barriers can be designed to prevent people from climbing over them (or, in the case of chain link fences, cutting through them), and be able to resist vehicle impacts where appropriate.

Typically a fence or barrier is placed on or close to the legal boundary of the right-of-way. Rights-of-way by their nature present a clear unobstructed space. However, a clear area along the outside of the fence line should be established when practical, by installing a double row barrier (an inner row of fencing enclosing the assets and an outer row along the property line) or by obtaining clearance easements along the right-of-way. Where possible, remote surveillance and/or intrusion detection systems can be installed to enable the transit agency to monitor the right-of-way.

In some areas, non-transit buildings may form the boundary of the right-of-way. This situation is common in older urban areas where buildings were constructed on lots with a "zero setback" that allows buildings to stand on the property line. Transit agencies typically do not have control over access to these buildings, and tenants have an expectation of privacy. In these situations, right-of-way equipment and passing trains are vulnerable to threats from people with easy access to the right-of-way. Security options available to a transit agency include taking ownership of the building, or leasing space adjacent to the track. Increased surveillance of these areas is another option. These situations should be handled by the transit agency on a case-by-case basis.

Perimeter Protection and Barriers overview: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access

Rights-of-way should allow transit vehicles to move easily, while discouraging access by unauthorized vehicles. Wherever possible, agencies should consider not locating rights-of-way adjacent to public roadways, especially not without barriers separating the two. Grade changes, fences and walls, and dense vegetation are all options for effective barriers. At-grade crossings with roads are a common vulnerability for rights-of-way. These can be monitored with surveillance equipment where possible to ensure rapid detection of trespassing. Rights-of-way may also have service roads and gates to provide access for transit agency maintenance vehicles. These points can be controlled with locked gates and other barriers where appropriate.

Human Access

As discussed in the subsections on **Site Analysis** and **Perimeter Security**, it is effectively impossible to control all human access to a right-of-way. For this reason, it is probably more cost efficient to focus on intruder detection methods that will initiate a security response, rather than on efforts at total access management.

A right-of-way protected with fencing and a grade change (below) is more difficult to access (than above).

6.3.7.4 Emergency Response

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. Agencies should consider developing emergency evacuation and access routes for all segments within the rights-of-way as part of an emergency response plan. They should also consider factoring the presence of a live "third rail" into any plans involving the evacuation of passengers by responding emergency personnel.

6.3.7.5 Protecting Critical Assets

Since most of a right-of-way has no ongoing staff presence, security measures must rely on remote surveillance and tamper detection to safeguard on-site equipment in addition to the access management measures already mentioned. Asset protection can include the following:

- Tamper-resistant housings and locks
- Remote tamper detection
- Remote Intrusion detection
- Audible/lighted local alarm systems
- Remote surveillance
- Redundant systems
- Regular inspections of assets

If assets are successfully destroyed or compromised, measures should be in place to detect and respond to the fault and reroute services as appropriate.

Tracks and Switches

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.

Transit agencies can use advanced telemetry systems 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.

Signaling Equipment

Signaling equipment provides collision avoidance by maintaining safe spacing between trains along the rail line. Rail lines are divided into electrically separated linear segments called "blocks." Each block is part of a circuit that controls a signal placed at the entrance to the block or blocks behind a train. These signals tell operators of other trains approaching the block either to stop or to proceed at a predetermined slower speed. As a train enters a block, the train becomes part of the circuit, causing the signal at the block entrance to indicate that a train is in the block.

Table 6-8. Security-Oriented Design Strategies for Rights-of-way, Tracks, & Signals

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
ROW set back from roads and parking areas	Deter/Detect	
Physical barriers such as bollards, fencing, and grade changes to enforce setbacks	Deter/Detect	X
Unobstructed sightlines along ROW	Deter/Detect	X
Appropriate treatment of likely entrance points to ROW	Detect/Deter	X
Interior Layout		
None		
Architectural Features		
Enclosed control signal boxes secured with locks or other access control measures	Deter	X
Tamper-resistant equipment	Deter	X
Structural Engineering		
None		
Systems and services		
Motion detectors or intrusion alarms on critical equipment	Detect	X
Redundant power/communication supply systems/routings	Minimize	X
Remote surveillance systems	Detect	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

Tampering with these systems is remarkably simple. Shorting the signaling system could cause the signal for that block to show red. At a minimum this would be an inconvenience, but this would also leave the sitting train vulnerable to attack. A coordinated effort could also use shorting to stop several trains simultaneously; transit staff could interpret this as a serious malfunction of network or control center equipment, triggering a system-wide shutdown while the problem is diagnosed.

A more sophisticated and serious sabotage method is modifying the circuitry so a signal shows green to an approaching train, even when a preceding train is in the block. This has the potential for causing a collision between trains.

Tamper-resistant housings for signaling equipment and telemetric systems to remotely monitor the conditions of track and switch signals are the best defense against deliberate attack. Where possible, signaling equipment can be located in a high visibility area (near a well-traveled intersection or adjacent to a transit station, for example) to increase the likelihood that tampering attempts will be seen and reported.

6.3.8 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.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.8.1 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. Refer to Section **6.3.8.5** for more information.

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.

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.

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.

6.3.8.2 Site Analysis

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 substation transformers and other structures, 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. See Appendix F1, "Codes, Standards, Regulations: Infrastructure", for more information on codes and standards.

Agencies should consider addressing security concerns relating to site layout for remote facilities and unmanned structures, and focus on preventing unauthorized access to the equipment, protecting the equipment from attack or tampering, and protecting the transmission lines to and from the transformer, tower or array.

6.3.8.3 Access Management

The following sub-sections present an overview of access management for remote equipment and unmanned structures, relating to perimeter security and human access. Cross-references are provided to more specific details in **Chapter 5: Access Management**.

Perimeter Security

Because substations and other remote structures should not be accessible to the public and because agency staff accesses them only periodically, the site's perimeter can be strictly secured. Since most of these facilities do not have an ongoing staff presence, perimeter security measures should be robust enough to prevent access attempts without direct human involvement. Most existing facilities, regardless of ownership, have security protection such as fences, walls, and other barriers to ensure safety of accidental or curious trespassers and to prevent vandalism. These measures may include alarms to local police and fire.

Agencies should consider designing perimeter security to prevent people from climbing over or cutting through existing barriers, and to establish a standoff distance sufficient to prevent an attacker from placing or throwing an explosive device next to key on-site equipment.

Perimeter Protection and Barriers overview: refer to Section **5.2.2**

Vehicle Barriers overview: refer to Section **5.3.5**

Vehicle Access

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. However, a determined terrorist with a large enough vehicle may be able to overcome these types of passive barriers. Agencies should consider using walls or more substantial barriers, especially if a high-speed approach is possible.

Human Access

Agencies should consider designing the site, equipment, and individual structures, if any, to discourage unauthorized access. The principal enhancements to existing perimeter security systems include increased remote surveillance and intrusion detection. Planners can consider passive access control methods (no on-site personnel required) for remote or unmanned areas. Techniques such as cipher locks and biometrics can also be used.

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.8.4 Emergency Response and Egress

Regardless of whether a remote structure is staffed, the site and all structures should have predetermined evacuation routes and procedures. The presence of high-voltage equipment and volatile substances pose serious threats to on-site staff and the surrounding area, and emergency routes and procedures should reflect their nature and locations. Agencies should consider incorporating rapid shutdown mechanisms incorporated into their equipment at high-risk facilities, to minimize the damage resulting from an attack.

6.3.8.5 Protecting Vulnerable Assets

Although there are certain pieces of equipment at a remote facility or unmanned structure that may be more critical to operations or more vulnerable to damage, agencies should consider treating the entire facility as a single asset. Since these facilities are often isolated and have little, if any, staff presence, it is extremely difficult to prevent attacks. For this reason, a security plan must focus on making the system more resilient to attacks. There are two protection strategies that agencies can consider: physical reinforcement and redundant systems.

Physical reinforcement focuses on strengthening the facility to resist attack. This includes many of the normal measures discussed throughout this document: access management, appropriate standoff distances, and reinforced structures that resist fire and explosion.

Redundant systems are a more effective strategy for minimizing the consequences of an attack on a substation or communications relay, in which redundant power-transmission or relay sources are established within the transit system, so that if a particular facility is incapacitated, an alternate means of power or communications delivery exists. This strategy increases the resiliency of the system as a whole. The same strategy applies to power lines; multiple possible routings decrease dependency on particular power lines and minimize the disruption of service that results from an attack. The power companies that operate the grid are generally responsible for and provide redundancy.

Table 6-9. Security-Oriented Design Strategies for Unmanned Structures

Design Feature	Goal	Able to Retrofit
Site Layout		
Structure set back from roads and parking areas	Deter	
Minimum number of entrances	Deter	X
Key equipment located toward center of site	Deter	
Entrance dimensions minimized	Deter	X
Interior Layout		
None		
Structural Engineering		
Reinforced structures	Deter/Minimize	X
Architectural Features		
Full enclosures (but must provide ventilation per local electrical / fire requirements)	Deter	X
Access doors secured with multiple locks or other access control measures	Deter	X
Systems and Services		
Emergency shutdown mechanism	Minimize	X
Remote surveillance and intrusion alarms	Detect	X
Redundant power supply systems and routings	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

7.0 Vehicles

The information in this chapter will help increase transit agency awareness and understanding of the relationship between vehicle design and security, and explain how transit policy makers and system designers can use the physical design of heavy rail, light rail (including trolleys), and bus vehicles to help protect their employees and passengers.[40]

The intent is to present a comprehensive set of practical security-oriented design considerations to which transit agencies can refer when preparing their procurement specifications or retrofitting their fleet. Identification of these design considerations is the first step in enabling transit agencies to make informed decisions about improving the security of their vehicle fleets.

How is this chapter useful?

For **transit managers** it is a resource for:

- Identifying issues relevant to vehicle design
- Identifying potential vulnerabilities of transit vehicles

For **security staff** it is a resource for:

- Exploring potential design solutions to improve security

Each transit agency is free to determine which of these considerations best suit the current and future needs of its system; some considerations are more relevant for some systems and less so for others. Transit systems with a low level of anticipated threat may not warrant some of the more extreme or expensive measures. Budgetary restrictions may also limit a transit agency's ability to implement ideal solutions.

Transit agencies should remember that vehicle design elements are only one of several tools available to achieve a desired level of protection. An agency may also consider infrastructure design, operational procedures such as training security personnel, or security-oriented policies (such as an Emergency Response Plan). A cohesive security plan interweaves vehicle design strategies, such as those in this chapter, together with other elements. These include balancing system security against other policy goals, such as operational efficiency and passenger convenience; reconciling security-oriented design considerations with existing design codes and standards; and reviewing agency standards in relation to the security considerations in this chapter.

7.1 Introduction

Vehicles are the foundation of every transit system; they provide the core service on which transit is based and are the primary interface with the public. As the most visible and most accessible elements of a transit system, vehicles are extremely exposed to possible attack. Transit system

[40] Safety and security regulations for commuter rail services are established by the Federal Railroad Administration (FRA), and are beyond the scope of this report.

designers need to recognize this and determine how best to protect their vehicles against potential threats.

To support system decision makers and vehicle designers in this effort, this chapter presents information on the following aspects of vehicle design and security:

- General security issues for transit staff
- **Potential security threats** to transit vehicles
- A comprehensive set of practical **design considerations** when preparing procurement specifications or fleet retrofits
- **Vehicle design considerations** relevant to security
- **Lessons learned** from national and international vehicle security events

7.2 General Considerations

This section presents several issues for transit staff to take into account when considering security during the planning of vehicle design: vehicles in relation to the overall system, vehicle role, accessibility, and vehicle operator protection.

7.2.1 Vehicles in Relation to the Overall System

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. Security-related design concerns for infrastructure are addressed in **Chapter 6: Infrastructure**, but it is worthwhile to keep in mind the relationships between transit vehicles and the following types of infrastructure:

- Tunnels and elevated structures
- Stations, including intermodal facilities
- On-street transit stops
- Vehicle maintenance and storage facilities
- Administrative facilities, including operations control and communications centers

- Signals and track and power
- Power substations

Transit agencies will benefit if vehicles are designed to promote the security of both the vehicles themselves and the other components of the transit systems.

7.2.2 Vehicle Roles

When transit agencies undertake security planning, they should consider their vehicles from three perspectives:

- **Target**. Transit vehicles are likely targets for terrorist attack because they often carry large numbers of people and are highly visible. Agencies should consider treating vehicles as assets to be guarded at two levels, the vehicles themselves and the people they carry.
- **Weapon**. A transit vehicle provides an excellent means of delivering a terrorist's weapon to a target, because of its public nature and the areas in which it will typically travel. Terrorists can plant a device on board—and then detonate it when the vehicle reaches the intended target, such as a transit station.
- **Means of Response**. After an attack has occurred, transit vehicles can comprise a significant element of emergency response: they can evacuate large numbers of people from dangerous areas, and can move emergency responders and equipment as needed. Accordingly, vehicles need to remain functional after an attack.

7.2.3 Accessibility

By their nature and purpose, transit vehicles are designed to be accessible to many people at a time and are therefore difficult to secure. Their design must facilitate quick boarding and exiting, with few impediments to passenger flow through the vehicle. Vehicles are often accessed from uncontrolled public spaces (especially buses), and it is impractical to pre-screen passengers entering a vehicle.

These factors make it difficult to implement measures that establish strong security on a vehicle. The design must often rely on passive elements to improve on-board security.

7.2.4 Vehicle Operator Protection

In most transit systems, drivers operate vehicles autonomously. For this reason, the safety of the operator and his/her ongoing ability to operate the vehicle are critical; the operator must be able to bring the vehicle safely to a stop after an incident, to remove the vehicle (and its passengers) from the immediate area of a threat, or to use the vehicle to support emergency response activities. All of this is subject to the operator surviving an attack on the vehicle and the control systems remaining functional.

For this reason, it is helpful to include design elements that will protect the operator in the event of an explosion, fire, and other types of attack.

7.3 Potential Threats to Transit Vehicles

Transit vehicles are an extremely visible element of most cultures, and are easily accessible to potential attackers. For these reasons, they are attractive targets for a terrorist attack intended to inflict civilian injuries, disruption of service, disruption of emergency response capabilities, and general panic. They may be the primary target of an attack, may be damaged in an attack on a transit facility, or may even be used as a means of delivering a weapon to an attack site. While it is acknowledged that transit facilities and vehicles impact the security of one another, this section focuses only on threats to vehicles.

Scenarios of potential threats to transit vehicles include:

- Explosives placed on or under a vehicle
- Armed assault on board a vehicle
- Chemical, biological, or radiological release on a vehicle
- Attack by another vehicle
- Derailment (rail vehicles only)

7.3.1 Explosives Placed on or Under a Vehicle

This scenario involves the detonation of an explosive device on board a vehicle while it is in service. Recent terrorist attacks abroad on buses and trains have used this type of attack to harm both passengers and non-passengers, as the explosions sent shrapnel throughout the surrounding area.

In these attacks someone brings the explosives on board or plants the explosives on or under the vehicle, either while the vehicle is in operation or when it is parked at a maintenance/storage facility. The on-board explosive device might be conventional, or could be a ‘dirty bomb’ designed to spread contaminants (see Section 7.3.3). In a subway system, an explosion in an underground tunnel could have catastrophic impacts on both the riders and the ongoing operation of the system.

7.3.2 Armed Assault On Board a Vehicle

This scenario involves a passenger attacking fellow passengers or the operator on the bus or train, either when the vehicle is stationary or underway.

There are several recent examples of this type of attack occurring on buses, including an assault on a Greyhound bus driver while the vehicle was in service. Most of these attacks have been crime-related rather than terrorist-related.

This type of situation could develop into a more serious incident involving the attackers barricading themselves on the vehicle, possibly with hostages. Attackers may even hijack the transit vehicle with the operator and passengers on board.

7.3.3 Chemical, Biological, or Radiological Release on a Vehicle

The release of a chemical, biological, or radiological substance on a vehicle could cause significant casualties. The impacts from such an event might be limited to on board the vehicle, or could disperse to the surrounding area, depending on the ventilation of both the vehicle and the area in which the release occurs.

In addition to the injuries incurred, these attacks also disrupt service for extended periods while the vehicles and immediate areas are contained and decontaminated to prevent further consequences. The release of sarin gas in the **Tokyo** subway in 1995 is an example of this type of attack. A substance can be released surreptitiously, either in person or via a remote device, or through the use of a "dirty bomb" that spreads contaminants in an explosion.

7.3.4 Attack by Another Vehicle

This scenario involves the intentional crashing of another vehicle into a bus or train to cause physical damage, injuries, an explosion, or fire. An alternate scenario would be for a terrorist to pull up next to the target in a vehicle carrying explosives and then detonate the explosives.

This type of attack has occurred several times in **Israel**. It is virtually impossible to prevent this type of attack on a bus because they travel on public roadways; rail vehicles whose rights-of-way are parallel to roadways or run beneath overpasses are also at risk.

7.3.5 Derailment (Rail Vehicles Only)

One of the biggest dangers for rail vehicles, short of an explosion, is from derailments or rollovers. By sabotaging either the vehicle itself or a section of track, a terrorist can initiate a chain reaction along a train of cars, pulling them all from the tracks. These incidents often result in numerous casualties, and require specialized equipment to clear the accident site and enable transit service to resume.

7.4 Design Issues

Many of the design issues discussed in this chapter will be more effective when combined with operational actions that are needed to ensure a robust integrated system of security. For details on operational improvements and recommendations related to safety and security, refer to the FTA Web site at **www.transit-safety.volpe.dot.gov**.

Security-oriented design considerations for transit agencies to take into account when preparing their procurement specifications or retrofitting their fleet include the following:

- CPTED
- Competing concerns
- Life-cycle timing of technology improvements
- Existing safety and security standards
- Vehicle design trends

7.4.1 CPTED

In many cases, measures taken to improve the day-to-day safety of the transit system against crime can result in improved security against larger threats, such as terrorism. The FTA is promoting the use of CPTED principles to help transit agencies reduce the incident of crime. CPTED is based on the idea that proper design and the effective use of the built environment can lead to a reduction in the number of crimes committed against passengers and the transit agency. For additional information on CPTED refer to **5.1.5.1** and to **www.cpted.com.au** or **www.cpted-watch.com**.

Other improvements being incorporated into vehicle designs to help reduce or mitigate criminal acts, such as the installation of CCTV or driver shields, may also help to reduce or mitigate the effects of a terrorist attack, or to preemptively discourage attacks.

7.4.2 Competing Concerns

A number of major variables should be addressed during the vehicle design process; balancing these competing concerns presents a challenge. Proposed design considerations that may improve one variable may have a negative effect on other variables. Transit vehicle designers need to decide which factors take priority and where compromises need to be made. These variables include:

- Safety
- Reliability
- Accessibility
- Purchase cost of the vehicle

- Maintenance cost over the life of the vehicle
- Weight of the vehicle

Safety, Reliability, and Accessibility

Safety of the vehicle passengers and operators is the paramount consideration for vehicle designers. A transit agency will be reluctant to include a feature that reduces vehicle safety. Unfortunately, safety and security sometimes conflict with each other in terms of their design requirements. For example, security might benefit from locked windows, but such windows might prevent passengers from evacuating a vehicle quickly during an emergency.

A transit vehicle must be designed so that it can operate in various urban and rural environments, make frequent stops, move large numbers of people, and provide accessibility to all. The nature of transit may limit the use of some security features that have proved effective in stationary facilities such as airport terminals.

Purchase and Maintenance Costs

Cost effectiveness is key to suggesting design considerations that are security oriented. Transit agencies are faced with difficult choices—between reducing the total cost of a vehicle, and adding technology or design features that contribute to the safety and security of a vehicle. It would be unrealistic to expect that transit agencies will be able to incorporate new design modifications unless they are affordable and multi-faceted. One key to ensuring that security systems are more widely used in vehicles is to make them serve additional functions, such as improving safety and crime prevention, or reducing maintenance costs.

Features should also be easy and inexpensive to maintain. Components that have high ongoing maintenance costs will be more difficult to justify.

Weight

Another trade-off involves the total weight of a vehicle. It is crucial to keep the weight of a vehicle within certain limits to minimize stress on the axles and wheels, as well as on streets or rail beds. Since 1982, the U.S. federal government has imposed a weight limit of 20,000 pounds for a single axle and 34,000 pounds for a tandem axle for buses, although federal legislation in 1992 allowed states to exempt certain classes of transit buses from these weight limits.

Given that many transit buses already exceed U.S. federal axle weight limits, any security design elements that add to the total weight of the vehicle must be evaluated against the need to keep the total weight of the vehicle below a certain threshold, or the need to compensate by reducing the weight of other vehicle components.

7.4.3 Life Cycle Timing of Technology Improvements

There are at least three points in the life of a transit vehicle when new technology can be incorporated into the vehicle to help improve security:

- New vehicle purchase
- Major overhaul
- Minor overhaul

New Vehicle Purchase

The ideal time for incorporating security design features is during the new vehicle design and purchase process. The technical specifications for a new procurement can incorporate design features that enhance security, and can be included in the overall design of a new vehicle fleet purchase. Other vehicle design elements can be modified to accommodate or even support security-oriented features.

Unfortunately, the life cycles of transit vehicles make these opportunities infrequent. According to the American Public Transportation Association (APTA), the typical lifespan of heavy rail and light rail vehicles is between 20 to 40 years, and buses have an average lifespan of 12 to 18 years. The lifespan of rail cars is significant because the likelihood that existing transit systems will change out an entire rail fleet is improbable. The most common approach is to replace a portion of the fleet with a new purchase and retire the oldest or most mechanically unreliable of the existing fleet. This means that relatively easy and inexpensive retrofits on existing rail car fleets are most feasible for transit agencies in the United States today.

Major Overhaul

The main purpose of a major overhaul is to address reliability issues and safety of operations activities, but security measures can also be incorporated. On average, rail vehicles receive a general overhaul (complete, heavy) approximately every 12 years, and buses receive one after 7-10 years. There are, however, different time and mileage criteria applied to each vehicle system and its related components and sub-components, so schedules may vary. There is also a great deal of variation among transit agencies on their major overhaul schedules.

Major overhauls provide an opportunity for extensive improvements to be made, including those intended to promote security. Large portions of the vehicle can be disassembled or modified, as needed.

Minor Overhaul

Minor overhauls occur on a more frequent interval and are often related to a specific component. At some agencies, these are called service and inspection cycles. Small-scale security design features can be incorporated during these maintenance functions, and minor safety modifications can also be made when cars are brought in for a particular cycle of maintenance. Industry experts advise that safety aboard existing vehicles can be enhanced significantly by performing simple tasks during a minor overhaul, such as properly securing equipment cabinets in walls and under seats.

7.4.4 Existing Safety and Security Standards

When evaluating potential design improvements to a vehicle, it is important to recognize that standards already exist that address the material composition of the car interior, including walls, floor, ceiling materials, seats, lighting fixtures, and windows. Many guidelines that agencies might consider have already been established as standards within the industry by Standards Development Organizations (SDO).[41]

APTA representatives have noted that historically the focus of standards development for transit vehicles has been on maintenance and inspection issues rather than on design criteria. For example, a review of recent literature on flammability and toxicity of materials used in rail vehicle construction indicates that room for improvement or at least for consistency across the industry exists.[42] Across the United States, there is inconsistency among rail vehicle procurement specifications and their testing. In general, European standards may be more stringent than U.S. standards for flammability and toxicity.[43]

Organizations that have produced standards and guidelines that are applicable to transit vehicle design and procurement include the following:

- The United States government issues regulations that are listed in the Code of Federal Regulations (CFR). These regulations are developed to comply with the legislative mandates passed by Congress and signed into law by the President. The federal government also issues recommended practices, which are non-regulatory, but provide an awareness of issues and tools to address them.
- APTA facilitates the development of standards for both rail and bus vehicles. A chapter on vehicle design criteria is included in the 1981 APTA Guidelines for the Design of Rapid Transit Facilities, and APTA also produced the Standard Bus Procurement Guidelines. For more information, refer to **www.apta.com**.
- American National Standards Institute (ANSI) is a private non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

[41] Regulations and rules (that have been promulgated) are the only requirements that can be and usually are legally enforceable.

[42] *Fire Safety Analysis for Rolling Stock*, Mark A. Davis; Material *Toxicity Test Issues in Rolling Stock Procurements*, Mark Davis, Balaji Krishnamurthy, Peter Katsumata.

[43] *Comparisons of American, British, French and German Standards for Flame, Smoke and Toxicity of Elastomeric Materials*, Rick Hopf, Carol Stream, Emily Witthaus.

- Institute of Electrical and Electronics Engineers, Inc. (IEEE) is a technical professional association that develops standards applicable to rail vehicles, in addition to other engineering areas.
- American Society for Testing Materials (ASTM) is a non-profit organization that provides a forum for the development and publication of voluntary consensus standards for materials, products, systems, and services.
- American Society of Mechanical Engineers (ASME) is an educational and technical organization setting many industrial and manufacturing standards.
- National Fire Protection Association (NFPA) develops consensus codes and standards intended to minimize the possibility and effects of fire and other life safety risks. NFPA 130 covers fixed guideway transit fire safety from a systems approach, including provisions for the fire and life safety of trainways and stations, as well as vehicles.
- FTA Recommended Fire Safety Practices Rail Transit Vehicle Material Selection specifies certain flammability and smoke emission tests and performance criteria. This has provided a tool for rail transit agencies to screen out particularly hazardous materials, which could rapidly ignite and spread fire or emit large quantities of smoke. FRA issued passenger rail equipment fire safety regulations in 1999 and 2002.
- Society of Automotive Engineers (SAE) develops engineering design and safety standards for the motor vehicle industry, including buses.

In addition, many transit properties supplement published standards with more stringent requirements, based on their experience and determined needs. For additional information about specific standards, refer to Appendix F2, "Codes Standards, Regulations: Bus Vehicles."

7.4.5 Vehicle Design Trends

There are several recent trends influencing transit vehicle design. While none is directly related to security, all influence the security of vehicles indirectly. These include:

- Modular components
- Accommodations for riders with disabilities
- Alternative bus fuels

7.4.5.1 Modular Components

To reduce the initial purchase price of a vehicle and the eventual maintenance costs, transit agencies are working with vehicle manufacturers to design the major vehicle components using modular components. This approach allows for the quick removal and replacement of modules and reduces repair and maintenance costs.

Modularization also provides a safety benefit. For example, modular seats have fewer small parts, which have the potential to become shrapnel and injure passengers and bystanders in the event of an explosion. A modular design also facilitates the replacement of certain components of a vehicle with new components that are more security-supportive.

7.4.5.2 Accommodations for Riders with Disabilities

The Americans with Disabilities Act (ADA)[44] and accompanying regulations (49 CFR Parts 27, 37, and 38) require that transit vehicles provide certain features to assist people with disabilities. A major focus of these regulations is to provide people who have ambulatory restrictions with access to vehicles, so that they are able to enter and exit a vehicle via a low floor or mechanical lift. Another key focus is to provide audible announcements of stops for the visually impaired.

ADA regulations have resulted in transit agencies moving toward vehicle designs that use low floors and designs that incorporate automated stop announcements using some type of automated vehicle locator system, usually based on the global positioning system (GPS) or transmitters embedded in the rail bed.

Public address systems help security by improving the vehicle operator's ability to communicate with passengers. The physical design elements intended to assist passengers with limited mobility, however, may preclude the installation of some security-oriented design features.

7.4.5.3 Alternative Bus Fuels

Different types of fuels are used to power buses in the mass transit fleets. Since the 1950s, diesel has been the predominant fuel for public transit buses that are 30 feet in length or longer, making up approximately 88 percent of the existing national transit bus fleet.

While diesel is the predominant power source, transit agencies have been increasing their purchases of alternative fuel vehicles, typically because of air quality concerns. According to APTA,[45] in previous years, compressed natural gas (CNG) -powered vehicles made up the greatest percentage increase in the vehicle fleet. In 2002, CNG-powered buses made up almost 10 percent of the overall transit bus fleet, as shown in Figure 7-1.

[44] http://www.usdoj.gov/crt/ada/adahom1.htm.

[45] APTA 2001. APTA Table 79, New Bus and Trolleybus Market by Power Source. For current data, see http://www.apta.com/research/stats/bus/busmktpower.cfm.

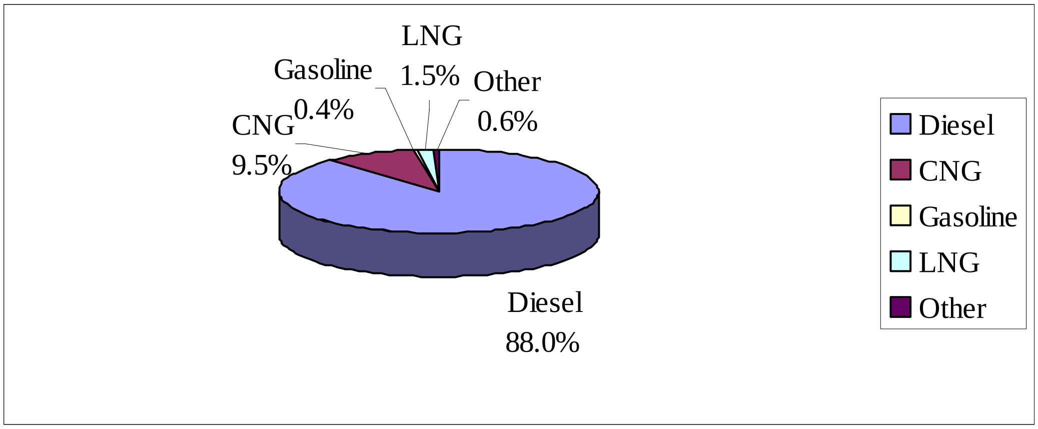


Figure 7-1. Percent of 2002 Transit Bus Fleet By Power Source

The trend moving away from diesel because of environmental air quality concerns appears to be continuing (APTA 2001). For buses either delivered or on order for the years 2001-2002, diesel-powered buses made up only 73 percent of the total market, with CNG-powered buses increasing to around 18 percent of the market. According to an APTA report, CNG-powered buses made up approximately 21% of potential orders for new buses that identified a fuel source for the years 2003 through 2008.[46]

This trend is significant for safety reasons. The two types of fuels react very differently to explosions and fire. While diesel fuel is more likely to spread into a pool and burn for a longer period of time, a CNG-powered system has a higher propensity for combustion when exposed to flame because of the high pressure in the system and the gaseous state of its contents. More recently, however, several operators have adopted or considered hybrid vehicles, which introduce fewer air pollutants and offer more versatility than vehicles powered solely by diesel fuel.

However, use of diesel hybrid power is beginning to rise. APTA reports indicate that dual-powered vehicles make up approximately 17% of orders in January 2004. Potential orders, though small, nearly double the amount of vehicles built in 2003. Such vehicles improve many of the environmental concerns posed by vehicles powered solely by diesel fuel, and do not carry the safety concerns associated with CNG-powered vehicles.

7.5 Suggested Security Strategies for Vehicle Design

In considering how to protect their vehicle fleets, transit agencies can incorporate a number of physical features and design elements to hinder a potential attack or to reduce the consequences of a

[46] APTA 2001. APTA Table 79, New Bus and Trolleybus Market by Power Source. For current data, see http://www.apta.com/research/stats/bus/busmktpower.cfm.

successful one. Agencies are reminded that these are suggested strategies only and each agency should determine which best suit the current and future needs of its system.

Lessons learned from prior events suggest that the following security strategies will help protect the vehicle fleet:

- Limit the ability to place or hide explosives on or under vehicle
- Improve the ability to see into and out of vehicle
- Reduce the damage that would result from an explosion
- Reduce the damage that would result from a fire
- Reduce the damage that would result from contaminants
- Enhance emergency egress through doors and windows
- Protect the driver from physical threat
- Network the vehicle with the OCC
- Enable communications between the vehicle operator and passengers
- Secure the vehicle from theft/unauthorized operations

Each strategy is summarized in the following subsections.

For more details on security strategies for buses, refer to **Table 7-1**; for rail vehicles, see **Table 7-2**. Each table includes information about design features, as well as the cost, timing, and difficulty of installing such features. These tables should help transit agencies make informed decisions about which measures are appropriate or feasible for their particular circumstances. Note that each table was prepared by separate panels of industry experts from the bus and rail vehicle industries, and while they contain similar data, there are slight differences in the types of information presented.

7.5.1 Limit the Ability to Place or Hide Explosives

One function of transit vehicles is to allow passengers easy access into and within the vehicle and to provide space for passengers to carry and store packages during their ride, but agencies must balance these needs against safety concerns when designing a vehicle.

Compartments

Compartments both inside and outside the vehicle should be lockable and designed to prevent unauthorized access to on-board systems and mechanical components.

Many older vehicles have no locking devices for compartments, but several large transit agencies are now specifying that their new vehicles must include locks for their major compartments, including those for fueling, storage, engine, electrical wiring, and HVAC. One solution is to equip the major access doors with locks requiring a specialized tool to open. A more secure method would require the use of a key to open the compartments, but this can present operational and maintenance problems. The interior of a vehicle should also be designed to reduce sheltered spaces where a package containing an explosive device or contaminants could be hidden from public view.

Detection Systems

Sensor/pager systems can be installed to detect dangerous substances, such as radioactive or bio-hazardous material, and alert the operator when the vehicle has been contaminated. The FTA is currently working on a prototype of a stationary detection system under the PROTECT program. PROTECT is intended to provide timely and accurate information about airborne chemical attacks in a station or tunnel. Adapting such systems to operate in vehicles presents significant technological challenges, and the cost of these systems is currently too high for most transit agencies.

7.5.2 Improve Visibility Into and Out of Vehicle

In the event of an incident on board a transit vehicle, responding law enforcement and emergency response agencies need to be able to assess the situation as quickly and as easily as possible. Their ability to see what has taken place in the vehicle, or what is currently happening, will enable them to respond in a manner that helps protect both their own safety and that of the transit passengers.

Similarly, improving a vehicle operator's ability to see what is taking place around the vehicle enables the operator to respond more quickly to impending threats and developing situations. While buses are often equipped with side view mirrors (and sometimes CCTV) to enable the driver to see all four sides of the vehicle, most rail transit vehicles do not have this feature and it may be difficult for an operator to assess what is taking place near the rear of the train.

Techniques for improving visibility into and out of transit vehicles include:

- Maximizing window coverage to the most reasonable extent (subject to conflicting structural and safety requirements).
- Locating windows strategically to provide important fields of view, and eliminating "advertising wraps" on the exteriors of windows that prevent people from seeing into the vehicle.
- Including on-board CCTVs; some buses already have CCTV installed to provide rear-facing views of the vehicle's exterior; adding these to additional vehicles would improve operators' ability to assess potential threats and operate the vehicles more safely.
- Design and selection of materials that minimize reflection/glare.

7.5.3 Reduce Damage from an Explosion

While it may be unrealistic to think that a vehicle can be made "bomb proof" or "bomb resistant," several design elements can improve a vehicle's ability to reduce the damage that results from an on-board or nearby explosion. This may even enable the vehicle to maintain at least basic operating capacity in order to evacuate the area being attacked (assuming the device was not on board the bus), and may protect the passengers on board.

Reinforcing key elements of the vehicle is a logical first step in improving blast resistance. Stronger elements may enable a vehicle to maintain structural integrity and prevent catastrophic collapse of the vehicle body. Stronger body components are less likely to fragment in an explosion, and can shield occupants from flying debris. Selection of structural materials such as stainless steel may also increase strength and temperature of phase change (i.e. melting temperature).

Windows

One of the biggest concerns is windows, because glass shatters more easily than other materials and shards can injure nearby people. Transit agencies can consider selecting windows constructed of safer materials that are more resilient and shatter into fewer pieces.

Modular Seating

Modular seating can also offer safety benefits; it is constructed of larger components, with fewer small pieces to become potential shrapnel in a blast.

Fuel Tank

On buses, the fuel tank is one of the most dangerous components because of the large volume of fuel stored in it. Fuel tanks for natural gas are usually placed on the top of a vehicle where they are less vulnerable; pressure-release devices have been designed to release the fuel at the top of the vehicle to direct it away from any possible ignition sources on the bus.

Current standards for alternative fuel containers are covered in ANSI standard NGV2. Transit agencies can consider strengthening fuel storage compartments against punctures, although this would likely add to the overall vehicle weight.

7.5.4 Reduce Damage From a Fire

In the event of a fire, there are a number of design measures that can minimize the damage and assist with response efforts. This can be critical to protecting vehicle occupants from flames and providing them with enough time to evacuate the vehicle. Note that many of the measures used to reduce blast damage assist with mitigating fire damage as well.

Vehicle Materials

While there is no completely non-combustible, non-toxic material in existence, certain materials will hinder fire spread, smoke emission, and the release of toxic gases. These types of materials should be used throughout the vehicle to the greatest practical extent, balancing their benefits against other criteria such as durability and cost. All materials in the passenger area should comply with existing fire safety standards (ASTME162 and E662). Vinyl seat coverings and foam seat padding should meet Federal Specifications CCC-A 680a. Seating upholstery should meet the requirements for textiles specified in Federal Aviation Regulations 25.853(b).

Firewall Barrier

A firewall barrier to prevent any flame propagation into the passenger area should separate the passenger area from major mechanical elements and fuel storage compartments. On rail vehicles, for example, ply metal floors are commonly used to isolate the passenger area from equipment beneath the floor. The 1984 FTA Recommended Fire Safety Practices require that the vehicle floor stay intact for a nominal time period of not less than 15 minutes, and most rail operators have their own performance criteria that exceed this specification.

7.5.5 Reduce Damage from Contaminants

In the event of a chemical/biological/radiological attack in which contaminants are intentionally released, the vehicle should be designed to limit the effects of those materials. This approach needs to take into account that such substances can be in solid, liquid, or gaseous form.

Contaminant Spreading

The first consideration is how to limit the spread of the dangerous substances. For example, aerosol contaminants can be circulated by the vehicle's HVAC system. The HVAC may also vent outside the vehicle, spreading the substance and contaminating surrounding areas. Providing a manual HVAC "shut down" button may enable the vehicle operator or emergency responders to deactivate the system in time to limit contamination to a certain section of the vehicle or to the interior of the vehicle.

Cleanup/Decontamination

Vehicles can also be designed to facilitate the required cleanup and decontamination process that follows this type of attack. An interior design with smooth surfaces is easier to clean and disinfect. Where possible, non-porous materials can be used to reduce the absorption of toxic substances, making it easier to ensure that all contaminants have been removed.

7.5.6 Enhance Emergency Egress

In an emergency, vehicle operators and passengers should be able to exit a transit vehicle quickly and easily. This can be critical to preventing further casualties in the aftermath of an attack.

Door Releases

Manually operated emergency door releases should be considered for all vehicle doors, with the door release interconnected to the braking system and the accelerator to bring the vehicle to a stop when the door release is activated. The emergency door release device should be visible to passengers, but secured behind a protective cover to prevent accidental activation.

Passenger Windows

The passenger windows, particularly on buses, should be designed to allow for emergency exit, in compliance with FMVSS 217. Currently, some rail transit professionals consider it very difficult for an average person to push out a rail transit vehicle window. The redesign of emergency windows might be considered to ensure that quick removal is possible by an average-sized person under duress.

7.5.7 Protect the Driver from Physical Threat

The vehicle operator is a transit agency's front line of defense against attack and for conducting emergency response activities. The safety of the operator and his/her ongoing ability to operate the vehicle are critical; the operator must be able to bring the vehicle safely to a stop after an incident, to remove the vehicle (and its passengers) from the immediate area of a threat, or to use the vehicle to support emergency response activities. All of this is subject to the operator surviving an attack on the vehicle.

On heavy rail vehicles, the driver is usually isolated from passengers in a secured compartment. In buses and light rail vehicles, however, the driver typically sits in the main body of the vehicle. While these operators need to be able to interact with passengers, threats against the driver can be minimized through vehicle design.

Compartment Barrier

Some transit agencies are incorporating a barrier around the bus driver's compartment, similar to those found in light rail vehicles, into the design of new vehicles. The barrier can extend from below seat level to near the ceiling and can be made of metal or polycarbonate material. This barrier is hinged so the vehicle can be operated with the barrier either closed or open, at the discretion of the driver.

Compartment Shielding

Shielding around the operator's compartment can also protect him/her from the effects of a bomb blast or other form of attack on the vehicle. This would help the operator retain the ability to move the vehicle to a safer location and to activate any on-board emergency systems after an attack.

7.5.8 Network the Vehicle with the OCC

A crucial element in detecting, delaying and responding to a crisis involving a transit vehicle is a reliable communications link between the vehicle and the OCC, which can enable vehicle operators and operations staff to share accurate information and make well-informed decisions.

Current communications technology on most transit fleets consists of a radio connection between the vehicle and operations, but there are additional possibilities.

Automatic Vehicle Locator (AVL)

An automatic vehicle locator (AVL) system allows the OCC to remotely track and monitor the position of a vehicle. AVLs are more relevant for buses than rail transit systems. In addition to security considerations, AVLs can improve a transit agency's operational capabilities. When linked with a GPS system, a transit agency can track vehicle on-time performance in real time and make on-board stop and location announcements, as required by ADA.

Mobile Data Terminals (MDTs)

Mobile data terminals (MDTs) installed in conjunction with an AVL system enable the OCC to communicate electronically with the vehicle driver. An OCC can send messages electronically to the fleet about an in-progress incident, or contact individual drivers to alert them to a specific problem. Currently, MDTs are used primarily by agencies operating paratransit services to schedule real-time assignments of trips.

Silent Alarm Systems

A silent alarm system can be as simple as a panic button that flashes lights on the front of the vehicle or as complex as a link with the AVL system to allow for the remote tracking of a vehicle by the OCC or the police. Another option is CCTV systems. Where these systems have been installed on vehicle fleets, they have been primarily intended as part of a safety program to help deter crime. However, a CCTV system can be set up to perform a variety of functions, such as recording an incident for later viewing, sending images to a control center, and streaming live video from a vehicle.

7.5.9 Enable Communications between Vehicle Operator and Passengers

During an emergency, it is extremely helpful for transit agencies to be able to keep their passengers up to date on the current situation and to provide instructions as needed. Likewise, transit vehicle passengers can inform transit staff of emergency situations taking place on the vehicle; this is particularly relevant for heavy rail systems, where large portions of the interior are not directly viewable by on-board staff.

On-Board Public Address Systems

On-board public address (PA) systems can be used to inform riders about service status. More importantly, during an emergency operators can use the PA system to provide instructions to passengers such as when evacuating a vehicle. Many transit systems already have this type of system in place, but not necessarily on all types of vehicles.

Emergency Call Boxes

Emergency call boxes in vehicles enable passengers to inform transit staff of security-related incidents taking place. This greatly improves security by involving riders in passive surveillance and enabling them to report incidents to transit staff quickly without leaving the site.

7.5.10 Secure the Vehicle from Theft/Unauthorized Operation

Traditionally, transit vehicles do not require any type of key to operate. For most transit buses, a driver simply activates the master run switch and then activates the engine start button.

"Smart" Card

To prevent the operation of a vehicle by an unauthorized person, installation of a key system or a "smart" card system can reduce the threat of vehicle theft. If a key system is used, a transit agency often uses one master key that operates a specific series of vehicles in a fleet. The smart card system could also provide a higher level of security by integrating the ability to start and operate a vehicle into a transit agency's credentialing program for its employees.

Vehicle Design

Vehicle design can also help to prevent unauthorized access to the operator compartment. Lockable doors and, in the case of buses and some light rail vehicles, partitions keep attackers from gaining access to the control system, while also helping to protect the vehicle operator. These also reduce the likelihood of vandalism or sabotage to the control systems.

Table 7-1. Bus Vehicle Design Solutions

Design Consideration	State of Technology Maturity Scale of 1 (least mature) to 5 (most mature)	Cost Scale of 1 (low) to 10 (high)	Retrofit: New Buses / Overhaul / All
1. Networking of bus to operations control center			
Install automatic vehicle locator (AVL) system to allow bus operations to monitor bus location	3 – Has been deployed to various degrees widely. Multiple technologies used to determine location and transmit messages	Range of 6 to 10 – Requires significant investment and support infrastructure. High increment of system maintenance required	All
Install mobile data terminals (MDT) to allow for electronic transmission of messages	3 – Can be integrated into AVL systems. Wide variety of commercial technologies	Range of 4 to 8 – Wide variety of commercial technologies available. Less infrastructure and management	All
Utilize GPS to allow bus operations to track the vehicle location	4 – GPS is widely used and commercially viable. Communication technologies for data transfer must be integrated for command and control	Range of 3 to 10 – Varies based on functionality requirements. From stand-alone units to full system integration	All
Install silent alarm system (panic button) with connection to bus operations, bus destination sign, and police department	5 – Silent alarm features triggered manually are incorporated in most transit system radio systems. Typically linked to on-board exterior signage for emergency alert	Range of 1 to 5 – Has been done in a variety of ways. Simple to do on vehicle; compatible with most communication systems	All
Install CCTV cameras. Cameras can either record for later viewing or broadcasting of sample images live to a control center	5 – Mature technology widely available. Real time transmission of video information is not widely available. Concerns are data management and evidence chain of custody	Range of 3 to 5 – CCTV technology has a relatively low cost if information does not require wireless communication	All
Real time transmission of CCTV data	2 – Currently a number of communication approaches are being used to provide real time transmission of on-board video images to command and security personnel	Range of 8 to 10 – Cost is high since technology is new and firm commercial processes are still under development	All

Design Consideration	State of Technology Maturity Scale of 1 (least mature) to 5 (most mature)	Cost Scale of 1 (low) to 10 (high)	Retrofit: New Buses / Overhaul / All
2. Limiting ability to place or hide explosives/Securing compartment doors			
Design compartments (fuel, storage areas, engine, and others) to be protected against unauthorized access	5 – Mature; already available for most applications	Range of 1 to 3 – Various technologies and solutions can be employed	New
Design compartments to be locked by specialized wrench	5 – Commonly used in current production vehicles	Range of 1 to 2 – Cost is nominally different than standard hardware	All
Design compartments to be locked by key	5 – Can be specified on production vehicles	Range of 1 to 3 – Minimal cost differential	All
Reduce or fill spaces that could be used to hide foreign objects	5 – Traditionally included in bus	1 – No cost	New, Overhaul
Install radiological, biological or chemical detector pagers inside bus to detect presence of these materials. The pager could be connected with the OCC	1 to 3 –New technology for this application. Not widely deployed; however, a number of projects and field evaluations are underway	Range of 5 to 10 – Acquisition cost of ownership for these technologies will be significant	All
3. Reducing the damage resulting from a threat (explosion, hijacking, fire, etc.)			
Review fire resistant and fire retardant standards (ASTM E162-02a and E662-03) for interior fixtures	3 – Can be done easily in new vehicles	Range of 1 to 4 – Materials meeting these standards generally have moderate cost increase vs. non-compliant materials	New
Harden exposed wiring and fuel lines	4 – Requires very little development investment	Range of 2 to 6 – Wide range of cost based on various strategies to limit access	New, Overhaul
Install silent alarm system (panic button) with connection to bus operations, bus destination sign, and police department	See item below	See item below	All
Design so that external destination signs and lights are integrated with silent alarm to issue alert of an emergency situation	5 – Already incorporated in base design of electronic signage	1	N/A
Place vehicle number on roof of vehicle to enhance identification from above	5 – Commonly done	1	All

Design Consideration	**State of Technology Maturity** **Scale of 1 (least mature) to 5 (most mature)**	**Cost** **Scale of 1 (low) to 10 (high)**	**Retrofit:** **New Buses / Overhaul / All**
Harden windows to prevent shattering	5 – Typical bus glazing is safety glass or polycarbonate	Range of 1 to 3	New
Provide video surveillance system	4 – Widely available	Range of 6 to 10 – Systems without wireless communications are in wide use; integration with communication system adds significant cost	All
Ensure windows are free from any coverings and provide clear view in/out	5 – Many agencies have banned covering windows with advertising wraps	1– Low	All
4. Isolating the driver from physical threats			
Enclose driver compartment	3 – Deployed to varying degrees	5	All
Provide operator shield	3 – Deployed to varying degrees	5	All
5. Hardening fuel storage compartments			
Harden fuel tanks of alternative fuel vehicles against intentional attack	4 – Most gaseous fuels are contained in roof-mounted storage vessels with limited access	3	New
6. Enhancing emergency egress through doors and windows			
Install emergency door release to allow for manual operation of doors	4	1	All
Improve window release to facilitate easier emergency egress	5	1	New
Strengthen window to be more shatterproof in case of onboard explosion	5	3	New
7. Securing the vehicle from unauthorized operation			
Design ignition system to require a keyed switch in addition to master run switch to start bus	5	1	All
Design ignition system to operate with a smart card technology that only allows permitted users to start and operate bus	5	Range of 3 to 5 – Easily integrated in current vehicle designs	All

Table 7-2. Rail Vehicle Design Solutions

Asset Components	Design Solution	Level of Difficulty	Best for New Vehicle	Feasible as Minor Retrofit
Passenger Compartment				
Seats/Wall and Ceiling Panels/Flooring	Fire resistant material that is easy to disinfect	Medium		
	Widen aisles to allow easier emergency egress	High	X	
	Lock compartment containing under-seat electronics	Low		X
	Eliminate hiding places in car or on roof	Medium/High	X	
	Modularization of components	Medium/High	X	
	Fire extinguishers in all cars	Low		X
	Fire protective sealant applied to voids where wiring or piping penetrates the floor – arrests spread of fire and smoke through openings	Low/Medium		X (for smaller fleets)
Doors	Clearly indicate emergency-release mechanism*	Low/Medium		
Windows	Harden any glass to prevent shattering – window glazing	Low/Medium		X
	Pressure panels for blast dissipation/mitigation	High	X	
	Ability to open from inside or outside	Medium		
Lighting/Signs	Battery backup*	Low		
	Emergency lighting in every car*	Low		
	Light diffusers and photo-luminescent signs made of fire resistant material*	Low		
Emergency Response Systems/ Equipment	Install silent alarms and covert microphones	Medium/High		
	Install on-board cameras	Low/Medium		
	Enable remote OCC control of on-board cameras (with proper cyber security precautions)	High		
Public Address System	Battery backup	Medium		
	Intercom in each car that allows passengers to communicate with the train crew	Low/Medium		X

Asset Components	**Design Solution**	**Level of Difficulty**	**Best for New Vehicle**	**Feasible as Minor Retrofit**
Operator Compartment				
Train Control Equipment	Key to operate	Medium		
	Kill switch for power*	Low		
	System to track train location	Medium/High		
	HVAC shut-down if outside air is contaminated	Medium		X
	Include interior mirrors for driver to see activity in the vehicle	Low		X
	OCC remote control of train functions such as power (with proper cyber security precautions)	High		
	Ability to disable unused operator compartment when the other is in use*	Low/Medium		
Communications System, including Internal/External Message Sign Control	Channel fixed radios	Low/Medium		
	Hand-held radios	Low		X
	Panic button to signal OCC, possibly with covert mike for OCC to hear activities in the vehicle	Low/Medium		
	On-board PAs and passenger assistance link	Medium		
	Vehicle-to-OCC link not only radio-based where there are tunnels	Medium/High		
	Computerized automatic communications from train-to-wayside and train-to-OCC	High		
Door Controls	Door locks*	Low		
	OCC remote control of door control (with proper cyber security precautions)	High		
	Ability to release passenger doors in an emergency when loss of power occurs*	Medium		

Asset Components	**Design Solution**	**Level of Difficulty**	**Best for New Vehicle**	**Feasible as Minor Retrofit**
Car Body/Car Control				
Car body Design	Conduct blast analysis – design implications	High	X	
	Install radiological pagers on vehicle bodies (roofs)	Medium		X
	Barriers between cars that can contain blast resistance and fire from adjacent cars	High	X	
	Paint car number on roof to facilitate identification of railcar by police and others	Low		X
	Secure any equipment compartments, interior or exterior, to prevent tampering	Medium		X
HVAC	Install smoke-clearing ventilators	Medium		
	Install radiological pagers on cars	Medium		X
	Enable OCC remote control of HVAC system (with proper cyber security precautions)	High		
Emergency Sys.	Conduct blast analysis – design implications	High	X	
Misc. Electrical	Standards for lighting in the event of loss of power that specify auxiliary backup capability	Low		

* Indicates solutions that are already prevalent in most rail vehicles.

7.6 Lessons Learned from Past Events

The security of transit vehicles is a worldwide concern. These brief descriptions of events involving vehicles can provide some insight into the issues faced by transit designers and system administrators.

7.6.1 Jerusalem, Israel

Over the past three years, there have been 15 attacks on Israeli buses, killing over 130 passengers. On February 24, 2004, the Israeli Transportation Ministry began an in-service test of components of a new security system to better protect buses from on-board terrorist attacks. Israeli Transportation Minister Avigdor Lieberman stated, "This system will help us impede the wave of terrorist attacks. It is clear that no solution affords 100 percent security."

In March 2004, five city buses in Jerusalem were equipped with portions of the system for a month-long evaluation period. The price of a turnstile, the most basic component, is approximately $2,000. A more complete set of components may cost between $20,000 and $30,000 for each bus.

The system consists of several components that can be installed individually or as part of an integrated system. The components include:

- Turnstile at the entrance to the bus: the driver is able to lock the turnstile, preventing entry to the bus, until he is satisfied that the passenger poses no threat.
- Two-way intercom: the intercom allows the driver to question a passenger before boarding.
- One-way barrier at the rear door: the barrier allows a passenger to exit through the rear door but prevents anyone from entering.
- Armor-plated glass: the glass is installed in the front of the bus shielding the driver and front row passengers.
- Sensors at the front door of the bus to detect explosives: the sensor will set off an alarm near the driver when it detects explosives within one meter of the sensor.

The FTA is monitoring the evaluation (results have not yet been provided) of this bus security system experiment and will incorporate any relevant findings into future revisions of the bus security design program.

7.6.2 Daegu, South Korea

In 2003, a fire erupted in the subway system of Daegu, South Korea. This event tragically demonstrated the value of some safety precautions that are standard elsewhere. Semi-permanent openings between cars in Daegu enabled fire to travel rapidly from car to car (barriers between cars are common in the United States). In addition, the doors in Daegu were not capable of manual operation from inside the vehicle, so that passengers inside could not open them, after the train crew closed and locked them.

7.6.3 Tokyo, Japan

In 1995, a terrorist group released sarin gas, a nerve agent, in multiple Tokyo subway trains during rush hour. Several passengers died, and over 1,000 people reportedly suffered symptoms from the attack.

As a result of the attack, one U.S. rail transit agency contacted during research for this report is now including a HVAC access button in their latest vehicle specifications. If the outside is contaminated, the HVAC can be shut down with the special button. In the case of bio-terrorism, the smoother the interior of a car, the fewer the components, and the simpler the design of the HVAC systems, the easier it will be to clean and secure the car after an attack.

7.6.4 New York, United States

Although not considered a terrorist attack, a widespread power outage in August 2003 enabled transit agencies in New York City and elsewhere to test their emergency preparedness. For example, when power was lost, low-voltage batteries maintained the emergency lighting, public address, radio, and intercom systems in NYC Transit (NYCT) vehicles. Manual override of door controls enabled the evacuation of vehicles during the power outage.

This page left intentionally blank

8.0 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.

This chapter reviews:

- General communications concerns for transit staff
- The role of **transit communications** in promoting security and emergency response
- Design-related **security measures** for transit communications systems
- **Threats** to transit communication systems
- **Protection strategies** for communication systems

Facility security, access management, cyber security, and vehicle security all impact the overall security and capabilities of a transit agency's communications system. Many of these topics are addressed in other sections of this document, and are cross-referenced where applicable.

How is this chapter useful?

For **transit managers** it is a resource for**:**

- Identifying important communications capabilities
- Considering different approaches to achieving the needed capabilities

For **security staff** it is a resource for:

- Understanding how to use communications systems in order to promote security.
- Understanding how preserve needed communications capabilities.

Each transit agency should consider how best to integrate diverse elements of a security program to support the agency's security goals.

8.1 Introduction

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:

The relationship between communications and security

- Transit communications systems are both an **asset** and a **tool.**
- Security strategies should focus on what communications capabilities are needed for both **everyday operations and for emergency response activities**, then identify **methods** of ensuring those capabilities remain available to the transit agency at all times.

- 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.

Transit agencies 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.

Security Considerations

- Communications are needed for both **everyday** and **emergency response** functions.
- Transit agencies need to be able to communicate internally, with other agencies, and with the general public.
- **Interoperability** between transit agency communications systems and other agencies is one of the biggest challenges.

8.2 General Considerations

When determining how to improve the security of an agency's communications systems, and how to use those systems to support a transit agency's role in emergency response, there are several issues to consider: the role of communications, goals, capabilities, and interoperability.

8.2.1 Role of Communications

At transit agencies, communications plays a role in managing everyday and emergency functions, coordinating system activities, and functioning as both an asset and security tool.

8.2.1.1 Managing Everyday and Emergency Functions

Communications systems are used extensively by transit agencies on an everyday basis and during emergencies. Agencies rely on communications systems to manage the movement of their vehicles, keep staff and passengers informed of changing events in real-time, and coordinate with other agencies. All of these functions are important on a day-to-day basis and are essential for smooth operations; they become even more critical, however, during emergencies and emergency response efforts, when there is a greater likelihood of confusion and timely action may be essential for protecting passengers and staff.

8.2.1.2 Coordinating Activities

Communications are essential for coordinating activity within a transit system. This is true within a single transit agency, as well as between independent agencies that cooperate to support common goals or activities. If a transit agency is to use a systems approach in its everyday operations and emergency response activities (see **Chapter 3: Security in the Transit Environment**), the ability to communicate effectively among staff members and partner agencies is vital.

8.2.1.3 Functioning as an Asset and a Security Tool

In a transit agency, communications capabilities enable transit staff to conduct normal operations. For this purpose, communications can be viewed as an asset that must be protected from any potential terrorist attack. However, communications are also an important tool that can help an agency respond effectively in case of an attack on any part of the transit system, or an attack elsewhere in the region. For this reason, the continued availability of communications is particularly important during an emergency, especially since transit agencies may also need to coordinate with outside agencies as a part of a coordinated regional response.

This dual role of asset and tool suggests that agencies should explore strategies that make their communications systems more resilient and able to withstand a variety of security events.

8.2.2 Transit Communications Goals

To allocate their resources efficiently, prioritize response actions, and maintain a high level of service, transit agency officials need to be able to effectively communicate:

- Internally, within the transit agency
- Externally, with other agencies including emergency responders
- Externally, with the public

A transit agency's goal should be to maintain communications capabilities with each of these groups, to the greatest extent possible, during everyday operations and particularly during emergency response.

Internal Communications

Transit agencies rely heavily on their communications systems to conduct everyday operations of their services; such as managing vehicle movement, informing staff and passengers about service changes in real-time, and coordinating routine activities with other agencies. A disruption in communications capabilities greatly hinders a transit agency's ability to carry out these everyday activities.

During emergencies, effective communication becomes critical in the different elements of a transit agency being able to respond to events in a coordinated manner, regardless of the type of incident.

This is particularly important during unusual events for which there may not be a pre-established protocol, and during situations when portions of the transit system become inoperable and other services must be adjusted to compensate.

External Communications with Other Agencies/Emergency Responders

At the most basic level, agencies communicate with other agencies to obtain information to enable them to make informed decisions about conducting agency activities. This may involve coordinating transit service with other transportation providers, civic agencies with a safety or regulatory function related to transit, or other organizations, or it could be as simple as obtaining updates about road construction that may affect bus routes.

Inter-agency communications become critical in situations when multiple agencies are conducting simultaneous emergency response activities. In almost all cases, all agencies need to coordinate their efforts in real-time. Ideally, this allows the agencies to be mutually supportive, and at a minimum prevents direct interference with each other. Having the capability to communicate directly and easily with other agencies helps a transit agency respond to an emergency effectively and safely.

External Communications with the General Public

Although transit agencies tend to focus on communications capabilities among their employees and with other agencies to promote security and emergency response, they also need to communicate with passengers in vehicles and stations, and with people within the agencies' wider service area. This allows agencies to inform passengers of situations and service changes as they occur, and to direct large numbers of passengers to safe locations during a transit system emergency situation.

Providing a means for passengers to contact vehicle operators or other transit staff enables passengers to inform transit staff of situations occurring in vehicles or stations of which the staff may not be aware. This greatly improves security within the transit system by empowering riders to perform passive surveillance.

8.2.3 Transit Communications Capabilities

To accomplish the transit communications goals in Section 8.2.2, transit agencies would benefit from developing certain core capabilities for their communications systems to support both everyday operations and emergency response efforts in the following situations:

- Between agency facilities and vehicles (voice and data)
- Between the transit agency and other agencies
- Between vehicles and other agencies
- Between passengers and vehicle operator

Between Agency Facilities and Vehicles (Voice and Data)

Transit agencies need to maintain voice contact between vehicle operators and the OCC or other fixed facilities, such as transit stations. This enables staff in both locations to inform each other of evolving situations, and to relay commands quickly.

Data communications with vehicles enable the OCC to track the locations and status of all vehicles equipped with appropriate hardware. In some systems, the OCC is even able to control vehicles remotely. These capabilities greatly facilitate any necessary rerouting of vehicles, and contribute to the prevention of theft and/or unauthorized operation of vehicles. For more details, refer to Section **7.5.8**.

Between Transit Agency and Other Agencies

The ability to communicate with other agencies is helpful on an everyday basis, but it becomes critical during emergencies and emergency response. Ideally, a transit agency acts as part of a coordinated citywide or regional effort to evacuate people, to carry emergency response personnel and supplies where needed, and to prevent transit vehicles from inadvertently entering dangerous areas. This is only possible when multiple agencies are able to communicate information quickly and accurately. Voice and data transmission systems not only need to maintain functionality during an emergency, but the independent systems used by different agencies need to be compatible with each other. More information is provided in Section **8.2.4**.

Between Vehicles and Other Agencies

While not yet a common feature of most transit vehicles, the ability for a vehicle operator to communicate directly with law enforcement or emergency response personnel might be a more efficient means of addressing transit vehicle situations. This is particularly relevant for buses and other vehicles operating on the road system, where they can be used as part of a flexible emergency response effort. Another option is the ability for personnel from other agencies to access real-time data feeds (e.g., video) from the vehicle, for example in the case of an on-board attack or hostage situation.

Between Passengers and Vehicle Operator

Transit system personnel regularly use on-board public address systems to inform riders about service status. These systems are also crucial for operators to provide instructions to passengers during an emergency. In-station PA systems allow staff to direct patrons to safe locations during an emergency.

Emergency call boxes in vehicles and stations enable passengers to inform transit staff of security-related incidents taking place. This greatly improves system security by involving riders in passive surveillance and enabling them to quickly report incidents to transit staff without leaving the site.

8.2.4 Interoperability

Wireless interoperability is the ability of public-safety agencies to communicate with one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed.[47] Interoperability should be a vital element of communications planning for a transit agency, particularly when planning its emergency response activities in conjunction with other agencies. Yet, it is also one of the most challenging aspects of communications for an agency to address effectively.

> "Foremost among the obstacles that can hinder an effective multi-jurisdictional response is the lack of interoperability among public safety agencies. Wireless interoperability is simply the ability of public safety officials to communicate across different wireless systems when necessary. Radio communications are often public safety personnel's only lifeline when operating in a crisis environment. Without communications interoperability, both life and property are put at significant risk."[48]

This capability becomes critical when transit agency staff must coordinate their actions with emergency responders from other agencies.

There are several technical obstacles to achieving interoperability, particularly the use of incompatible hardware by different agencies. For more details, refer to Appendix G, "Lessons Learned from Transit Communications Emergencies."

8.3 Overview of Communications Systems

Transit agencies use a wide variety of systems to transmit voice and data among their employees and with other agencies. This section provides a brief overview of the types of communication systems used.

- Wireless systems
- Wireline systems
- Operations control centers
- Public communications system
- Systems for interoperability

No one system or set of systems is perfect for all transit agencies. An agency should select a communication system based on the size of the agency service area and staff, budget, and other logistical factors.

[47] National Task Force on Interoperability and Project SAFECOM.
[48] The Role of States in Public Safety Wireless Interoperability, Public Safety Wireless Network Program.

8.3.1 Wireless Systems

All wireless systems operate using the electromagnetic spectrum – radio waves, TV waves, and radar – to send signals between devices. These waves are distinguished from one another only by frequency and wavelength.

Systems used by transit agencies include mobile radio communications, low-powered localized transponders, rail vehicle communications and control, and OTS commercial systems and equipment.

Mobile Radio Communications Systems

Most transit agencies use mobile communications systems (also known as "mobile radios") in everyday fleet operations. In normal operations these system are used for communicating with the transit vehicle operators, dispatch, monitoring vehicle location and status, vehicle rerouting, and for notification about on-vehicle emergencies.

The system is often owned and maintained by the transit agency, and consists of a base station antenna and transceiver, additional towers ("repeaters") for providing required coverage, and both vehicle-mounted and handheld transceivers. The repeaters consist of a tower-based antenna and often a housing for the transmit/receive equipment; a landline tie to the OCC is typical.

Vehicle-mounted mobile transceiver

Low-Powered, Localized Transponders

Some transit agencies use low-powered systems for very short-range operational applications. Uses include downloading bus-stored data on passenger counts when the bus returns to the garage, providing bus access to special travel lanes and to facilities like parking lots, and granting traffic signal priority to transit vehicles.

The system typically involves a low-powered transmitter aboard the vehicle that communicates with a fixed-site transponder. The transponder receives the transmitted signal from the vehicle and transmits a response or data back to the vehicle.

Rail Vehicle Communications and Control

A specialized use for short-range transponders is rail vehicle communications and control systems. Some newer transit systems even use such systems for all rail vehicle control, eliminating the need for on-board vehicle operators.[49]

These systems use a combination of wireless radio frequency (RF) communication, landlines, and commercial cellular digital packet data (CDPD) services for vehicle-to-dispatch communications, train location monitoring, vehicle identification, and emergency remote train control. On trains, data is transferred between a low-powered, on-board transponder and a series of fixed transponders situated at intervals along the rail right-of-way.

Off-the-Shelf (OTS) Commercial Systems and Equipment

Transit agencies often supplement the communications systems they maintain and operate themselves with additional, commercial systems. These OTS systems enable an agency to expand its capabilities without requiring large capital costs for equipment and infrastructure.

These systems include: cellular/mobile phone service, handheld devices and pagers, walkie-talkies, microwave links, satellite phone systems, and wireless fidelity (WiFi) networks.

8.3.2 Wireline Systems

Wireline systems (also known as landlines) normally connect two fixed points by transmitting voice and data over wires or cables, either buried or strung along telephone poles. A landline can be a dedicated system owned and operated by a transit agency, or it can be leased from a commercial service.

Systems used by transit agencies include conventional telephone systems, dedicated landlines, and high-capacity landlines.

Conventional Telephone Systems

Conventional telephone systems can be either digital or analog, and are typically routed through commercial operators’ landline systems connected to the international network.

Transit agencies use conventional telephone systems on a daily basis for many purposes: voice communications between facilities and with external agencies, fax transmissions, and low-bandwidth Internet connections.

[49] Advanced Public Transportation Systems: The State of the Art Update 2000.

Dedicated Landlines

Some agencies, especially those operating subway and/or light rail service, use dedicated landline services to directly communicate between facilities, without involving a commercial routing facility. Dedicated landlines can be owned and maintained by the transit agency or by a commercial service.

Transit agencies typically use landlines to link remote repeaters with the OCC, to link wayside transponders along rail lines with the OCC, or to establish internal analog phone systems for additional backup. Dedicated landlines can also be part of a rail vehicle control system, enabling the OCC to control the rail system's trackside signals.

High-Capacity Landlines

As transit agencies adopt new technologies for communications, parts of their communications networks rely on high-capacity landlines, which may be agency-owned or leased from private commercial vendors. These include fiber optic cables and other landlines used for high-bandwidth data transmission, computer network connections, data feeds from remote devices such as CCTVs, and Internet connections.

8.3.3 Operations Control Centers (OCCs)

Agencies manage their communications systems from their OCCs. Activities can include communicating with all fleet vehicles, dispatch, ongoing supervision of tracks and signals, vehicle tracking, communicating with external agencies, and coordinating emergency response.

These activities may or may not be integrated into a single, centralized facility. Larger transit systems may have separate OCCs for rail, bus, and other modes. For more information, refer to Section **6.3.3**.

8.3.4 Public Communication Systems

Transit agencies must be able to quickly and efficiently communicate information about incidents in facilities and/or vehicles, changes in transit service, and emergency operations to the public at large, particularly riders within their system. Intelligent 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:

- Public address (PA) systems (in-station and in-vehicle)
- Variable message sign (VMS) systems (in-station and in-vehicle)
- Emergency intercoms for passenger use (in-station and in-vehicle)
- Service area-wide broadcast methods (transit agency Web site, local media outlets)

8.3.5 Systems for Interoperability

Transit agencies must coordinate with other emergency response agencies to exchange voice and data communications quickly and accurately. Systems used by transit agencies include interoperable voice communications and data-sharing systems.

Interoperable Voice Communications

In most cases, transit agency staff will benefit from establishing wireless voice communications with other emergency responders; since this allows agency staff in vehicles and other non-stationary locations to maintain contact.

The two types of interoperable wireless communications are shared systems on dedicated spectrum used by multiple agencies, and radio communications switches that act as interpreters between incompatible systems. A third option, software-defined radios offering multiple transmission frequencies and formats, will be available in the near future.

Data-Sharing Systems

Many agencies have started to use recently developed data-sharing systems that are improving their ability to exchange data about vehicles, staff, and facility locations in real time with other agencies, and to overlay information from different agencies within a single system.

8.4 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 a transit agency's communications, agencies 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.

8.4.1 Physical Damage to Agency Equipment

A broadcast tower

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.
- **Example.** During a 1994 earthquake in the Los Angeles area, physical damage to both switching centers and telephone lines disrupted landline telephone use, which was one of several communications challenges that area transportation agencies faced.

8.4.2 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.

8.4.3 Communications Failures Outside the Agency

In addition to a power outage, other types of external failures may occur that could affect transit agency operations. Because agencies often use privately owned communications backbones or lines to supplement their own communications systems, a point of failure may lie outside of the agency's own equipment. Externally provided services, such as commercial mobile phone systems, are often an easy way to increase an agency's communications options, but transit agencies should consider system vulnerabilities. Since these systems are outside the control of the transit agency, it can be difficult to ensure sufficient measures have been taken to ensure uninterrupted service.

- **Example.** A central switching office for a telephone-service provider was destroyed in the September 11, 2001, attacks, and a large number of telephone radio towers and repeaters located atop the Towers were lost, causing a widespread loss of both conventional and cellular phone service in the area.
- **Example**. In the 2003 Northeast blackout, although equipped with backup power on-site, New York City's 911 system experienced repeated failures due to a loss of power at privately owned switching stations. Similarly, although the communications center at the Suburban Mobility Authority for Regional Transportation in the Detroit area was fully operational, the loss of its commercially provided Internet service provider (ISP) service compromised the agency's ability to schedule para-transit trips using a GIS-based computer application.

8.4.4 Network Failure from Excessive Demand

Networks are designed to carry out certain functions within certain capacity limits. Emergency situations typically generate significant demand for communications services, which can sometimes overwhelm systems even if the equipment is fully functional, especially systems shared with the general public.

- **Example.** Cingular Wireless, the second largest U.S. wireless carrier, reported a 1,000-percent increase in calls in New York on September 11, 2001. During the 2003

Northeast power outage, one transit agency's communication system was overwhelmed as field staff all tried to communicate with the operations control center at once.

8.4.5 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.

Transit agencies should consider whether their communications hardware, software, and networks are able to withstand cyber attacks. Further analysis of this issue and corresponding security strategies are beyond the scope of this document. (For more information on cyber security, refer to U.S. Computer Emergency Readiness Team's Web site at **http://www.us-cert.gov**.)

8.5 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. An agency 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. Appendix G, "Lessons Learned from Transit Communications Emergencies" describes two recent emergencies that transit agencies can learn from; the September 11, 2001 terrorist attacks on New York City and Washington, D.C., and the August 14, 2003 blackout across the Northeastern United States.

8.5.1 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.

Further analysis of access management and hardening techniques is beyond the scope of this chapter; refer to **Chapter 5: Access Management** and **Chapter 6: Infrastructure** for information.

8.5.2 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.

8.5.2.1 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 transit agency'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. Each agency 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 (see below)

Alternate Communications Center

A transit agency may consider the purchase and operation of a field-mobile communications center for use in an emergency or large special event, to replace or supplement the primary communications center. This center usually consists of a bus or truck retrofitted to include technology that allows a transit agency to perform its normal operations activities from the vehicle. Installed equipment can include radio communications, satellite communications, computer linkups, CCTV monitoring capability, and telecommunications technology.

A mobile command post

- **Example.** Both New York City Transit and New Jersey Transit used mobile communications centers—transit buses equipped with satellite and computer technology—as command posts for communications and decision making during the September 11, 2001 terrorist attacks, and again during the 2003 Northeast blackout.

Capital and operating costs of a mobile communications center can be high and may only be feasible for larger transit agencies.

8.5.2.2 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 been useful, but an independent system such as a dedicated internal phone line might have worked.

In general, prior events show that the more diverse the agency's communications technology options, the better.

- **Example.** During the Northeast power outage in 2003, having a range of options proved to be very valuable. While most forms of communications technology—VHF and UHF radio communications, train control communications, cell phones, landline telephones, Internet, and text messaging—worked at certain times during the blackout, none of them were reliable all the time.

  Some agencies found that text messaging using pagers and handheld devices was particularly effective for maintaining a communications link between the central office and field staff while network service was spotty. With the loss of power, some agencies lost their landline telephones that operated through a networked system, but those that had dedicated landlines separate from the network were able to continue to operate. For others, the conventional telephone system was their one source of communications that did not go down with the power grid.

A range of options can help ensure the ability to communicate with vehicle operators.

- **Example.** Alternate types of communications also proved valuable when a freight train caught fire in a Baltimore tunnel in 2001. The train crew was unable to contact the operations control center using the radio communications system because there was no radio signal where the incident occurred, but the train crew was able to communicate with the operations center by using a cellular phone after walking toward the tunnel portal.

As with redundancy by duplication, physical dispersion of an agency's different systems might help ensure that not all communications technologies are disabled by the same event.

- **Example.** In the 2003 Northeast blackout, an agency based in the New York City metropolitan area maintained its ability to batch-fax to partner agencies through its Florida-based faxing service.

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 scaleable, 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.

An agency 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

8.5.3 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, on-site 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 on-site 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.

8.5.4 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 Service[50] (GETS) and the Wireless Priority Service[51] (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

[50] More information on GETS can be obtained at http://gets.ncs.gov/.
[51] More information on WPS can be obtained at http://wps.ncs.gov/.

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.[52]

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.

8.5.5 Network Security

Transit agencies should consider ways to secure their electronic networks from interference. Different measures might be appropriate for different types of networks. Despite a move to integrate many systems, agencies may elect to keep certain vital systems isolated from any integrated systems. For example, train control and fare management are given special consideration by many agencies.

An in-depth discussion of cyber security is beyond the scope of this document, but transit agencies should consider options for protecting the digital elements of their communications systems. (For more information on cyber security, refer to the U.S. Computer Emergency Readiness Team's Web site, **http://www.us-cert.gov**.

8.5.6 Design Solutions

Table 8-1 lists design options for hardening the communications systems in a transit agency. Potential solutions are organized by the three main types of capabilities discussed earlier in this chapter: internal communications, external communications with other agencies, and external communications with the public. Each option either provides the associated capability or serves to help protect the systems that do.

While there are many possibilities to consider in new design or upgrade options for the system, it is important to also evaluate the feasibility of these design considerations. Given the constrained fiscal environment in which the transit industry operates, it is not sufficient to simply list the technical options that are currently available. In addition to listing design considerations, the table addresses the current state of technological maturity and of the feasibility of those considerations. There are issues of initial cost, available space, and the ongoing maintenance responsibilities that accompany the selection of any of these design options.

[52] In its own assessment after the blackout, the City of New York reported difficulties accessing the GETS system. This may have been due to the electrical outages impacting equipment.

Table 8-1. Security-Oriented Design Considerations for Communications Systems

Design Solution	**State of Technology Maturity** Scale of 1 (least mature) to 5 (most mature)	**Cost** Scale of 1 (low) to 10 (high)	**Design Goal** (Detect/deter/ minimize)	**Retrofit**	**Feasibility** Scale of 1 (easy) to 3 (hardest)
INTERNAL COMMUNICATIONS: MOBILE RADIO SYSTEM					
Communications System Control Center (Base Station)					
Mobile Communications OCC with redundant capability	3 - currently deployed to varying degree by largest transit agencies	Range of 5 to 8 - wide range of costs depending upon technology installed	Detect, Minimize, Deter	Maybe	3 (expensive, possible space issues)
Provide power supply backup generators): UPS, gas, electrical	4 - mostly mature, with wide range of types of backup power supplies available	Range of 1 to 8 - a wide range of costs depending on type of backup system used and amount of technology protected	Minimize	Yes	2 (requires routine maintenance)
Provide redundant base station antenna* on roof or separate tower	5 - mature technology, but requires additional infrastructure	Range of 5 to 8 - the costs depend upon whether the agency is able to use its own facilities for the towers	Minimize	Yes	2 (expensive, possible space issues)
Remote (Repeater) Towers, Transceivers					
Provide perimeter protection to towers/equipment shelter	5 - mature technology	Range of 1 to 4 - costs can be relatively low	Minimize	Yes	1
Provide power supply backup	4 - mostly mature technology	Range of 3 to 8 depending upon how extensive the backup system is and what components are included	Minimize	Yes	1
Provide protection to antenna to shelter cabling	5 - mostly mature	Range of 2 to 4	Minimize	Yes	1
Provide redundant landline connection to base station	5 - mature	Range of 3 to 8 depending on the infrastructure requirements; also requires monthly operating costs	Minimize	Yes	2 (expensive)
Mobile Transceivers – vehicle mounted					
Limit access to devices	5 - mature	Range of 1 to 4	Minimize	Yes	1

Design Solution	**State of Technology Maturity** Scale of 1 (least mature) to 5 (most mature)	**Cost** Scale of 1 (low) to 10 (high)	**Design Goal** (Detect/deter/ minimize)	**Retrofit**	**Feasibility** Scale of 1 (easy) to 3 (hardest)
Assign emergency channel with push-button access	4 - mostly mature	Range of 2 to 5	Detect, Minimize, Deter	Yes	1
Install silent alarms and covert microphones	4 - mostly mature and becoming standard installation during bus purchases	Range of 4 to 8; the costs depend upon when the installation (new or retrofit) is done and the extent of the alarms	Detect, Minimize	Yes	2 (expensive)
Mobile Transceivers – handheld					
Limit access to devices	5 - mature	Range of 1 to 4	Detect, Minimize, Deter	Yes	1
Assign emergency channel with push-button access	4 - mostly mature	Range of 2 to 5	Detect, Minimize, Deter	No	1
Walkie-talkies/pagers					
Limit access to devices	5 - mature	Range of 1 to 4	Detect, Minimize, Deter	Yes	1
INTERNAL COMMUNICATIONS: LANDLINES					
Remote Repeaters to OCC					
Provide redundancy	5 - mature	6 - costs involve both capital and ongoing operating costs	Minimize	Yes	2 (expensive)
Along rail right-of-way with linkage to OCC					
Provide redundancy	5 - mature	6 - costs involve both capital and ongoing operating costs	Minimize	Yes	2 (expensive)
EXTERNAL COMMUNICATIONS: WITH EMERGENCY RESPONDERS/EMERGENCY RESPONSE CENTER					
Interoperable Wireless Communications System					
Develop common system with emergency response agencies	1 - a technology that is rapidly evolving but lacks common industry standards	Range of 5 to 10	Detect, Minimize	No	3 (spectrum issues, cost)

Design Solution	**State of Technology Maturity** Scale of 1 (least mature) to 5 (most mature)	**Cost** Scale of 1 (low) to 10 (high)	**Design Goal** (Detect/deter/ minimize)	**Retrofit**	**Feasibility** Scale of 1 (easy) to 3 (hardest)
Landline/conventional phone system					
Use dedicated landlines and conventional phone system	5 - mature	2	Detect, Minimize	Yes	1
Cell phones					
Use commercial mobile service	5 - mature	2	Detect, Minimize	Yes	2 (service availability issues)
EXTERNAL COMMUNICATIONS: PASSENGER INFORMATION IN STATION					
Station Public Address System/Message Sign Control*					
Redundant hardware and wiring	4 - mostly mature	Range of 4 to 8 - can be expensive depending upon the station infrastructure	Minimize	Yes	1
Battery backup	4 - mostly mature	Range of 4 to 8 - can be expensive depending upon the station layout and installed technology	Minimize	Yes	2 (cost)
EXTERNAL COMMUNICATIONS: PASSENGER INFORMATION IN VEHICLE					
Vehicle-based Message Sign Control/Crew-Passenger Communications*					
Intercom in each car allows passengers to communicate with the train crew	4 - mostly mature	4	Detect, Minimize	Yes	1
Handheld crew radios with comm. switch	5	4	Detect, Minimize	Yes	1
On-board PAs and passenger assistance link	5	3	Minimize		
EXTERNAL COMMUNICATIONS: SERVICE AREA BROADCAST					
Web-based notifications; TV, radio notifications	4 - maturing technology seeing increasingly innovative applications	1- the costs are low	Minimize	Yes	1

This page left intentionally blank

9.0 Security Systems Integration

Enhanced security in the transit environment depends on three elements:

- Appropriate design, of the physical objects that together form the transit system, as discussed in previous chapters
- Relevant information and data, such as video images, being collected and delivered to appropriate decision makers
- Training and focus on human factors to maximize deterrence, detection, minimization, and response/recovery

Security systems integration is essential if these factors are to work together. Security systems integration implies that all types of systems and their subsystems are *linked together* to enhance transit system security.

How is this chapter useful?

For **transit managers and security staff** it is a resource for:

- Understanding the concept of systems integration
- Understanding how higher levels of systems integration enhance transit system security
- Identifying the methods and tools needed to achieve well-integrated systems

This chapter defines a methodology for achieving systems integration and helping agencies meet the challenge of building integration into the systems design. The chapter reviews:

- Systems integration as an overall concept
- Systems integrations from a project perspective:
  - **Benefits of systems integration**
  - **Transit agency experience with systems integration**
  - **Methods and tools used to achieve integration**
- **Systems integration from the point of view of the decision maker,**
- **Systems integration from the point of view of the agency's system development management process,**
- **The importance of security systems integration**

Chapter 2: A Systems Approach to Security Design describes the need for a systems approach in designing transit security systems. This chapter defines and describes "system" in the context of the transit security system and systems integration as an outcome of the system development process and focuses on the "how-to" of systems integration.

9.1 The Challenge of Integration

Systems integration in the initial stages of a security systems project is a conceptual as well as a technical challenge. Key decisions relating to system boundaries, interfaces, and architecture are made early in the development process. The implications of these decisions may not be apparent until later stages of the development cycle when the system is about to be deployed.

To examine the challenge of applying the concept of integration to an actual transit security system development project, this chapter begins by defining transit security system and systems integration as an outcome.

9.1.1 Transit Security System

A system is a set of interrelated components that interact in an organized fashion toward a common purpose. System components may be quite diverse, including:

- Persons and organizations
- Software and data
- Equipment and hardware
- Facilities and materials
- Services and techniques[53]

A transit security system encompasses all physical and logical components that contribute to the safety and protection of a transit system's sites and assets. System components include physical barriers, staff credentials, electronic devices, software applications, data management, telecommunications equipment, and security personnel.

The function (output or product) of a system is the organizing principle that links disparate parts and determines which parts are needed, how they should be organized, and how they should be linked.

The transit security system also interfaces with other systems, such as facilities management, personnel management, and emergency services communications systems. For any security system project, the systems integration perspective can be used to evaluate how the capabilities of the security component being considered for installation relate to the capabilities of other associated elements. Agencies can then either immediately implement the link between components or defer the connection. In either case, the potential link should be recognized early in the design process and the "now or later" implementation decision should be made explicitly.

[53] Adapted from: James Martin, "Systems Engineering Overview" **www.incose.org/ntexas/meetings/0004what_is_se.ppt**.

Figure 9-1 illustrates the system architecture for a generic transit security system.

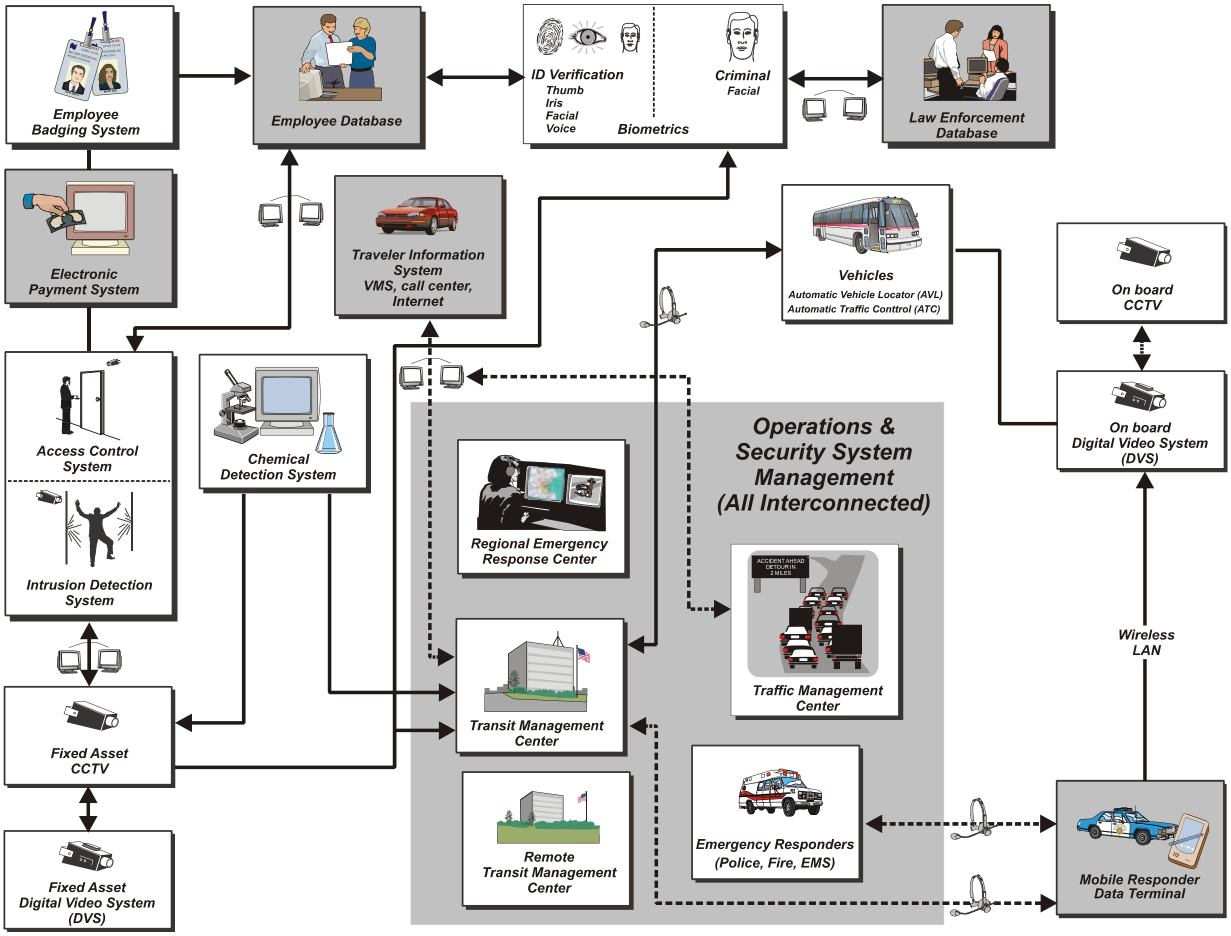


Figure 9-1. FTA Generic Security Architecture

Ideally, the integrated transit security system is a real-time networked data system linking all functional elements to decision support software and/or to decision makers. If a communications and data management infrastructure is used to achieve systems integration, the integrating infrastructure itself must also be secured; and information and relevant cybersystems security included in transit security planning objectives. Dimensions of information security include such items as hardening information communications infrastructure, access control to infrastructure, protection of mass storage media, disaster recovery measures, routine back-up procedures, and continuity of operations plans and procedures.

9.1.2 Systems Integration as an Outcome

The outcome of systems integration for a transit agency is systems and equipment that are able to effectively intercommunicate.

Systems integration applies both to how the security system's components work together as a whole toward the intended function, and to how the security system communicates with other systems having related transit functions. Federal standards define systems integration as the "progressive linking and testing of system components to merge their functional and technical characteristics into a comprehensive, interoperable system. …[The] integration of data systems allows data existing on disparate systems to be shared or accessed across functional or system boundaries."[54]

High levels of transit security systems integration lead to timely and relevant information transfer among both security and non-security systems, and contribute to improvements in:

- Deterrence: measures that discourage a terrorist from acting
- Detection: measures that discover and identify the nature of a terrorist attack
- Minimization: measures that mitigate against the destructive and injurious effects of an attack[55]
- Response: measures that enable officials to counteract the terrorist attack, and to protect the public
- Recovery: measures that enable the system to resume normal operations

When looking at the outcome of systems integration; there are two important questions: "How do you know when you have reached the goal of an integrated system?" or "what are the characteristics of such a system?" and "What methods can be used to reach a high degree of systems integration?" The following subsections address these questions.

9.1.2.1 Characteristics of an Integrated System

In the same way that a system has multiple facets, systems integration occurs over spatial, temporal, institutional, functional, and data dimensions.

An integrated system has the following characteristics:

- Information generation: synthesizing data into information that can be used for decision making; for example, automatically identifying suspicious activity by flagging anomalies in a stream of visual or auditory data

Systems integration provides networked, real-time data collection, management, and dissemination for decision support to all relevant institutional players.

[54] ANS T1.523-2001, Telecom Glossary 2000 is the update and revision of FS-1037C, Telecommunications: Glossary for Telecommunications, http://www.its.bldrdoc.gov/fs-1037/.

[55] The ability of integrated systems to minimize the immediate effects of an attack in progress is indirect. Most minimizing countermeasures are items like standoff zones around facilities and hardening building structures.

- Communication: delivering the information to relevant decision makers, including external agencies and the public, where applicable
- Multiple internal and external organizations: linking multiple agencies enabling coordinated action
- Multiple devices: linking multiple devices, including single types of devices from multiple vendors and multiple types of devices; for example, an attempted unauthorized access could trigger video camera surveillance
- Multi-directionality: enabling multi-way communications among devices and control centers where needed
- Redundancy: maintaining the functionality of a security system during an attack is critical, especially if one part of the system has been disabled
- Persistence: preserving the ability to investigate past system states

9.1.2.2 Measures of Integration

Integration is more than an all-or-nothing attribute of systems. It can be present in degrees and can be implemented as part of a phased system-development process. Agencies can evaluate the degree to which integration is achieved within a system based on the following system characteristics:

- Real-time information
- Real-time communication
- Comprehensiveness
- Interoperability

Real-time Information[56]

The integrated security system will need to present data about an event from multiple sources, as close to the beginning of that event as possible. The data will need to be transmitted in a form that matches the requirements of the organization, person, or system receiving it.

Systems integration as an outcome can be recognized when the system provides *timely, actionable information* to organizational entities that did not have that information available prior to system implementation.

An integrated security system will also need to be able to archive data being collected, for later investigation and analysis. In the event of an attack or attempted attack, past data should be available to investigate possible prior probes and tests made by the attackers.

[56] Most dictionary definitions regard data and information as synonyms; however, a distinction between "data" and "information" is useful and is maintained in this document. "Data" refers to a structured representation of the real world, including ideas and opinions, that is amenable to analysis by humans or by machines. Information is data that has been analyzed or further structured so that it has meaning (or semantic content) for human beings and is actionable.

Real-Time Communication

Communications is both a means and an end of transit security systems integration. Data and information are transmitted among diverse system components to integrate the actions of those components. The communications channels used by the security system may also be used to transmit information to system staff, external agencies, and the public during an attack.

To deliver the density of real-time data needed to ensure transit security, the security system must be capable of sending large amounts of data at high speeds. This speed is determined by how long the data takes to travel across the network, and the amount of time the data may be held at the originating device and intervening nodes before being transmitted.

Comprehensiveness

Comprehensiveness refers to the full scope of a security system's capabilities. This is not evaluated as the sum of the capabilities of individual system components, but rather as how the components communicate among each other to achieve desired ends. The degree of integration present in a system depends on whether it has interfaces to systems that have related functions. If a system has no interfaces, then the information it produces cannot be leveraged to other uses.

Interoperability

Interoperability is: "the ability of two or more systems or components to exchange information and to use the information that has been exchanged."[57] Interoperability can be a matter of degree and of the observer's point of view. If a system can accommodate diverse devices and enable them to communicate functionally, the degree of interoperability is high.

The ability of systems to interoperate is usually dependent on the existence of and adherence to accepted, widely distributed standards, which are discussed in Section 9.4.3. A transit security example of interoperability is a video surveillance system, where the components may have been acquired from different vendors at different times, but can all be networked to a central monitoring facility.

> Interoperability is: "the ability of two or more systems or components to exchange information and to use the information that has been exchanged."

9.2 Benefits of Integration

Integration benefits result both from the avoidance of the opportunity costs of building stovepipe systems and the increased efficiency resulting from the ability of integrated systems to improve the delivery of transit services and enhance security.

[57] Institute of Electrical and Electronics Engineers. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York, NY: 1990.

Since there are few transit projects with a strong systems integration focus, there are few quantifiable measures of the benefits of integration in the transit industry. However, the experience of the aerospace industry and other industries developing large-scale integrated systems, provides some measures of the kinds of benefits for transit security.

These include:

- Reduced maintenance costs
- Integrated future system enhancements
- Enhanced cost distribution across functions
- Inter-organizational coordination
- Economies of scale
- Fast delivery of information
- Leveraged specialized expertise
- Visibility of security issues
- Continuous technology improvements
- Application to other systems
- Avoidance of installation failures

Reduced Maintenance Costs

Respondents at agencies with multiple systems performing the same function in different locations report that the costs of training personnel to maintain diverse systems exceed a desirable level. More uniformity in devices and communications architecture will ease the agency's ability to maintain the security system.

Integrated Future System Enhancements

With the development of new transit facilities, such as a new transit line, a transit property with multiple security system architectures must evaluate how each of these system architectures will be integrated with the new system. If there has been a more uniform implementation for all of the project architectures, the evaluation of integrating new systems architectures is likely to be more straightforward.

Enhanced Cost Distribution Across Functions

Security consultants and studies emphasize the benefits of multipurpose systems. One such study, completed by the National Research Council (NRC), calls for "security methods and techniques that are dual-use, adaptable, and opportunistic." These methods "mesh security with other operational tasks and objectives, such as curbing crime, dispatching and tracking vehicles, monitoring the condition of infrastructure and assuring safe operations."[58] A major benefit is the ability to

[58] National Research Council, op. cit., p. 220.

distribute costs among different cost centers. For example, one transit agency uses the same smart card technology for fare collection and facility access control; thus, distributing the costs of acquiring and maintaining this technology across functions.

Inter-organizational Coordination

From debriefings of transit and transportation agency response in New York, New Jersey, and Connecticut on September 11, 2001, it is clear that inter-organizational and interpersonal relationships developed prior to that date were instrumental to the impressive system response, even in the face of the failure of many communications channels. Early and continuing stakeholder input over many projects increases the ability of system personnel to mount a robust response to major incidents.

Economies of Scale

Related to the reduction of maintenance costs, total system development life cycle costs can be reduced by increased system integration and the replication of security system elements throughout a transit network. In the past, piecemeal solutions have been implemented by transit agencies because resources could not be obtained to acquire system-wide solutions. Nevertheless, the case can be made that the total cost of ownership of an integrated system will be less than the sum of the costs of ownership of multiple non-integrated systems.

Fast Delivery of Information

A respondent described the ideal video surveillance system as delivering images to the operations, police, and safety units. Another respondent stressed that images produced by video systems installed in transit vehicles must be viewed in real-time by the transit police, so that law enforcers can respond as quickly as possible with as much information as possible. Integrated systems have the potential to increase the ability to quickly deliver information to the parties that need it when they need it.

Leveraged Specialized Expertise

Systems integration is a function of the convergence of communications, information, and electronic technologies with transportation system elements. Specialized expertise is needed to implement these systems. Regardless of whether this expertise is in-house or outsourced, increased systems integration means that the level of expertise can be leveraged across individual projects. If heterogeneous systems are installed, the opportunity to build the expert capability can be lost.

> A standards-based architecture allows for upgrades using industry-wide procedures and is not dependent on the continued support of a single vendor.

Visibility of Security Issues

In conversations with transit officials, the perceived relevance of transit security systems for countering terrorism is low (except in the case of the largest systems in cities assumed to be terrorist targets). One respondent even called security "an afterthought." Transit agencies remain focused on everyday concerns, such as crime prevention. An integrated approach that treats security issues along with crime prevention, safety, and other concerns will help keep security on the table as a function of new access control, video surveillance, and other systems being planned.

Continuous Technology Improvements

The systems engineering approach takes into account future developments in technology, enhancing the ability to integrate future enhancements. A known architecture built of elements based on standards presents an upgrade path that is not possible with heterogeneous systems or with many proprietary systems. A standards-based architecture allows for upgrades using industry-wide procedures and is not dependent on the continued support of a single vendor.

Applications to Other Systems

The systems integration processes applied to transit security systems can be used for other transit-related systems using convergent technologies. As with other benefits of systems integration listed in this subsection, the process and technical expertise acquired by the transit agency can be applied to other agency development projects that incorporate increasing levels of digital and communications technology. A prime area of convergence are the technologies used in ITS.

Avoidance of Installation Failures

Agencies have a greater chance of avoiding system failures in implementing transit security systems, if they use the systems engineering process and focus on building systems integration into the system. For example, the defective installation of properly specified equipment can be avoided if the systems engineering process institutes quality assurance controls and if the agency recognizes that the specifications for installing the device were as important as the specifications for the device itself.

9.3 Transit Agency Experience with System Integration

Transit industry respondents report that their agencies operate with highly insular organizational structures. New projects are run from the perspective of "getting the job done at the lowest cost" and fending off interference from other agency departments. Most transit agencies make contract awards to the lowest cost bidder without a separate assessment of the technical merit of the proposal. Without close attention to the technical parameters of the procurement, the procurement method may not be adequate for evaluating issues like future expandability and interoperability.

A principal benefit of building integrated systems is institutional. Once organizations begin working together on technology-centric issues, the lines of communication begin to be created for intra-agency cooperation around other strategic and operational issues.

Systems integration is seen as expensive, time consuming, and placing potential barriers in the way of completing a project. One networking official observed that although his shop had responsibility for the design and operations of the OCC, new security systems being installed were not integrated with OCC operations. Another operations executive mentioned that new train control systems were kept from the communications networking unit.

Transit professionals report that systems expertise is most available from systems service and equipment vendors. However, the vendors promote proprietary systems that are not likely to be interoperable with future systems to be installed. Transit agencies reportedly lack the detailed technical knowledge about information technology and telecommunications to write procurement specifications that hold vendors to open standards. Agencies have found that the vendors offer their proprietary systems at cheaper costs than systems with a higher capability for interoperability. One large transit agency was reported to have installed a series of proprietary access control and video surveillance systems over time, none of which interoperate with each other.

Interoperability can lead to an increased ability to use a single technology for different purposes. Examples of leveraging technological installations among various functions in a transit agency include:

- Voice and text communications between operations center and bus operators
- AVL monitoring through laptops and from police vehicles and traffic helicopters
- Linking environmental and power control systems, such as heating, ventilation and air conditioning (HVAC), to security control operations based on information about an incident
- Establishing a back up operations center with back-up power

Respondents for this study agree that transit agencies tend to be divided into silo organizations, which are turf-conscious and often not overly willing to share information across organizational lines. A principal benefit of building integrated systems is institutional. Once organizations begin working together on technology-centric issues, the lines of communication begin to be created for intra-agency cooperation around other strategic and operational issues. Practiced communication will be essential in responding to a serious incident.

9.4 Systems Integration Toolkit

Section 9.1 describes systems integration as a desired outcome. This section describes the processes, methods, and tools that can be used to achieve systems integration, and how they lead to a definition of the security systems project that is comprehensive and holistic, and that takes into account the present and future requirements of related external systems.

The section defines and describes the following concepts:

- The integration process
- Systems engineering

- Standards
- System architecture

9.4.1 The Integration Process

It is tempting to think of systems integration as assembling the subcomponents of a system or joining the system through interfaces to other systems. However, systems integration begins before the project comes into formal existence. Without the ability to integrate being designed into the system requirements, the ability to integrate the system with other systems in its environment is reduced.

Agencies should consider starting the integration process before identifying and defining a particular project.

This subsection outlines the steps that agencies should consider for achieving systems integration, both at the beginning and at the ending stages of the system development life cycle. These include defining system scope and characteristics of the integration process.

9.4.1.1 Defining System Scope

The critical step toward an integrated system is determining what to include as part of the system. It is essential to promote an inclusive perspective. Even if practical limitations restrict the scope of any final implementation, a comprehensive view should inform the planning process.

Factors to consider include:

- Stakeholders
- Time horizon
- Spatial elements
- System lifecycle

Stakeholders

Identifying stakeholders and collecting their input is the first step in system definition. Depending on their roles within the security infrastructure and the transit system at large, different stakeholders may have very different perspectives on what should be included in the definition. If only a narrow set of perspectives is used to determine system boundaries, then opportunities for leveraging the system and making functional links with other systems may be missed. Relevant stakeholders may include any staff at transit agencies and other agencies working in the areas of information technology, telecommunications, ITS, transit police activity, facilities planning and construction, maintenance, and transit operations

Time Horizon

Based on past transit system experience with technology, system designers can expect that budget constraints and institutional conservatism will lead to transit security systems remaining in service for as long as practicable, despite expected lifetimes, or advances in technology. It becomes critical that agencies consider extending systems operation analysis well into the future with no limitation of existing conditions or technology.

Predictive analysis enhances the ability of the security system to adapt to changes in many factors, including:

- Size of the transit system (ridership, assets)
- Configuration of the transit system
- Transit system service demographics
- Technology (ITS, information systems, communications, security systems)
- Level of terrorist threat and public expectations of adequate threat response

Spatial Element

Agencies should consider inspecting the expected physical scope of the security system in tabletop exercises and on the ground in the earliest stages of system definition. System planners should be as inclusive as possible. Agencies should also consider not constraining spatial dimensions by organizational or institutional boundaries. Where a transit facility is co-located with a facility owned by another agency or company, it is critical for the security plan to indicate the existence of the adjacent facility and exploit opportunities for linking security systems where possible.

> Any particular instance of a security installation project may not encompass an entire system, but system planners should understand how that project affects, and is affected by, the rest of the system.

System Life cycle

Life-cycle activities, from system conception through system retirement, are usually presented in a list as if they occur linearly. In practice, these activities are often iterative, can be simultaneous, and are driven by negotiations among system stakeholders, developers, and sponsors. Agencies should consider continually revisiting system boundaries at each milestone in the lifecycle, to ensure the existing plan reflects any new information or decisions added in the course of development.

Overall, the inclusion of relevant stakeholder representatives and adopting a wide view of system boundaries will encourage the development of an integrated system. This counters the tendency to pursue stovepiped development that narrowly draws system boundaries to minimize the technological and political challenges that arise. The development of an integrated transit security system requires that, at a minimum, connectors be built among the stovepipes, but ideally that stovepipes not be built at all.

9.4.1.2 Characteristics of the Integration Process

Successful integration is made up of the following characteristics:

- Top-down and bottom-up
- Application of standards
- Use of systems engineering
- Construction of a systems architecture
- Layered, phased approach

Top-down and Bottom-up

Producing an integrated system should be both a top-down and bottom-up process. Top-down analysis focuses on the big picture, and is especially important in the initial planning, analysis, and design phases of development. A top-down focus promotes an integrated design that can accommodate later expansion through the addition of more device types or data types.

Bottom-up processes address the separate components, which must be integrated into a functional whole. This is particularly relevant in the last stages of the development, when the integrated system is assembled, tested, and implemented.

Application of Standards

Standards can be applied to the components that are developed, as well as to the process used to achieve integration. The use of standards to drive the process will help ensure that the activities needed to produce an integrated system are carried out and that all stakeholders are aware of the reasons for the activities. (See Section **9.4.3**).

Use of Systems Engineering

This document proposes the use of the systems engineering methodology as the standard for developing an integrated transit security system. (See Section **9.4.2**)

Construction of a System Architecture

Creating a security system architecture provides a context for the design of individual projects and increases the likelihood of a high degree of systems integration. The National ITS Architecture will be the framework of the system architecture, where applicable. (See Section **9.4.4**)

Layered, Phased Approach

The application of a layered, phased approach to developing an integrated transit security system produces an architecture that has distinct building blocks or subsystems, and can be phased in over time.

9.4.2 Systems Engineering

Systems engineering is a methodology for achieving integration. System engineering expert James Martin describes the method as:

- An approach which views the entire system of components as an entity rather than simply an assembly of individual parts…a component designed to work properly with other components rather than to function by itself.
- A methodology that can be applied across engineering disciplines and is now considered a discipline in and of itself.
- A way of thinking that is holistic.[7]

The key objectives of systems engineering do not involve building or assembling the actual system components, but instead focus on ensuring that integration is built into the system. Systems engineering objectives and activities may be considered as being "above-the-line"; having a higher-level, holistic, and integrative perspective. Designing and constructing the detailed components of a system may be thought of as lower-level or "below-the-line."

Systems engineering (or "above-the-line") objectives include:

- Goals/Concept of Operations (ConOps). Identification and quantification of system goals.
- Design and Architecture. Creation of alternative system design concepts and performance of the selected design concept.
- Integration Test: Verification that the design is actually built and properly integrated in accordance with specifications.
- Validation: Assessment of how well the system meets the goals.[8]

What is Systems Engineering?

The systems engineering method provides a disciplined focus on the end product, its enabling products, and its internal and external operational environment (i.e., a system view) both at the beginning and end stages of the systems project.

It also provides a consistent vision of stakeholders' expectations independent of daily project demands (i.e., the system's purpose).

9.4.2.1 Concept of Operations

To guide the process, agencies should consider developing a concept of operations (ConOps) document as a guide. The ConOps is a critical document that describes the characteristics of the to-be-delivered system from the users' viewpoint, and communicates the overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements. It describes the user organization(s), mission(s), and

[7] Adapted from: James Martin, "Systems Engineering Overview" www.incose.org/ntexas/meetings/0004what_is_se.ppt.
[8] Ibid.

organizational objectives from an integrated systems point of view.[9] This could be an initial step to plan the introduction of a transit system credential.

The following subsections describe the systems engineering method. Section 9.4.2.2 describes the "vee" model which distinguishes systems engineering from component engineering and Section 9.4.2.3 gives a brief discussion of the activities and their products contained in the engineering activity flow. Other sections describe how development and device standards and the system architecture contribute to systems integration.

9.4.2.2 The "Vee" Model of System Development

A key concept in systems engineering, the "Vee" model is an approach that takes into account both a "bottom-up" and "top-down" perspective. (See **Figure 9-2**.) This model also illustrates the difference between systems engineering and component engineering. Note that the "above-the-line" activities match the objectives presented in Section 9.4.2.

The top-down portion of the Vee on the left of Figure 9-2 represents activities that define the system and its components in greater and greater detail, but with continual attention to the overall goal of the whole system. The bottom-up portion of the Vee on the right represents activities that build an integrated system, by assembling the lowest discrete components into modules, modules into subsystems, and so on, with continual verification that the components meet requirements of the entire system.

The vertex of the Vee represents the phase in which the component parts are built, acquired, or assembled. This approach should be applied to the whole system, as well as to each successive layer of components that make up the system. The development process is therefore a series of Vee's that are applied to each of the building blocks (and sub-building blocks), as well as to the whole.

[9] IEEE P1362, *IEEE Guide for Concept of Operations Documents*, Draft 3.1, 4 January 1998.

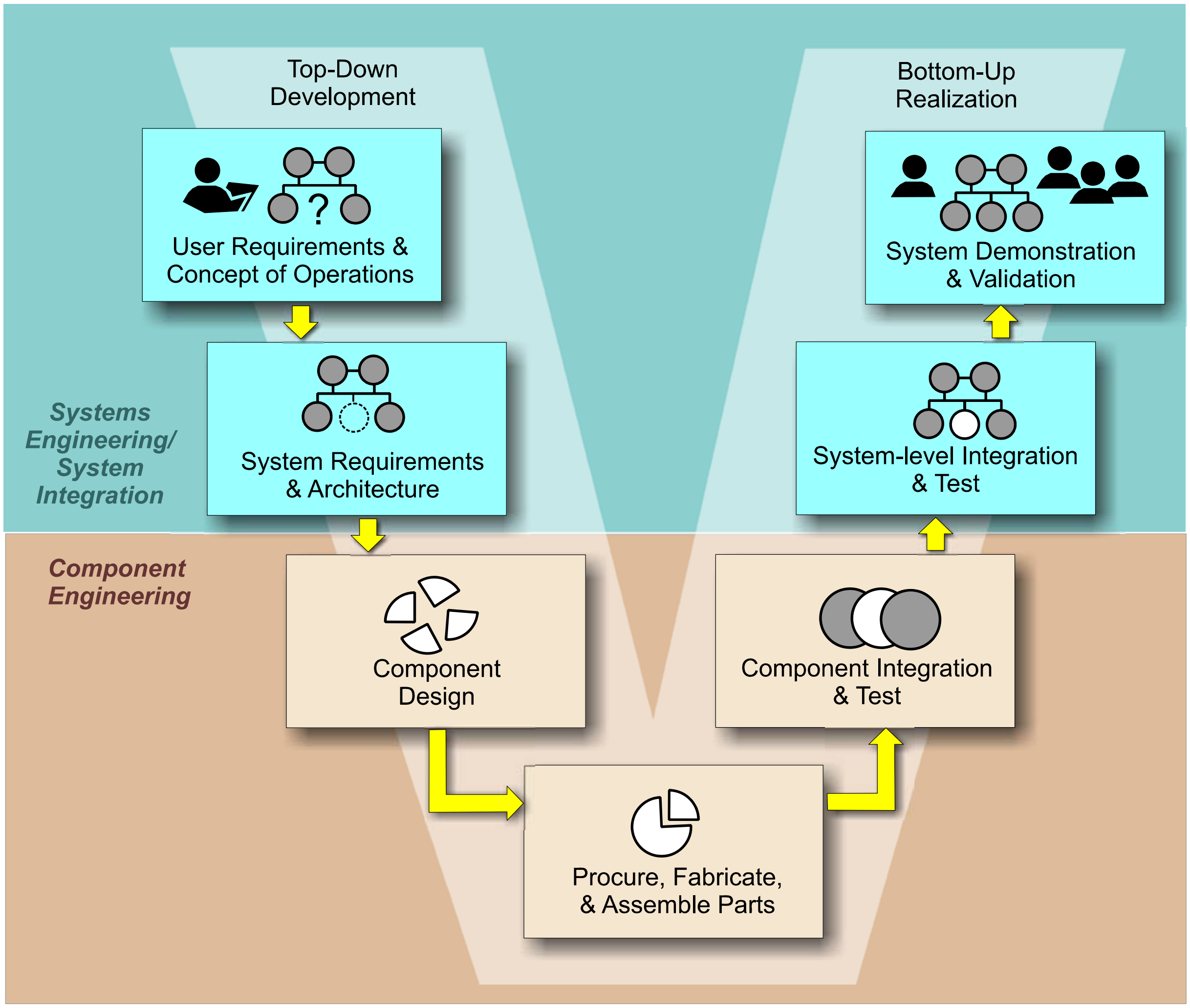

Top-Down Development
Bottom-Up Realization
User Requirements & Concept of Operations
System Requirements & Architecture
Component Design
Procure, Fabricate, & Assemble Parts
Component Integration & Test
System-level Integration & Test
System Demonstration & Validation
Systems Engineering/ System Integration
Component Engineering

Figure 9-2. "Vee" Model of System Development[10]

9.4.2.3 Engineering Activity Flow

The systems engineering activity flow[11] in Table 9-1 provides more detail on the range of activities needed to produce an integrated system. The table lists the questions and sample outcomes from each activity that should be answered at each flow step. The last column relates the activity to the systems engineering objectives listed in Section 9.4.2 and the "Vee" model of system development in Figure 9-2.

[10] Martin, op. cit.
[11] Adapted from Martin, op. cit.

Table 9-1. Systems Engineering Activity Flow

Engineering Activity	Example Questions Posed in Step	Examples of Step Outcomes	System (S) or Component (C) Engineering Activity
Need	What needs are we trying to fill? What is wrong with the current situation? Is the need clearly articulated?	Project Charter System Acquisition Documents	S (Goals/ConOps)
Operational Concept	Who are the intended users? How will they use our products? How is this different from the present?	Concept of Operations	S (Goals/ConOps)
Functional Requirements	What specific capability will we provide? To what level of detail? Are element interfaces well defined?	User Requirements	S (Goals/ConOps)
System Architecture	What alternative designs exist to fulfill user requirements? What criteria will be used to choose among the alternatives? What is the overall plan of action? What elements make up the overall approach? Are these complete, logical, and consistent?	System Design	S (Design and Architecture)
Allocated Requirements	Which elements address which requirements? Is the allocation appropriate? Are there any unnecessary requirements?	Technical Requirements	S (Design and Architecture)
Detailed Design	Are the details correct? Do they meet the requirements? Are the interfaces satisfied?	Sub-System/ Component Specifications	C
Implementation	Will the solution be satisfactory in terms of cost and schedule? Can we reuse existing pieces?	Sub-system/ Component Construction/ Acquisition	C
Test and Verification	Has the as-built system met specifications? Do components function as a whole according to the design?	Test Results Integrated System	S Integration Test
Validation	Does the system meet customer goals? Does the customer accept the system?	Acceptance Test Results Deployed System	S Validation

Note:
Shaded columns denote component engineering "below-the-line" activities
Unshaded columns denote systems engineering "above-the-line" activities

9.4.3 Standards

Standards reflect agreements on products, practices, or operations by nationally or internationally recognized industrial, professional, trade associations, or governmental bodies.[64] The use of standards can contribute to systems integration by increasing the likelihood that the subsystems or modules can be assembled into an integrated system without further rework and that the system will be able to link with related systems.

Standards and System Integration

The use of standards can contribute to systems integration by increasing the likelihood that the subsystems or modules can be assembled into an integrated system without further rework and that the system will be able to link with related systems.

Standards can apply not only to hardware, data formats, and communications protocols, but to the systems-development process and other processes, such as risk management and quality assurance. System development standards can increase the likelihood that a developed system will show a high and functional level of systems integration.

While the use of standards may be a necessary precondition for systems integration, they are not sufficient. There are typically multiple standards for any field, and the choice of standards can be confusing given the profusion of organizations managing the development and publication of standards, namely the standards development organizations (SDOs), national versus international standards, standards that cross engineering disciplines, and evolving standards that are in a continual cycle of playing catch-up with advanced digital and telecommunications technologies.

A key to selecting standards is to determine which existing published and unpublished standards are the actual, current, de facto standards in the transit operations and transit security communities. This is best accomplished by peer-to-peer communication.

Examples of relevant standards and associations for systems integration include ITS standards, other applicable systems development standards, and SDOs.

9.4.3.1 ITS Standards

ITS applies digital, communications, and electronic technologies to transportation operations. To accelerate the deployment of ITS technologies, the U.S. Department of Transportation has sponsored the development of a series of standards that are applicable to ITS projects. These standards address the full range of system components, including communications protocols, communications interfaces, data dictionaries, and message sets. They are based on open technologies and are meant to reduce reliance on proprietary systems.

The Transit Communications Interface Protocols (TCIP) are ITS standards that address the data communications requirements for public transportation, including the exchange of information

[64] From Federal Standard 1037C. See **http://glossary.its.bldrdoc.gov/fs-1037/dir-034/_5071.htm**.

among public transit vehicles, transit operations centers, external agency operations centers, and other transit facilities. These standards are being used in field operational tests.

9.4.3.2 Other Applicable System Development Standards

Achieving systems integration depends on communication, either as part of the system being implemented or as a means to determining how all system elements (such as mechanical or electromechanical devices) should be integrated.

Examples of standards related to the process of system development include:

- EIA 632, Processes for Engineering a System: This standard, based on a compilation of best practices already in use, defines what the processes are and what their results should be, but it does not define how the processes are accomplished or what tools should be used.[65] The approach for transit security systems integration in this document is based on EIA-632.
- ISO/IEC 15026, System and Software Integrity Levels Managing Risk: This standard focuses on system risk assessment and mitigation. It assigns an integrity level (performance reliability) to each functional component of the system, and uses these integrity levels to evaluate the overall system.[66]

9.4.3.3 Standards Development Organizations (SDOs)

SDOs that are active in areas relating to transit security systems integration are a helpful resource for selecting and establishing standards.

Relevant SDOs include:

- American National Standards Institute (ANSI)
- American Public Transportation Association (APTA)
- American Society for Testing and Materials (ASTM) formerly, now ASTM International
- Electronic Industries Alliance (EIA)
- International Electrotechnical Commission (IEC)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- International Organization for Standardization (ISO)
- Institute of Transportation Engineers (ITE)

[65] For additional information, see ANSI/EIA-632-1998.

[66] For additional information, see ISO/IEC 15026, *International Standard – System and Software Integrity Levels,* as quoted by "FAA Safety and Security Practices – Call for review". http://www.faa.gov/ipg/pif/evol/IntegrityAssuranceReviewPackage-18Nov.pdf

- National Electrical Manufacturers Association (NEMA)
- National Transportation Communications for ITS Protocol (NTCIP)
- Society of Automotive Engineers (SAE)

9.4.4 System Architecture

System architecture is an intermediate step in the system development life cycle between requirements specifications and the detailed design of system components. Using an object-oriented perspective,[15] the system architecture identifies the basic uses of the system, allocates those uses among active objects, and allocates the objects among the hardware, communications, and software components of the system. The architecture identifies system components to be developed in the immediate project, as well as those that will be part of future system development phases.

9.4.4.1 Model of a System Architecture

The system architecture provides a blueprint of the system's components and how they fit together. It is essential to achieving a high degree of systems integration for any system development effort.

The system architecture identifies:

- Security devices, such as CCTV
- Production and (if different) development hardware/operating systems
- Major software objects or components—both process and data—and their interactions
- How the technical architecture will link the components into a whole
- Standards to be used in the implementation

Figure 9-3 is a high-level model of a system architecture, illustrating the types of entities that an actual system architecture would describe in detail. The National ITS Architecture is presented as the overarching framework under which a transit security system is likely to be designed.

[15] Object-oriented systems analysis refers to associating functions and data in objects, which can be related to each other, for example, in classes where objects that belong to a class can inherit characteristics from the object that defines the class.

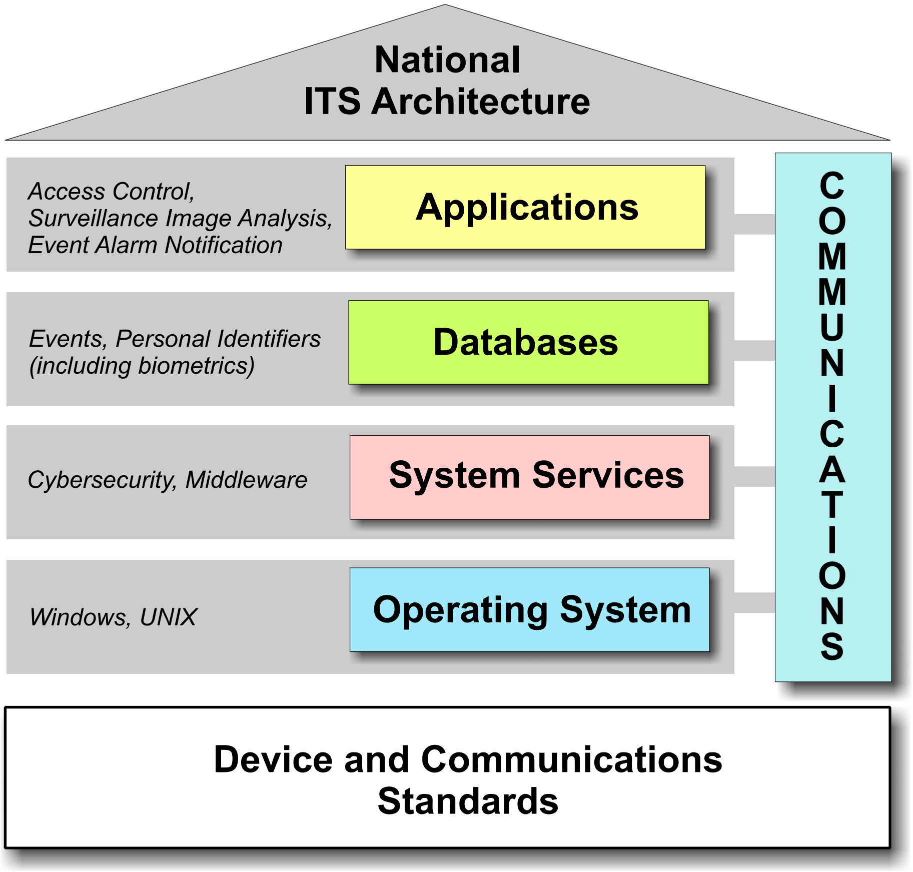


Figure 9-3. Example of a High-Level Security System Architecture

9.4.4.2 The National ITS Architecture

The National ITS Architecture defines the physical entities or subsystems, the data flows among them, and the functions that govern those flows. The overarching national architecture provides the framework for a regional architecture, which in turn provides the framework for the architecture of implemented local systems. One of the 31 user services defined by the National ITS Architecture is Public Travel Security, which defines the information flows "to create an environment of safety in public transportation."[68]

Agencies can decide which standards to use when they determine the system architecture. The use of ITS standards may be required by the FTA, depending on the development status of the particular standard, and the use of some ITS standards will have already been incorporated into the regional ITS architecture. Note that the FTA requires its grantees to use the National ITS

[68] *National ITS Architecture 5.0*. See http://itsarch.iteris.com/itsarch/html/user/usr24.htm.

Architecture and the relevant regional architectures for projects such as security systems.[69] There are opportunities to leverage security applications with ITS applications, and take advantage of ITS standards, especially in communications. For information on ITS standards refer to **http://www.its.dot.gov/arch/arch.htm** and **www.standards.its.dot.gov**.

9.5 Security Integration Issues for Decision Makers

Many transit information technology and security professionals recognize the benefits of security systems integration. However, given the transit system planning and procurement environment of slow technological change, long capital depreciation horizons, and well-understood requirements, security systems, which include devices based on rapidly changing information and communications technologies, pose a challenge.

To the extent that transit systems focus on security concerns, they mostly plan for a response during and after the event. Recognizing the need to provide help regarding security threats and vulnerabilities, the FTA is providing multi-disciplinary technical assistance teams to the 50 largest transit agencies.[70] The result is that the transit industry is now identifying critical assets and methods to harden their systems.

Measures related to pre-event prevention, detection, and deterrence tend to be considered when new facilities are being planned, designed, and constructed. Transit professionals recommended the following overall strategies for developing integrated transit security systems:

- Implement and evaluate pilot projects as part of a comprehensive plan that enables the transit agency to avoid a proliferation of pilots and a low level of integration
- Use proven, widely deployed, commercial-off-the-shelf solutions
- Test and retest systems for robustness in 24/7 operations for the desired level of integration
- Secure the communications system with layers of security that employ both authentication and encryption

Transit agencies should consider addressing issues relating to the degree of transit security system integration. These issues are based on systems engineering literature and the experiences of transit agencies and are classified into technical integration issues and institutional integration issues.

[69] FTA Master Agreement, **http://www.fta.dot.gov/library/legal/agreements/2004/ma.html**.
[70] For further information, see **http://transit-safety.volpe.dot.gov/Security/Default.asp**.

9.5.1 Technical Integration Issues

Budget constraints are a reality and require tough decisions with resource allocation. The following technical issues are considered the most important for agencies to address to enhance system integration when developing a transit security system.

- Design considerations
- System architecture and standards
- Device compatibility
- Data communication and fusion
- Integrated legacy systems
- Security system security
- Testing and simulation
- Technology trends

These issues assume that the agency is following the systems engineering process outlined in Section 9.4.2, in particular the production of a concept of operations document.

9.5.1.1 Design Considerations

Agencies should consider investing adequate resources in the planning, requirements definition, and design stages of a systems integration project. One author, referring to information systems development, reports that "[I]nsufficient investment in the early design phases (5 to15 percent) is likely to lead to project cost overruns [*sic*] of between 50 and 100 percent for both hardware and software projects."[71]

The budget constraints faced by transit agencies may lead to reducing funds, time, and personnel dedicated to the initial project stages. However, especially for projects introducing new technologies and for projects integrating new and legacy technologies, it is critical for system planners and developers to reserve adequate resources for initial project stages.

One respondent, a security consultant, observed that transit agency personnel face time pressures that hinder their ability to learn enough about the capabilities of new technologies to frame clear requirements. Transit agency personnel should consider creating the policies and procedures for using the information that is being generated by the integrated security system.

In addition, there are institutional pressures for early, concrete project results. These may lead to premature system development and failures, like the inadequate installation of security system devices at one transit system.

[71] Cook, op. cit.

Recommendations for enhancing security systems integration include:

- Use tests, simulations, and table top exercises to determine the requirements for the system during the initial stages of the development life cycle (not just at the end)
- Increase spending on the initial stages of the life cycle when the project contains new technology and new capabilities outside the experience of the transit agency
- For the largest systems, consider creating a special-purpose security operations unit within the OCC, with the requirement that the unit be physically and technologically able to communicate freely with other OCC staff
- Create the design in layers, including layers of deterrence, detection, and response, and layers to protect the security system itself
- Generate well-formed system requirements, including data sources, data stores, information users, and operational procedures
- Visit transit agencies of similar scale and network characteristics that have installed security systems, when possible, and evaluate the extent of integration in evidence for those systems.

9.5.1.2 System Architecture and Standards

Most respondents favored the use of an architecture based on standards, rather than one based on a proprietary system. At the same time, most respondents acknowledged that existing transit security systems were constructed around proprietary systems, either because the legacy systems predated relevant standards or because the proprietary system was seen as the least costly option.

New systems development presents more of an opportunity to implement standards. The practitioners cited ITS standards as well as the communications and information technology standards used across economic sectors that have been developed by standards development organizations, such as the Institute of Electrical and Electronics Engineers (IEEE). One practitioner found ITS standards useful in the new system context, because they improved the ability to link the system with ITS functions.

In each of the system component types indicated in **Figure 9-1**, the agency system developer should consider whether or not to use newer technologies. Different transit systems are likely to reach different conclusions on the use of cutting-edge technology and devices. The choice will depend on the organization's tolerance for risk, comfort with innovation, and willingness to predict the likely direction of technology in the future. Trailing-edge technologies may be proven, and reliable, but may face obsolescence and be unable to interface with newer technologies in a relatively short time frame.

9.5.1.3 Device Compatibility

A fundamental decision for systems integration is determining which components (human or electronic) need to communicate with each other. This decision needs to be made for both devices with the same function as well as devices with differing functions.

Agencies must carefully specify the parameters that determine the interchangeability and interoperability of security devices to ensure that functional compatibility will exist. Practitioners recommend using a disinterested expert to develop specifications for the devices, such as university researchers, although this group is likely to be biased in favor of new technologies.

9.5.1.4 Data Communications and Fusion

Data integration is essential to the achievement of an integrated system. When integrating diverse system architectures, especially when creating interfaces to external agency systems, data fusion (or combining data stored or generated by diverse systems) can be a complex, costly, and risk-filled exercise.

Importance of Defining Data

Subtle differences that exist in data definitions between agencies may make the exchanged data misleading and, perhaps, unusable.

Data communications are usually modeled as a stack of interacting layers from the link's physical characteristics (e.g., the type of wire) at the lowest level, to the data's semantic content at the highest level. The key to data integration is the use of standards and careful accounting for any deviations from the standards chosen.

9.5.1.5 Integrated Legacy Systems

Given the fiscal constraints faced by most transit systems, it is expected that integrating new technologies into legacy systems will be a constant feature of security systems development. One large transit system currently uses surveillance video systems to determine the state of system operations, such as train location and the density of crowds on station platforms. The transit agency is now considering enhancing these systems for use in video surveillance for crime prevention and for countering terrorism.

Integration issues to be evaluated include:

- The remaining useful life of the equipment
- Camera placement
- Enabling video feeds to the security operations center
- Installation of a SCADA system for the video equipment; the downtime of a camera used for operational purposes is not as critical as the downtime for a security system, since the disabling of the system may mark the onset of a security incident.

Comprehensive legacy system documentation will support the integration process, including original vendor manuals, records of the installation process, and records of all changes made to the system.

Agencies should consider linking to the legacy system through an interface, rather than through extensive changes to the architectures of either the legacy or the new system.

9.5.1.6 Security System Security

Transit agencies are already aware of the necessity for securing the security system against inadvertent or willful damage. Transit agency respondents using wireless information technology for operations stressed the importance of paying attention to the details of cybersecurity.

A strong case can be made for over-engineering the security of security systems, particularly for vulnerable, high-visibility targets, and as an insurance against known and unknown future threats. For each system, security officials should conduct security audits and establish policies that address the following:

- Device hardening against tampering and vandalism
- Device positioning (including concealment) to prevent tampering and vandalism
- Cybersecurity, for wireline and wireless networks; including firewalls
- Access control for the OCC, Network Operations Center, and/or Security Operations Center
- Protection of the transmission channel
- Protection of power sources
- Visual inspections of devices, and fixed and rolling assets
- Securing handheld and portable equipment by personnel training and strong password policies
- Encryption and authentication of data communications
- Installation of a SCADA system to monitor security system elements, power, and environmental control devices

9.5.1.7 Testing and Simulation

Testing is a line item that may be negatively impacted by budget constraints, but due to the failsafe nature of security systems, a robust test program is essential. Contracts with system vendors must specify that the contractor adhere to development and quality assurance standards that require life-cycle testing.

Testing begins during the initial stages of the project. Simulations, through table-top exercises that involve all stakeholders, can identify the functions and boundaries of the system and its requirements for interfaces with external systems. Pilot tests, demonstrations, and operational tests are most

Importance of Testing in the System Development Lifecycle

Transit security professionals stressed the necessity for testing throughout the development life cycle when asked how it was possible to determine the degree to which a security system was integrated.

important for technologies that are new to the transit agency installing the security system, but are useful at any time new equipment is being acquired. In the most vulnerable segments of the largest transit systems, computer models of the transit properties being protected will be useful in designing the security system.

9.5.1.8 Technology Trends

Technological change is constant and fast. Moore's Law[72] states that the capacity of integrated circuit chips will double every 18 to 24 months. This exponential growth has been roughly maintained since 1965. Security system planners need to be aware of both near- and long-term changes on or just over the horizon.

Security systems are beginning to use the following technologies:[73]

- Ubiquitous Computing. Intelligence is being incorporated into all kinds of everyday objects and appliances. With cheap, powerful, and embedded processors, security systems functionality is likely to be "built in" to fixed and rolling assets acquired by transit systems.
- Networked Sensors. Sensors will allow detection not only of chemical, biological, and radiological agents, but also (privacy concerns notwithstanding) of individuals as they traverse a space.
- Wireless Connectivity. Wireless communications can be combined with ever-present computing and networked sensors to build an intelligent sensor net that continuously monitors a vehicle or a spatial area.
- Autonomous Applications. Video applications are being developed that no longer require security personnel to monitor video images in real time; these applications include facial recognition and detection of unusual events (such as placement of a suspicious parcel on a station platform).
- Global Positioning. GPS will be applied to all vehicles and many individuals; combining GPS with wireless technology and network connectivity will extend GPS capability to enclosed spaces.

9.5.2 Institutional Integration Issues

Transit agency respondents commented on the extent to which the individual units of their organizations operate independently. They acknowledge that a high degree of systems integration cannot be achieved without paying attention to issues of institutional integration, and recounted instances in which critical departments were either not included in the planning for security systems,

[72] Attributed to Gordon Moore, co-founder of Intel.

[73] James A. Lewis, "Security and Surveillance," Center for Strategic and International Studies, June 2002. http://inet2002.org/CD-ROM/lu65rw2n/papers/g10-b.pdf.

or did not wish to be included. The effectiveness of the technology depends on the effectiveness of the institutional and procedural policies that govern how the technology is used.

Issues include:

- Stakeholder involvement
- Interfaces with internal/external organizations
- Inter-organizational data sharing
- Construction and installation
- Systems operation and maintenance

9.5.2.1 Stakeholder Involvement

As described in Section **9.4.1**, gathering all of the stakeholders together at the outset of system planning and throughout the development process is a critical step. Budget considerations and personnel time constraints may discourage full stakeholder participation. One strategy used in a transit agency was to use a third party to help bring all relevant stakeholders together. Ideally, that organization or person should have links to all of the potential participants.

9.5.2.2 Interfaces with Internal and External Organizations

Routine inter-organizational contact can foster special-purpose communication. One agency respondent stressed that transportation department personnel participate in regular meetings with emergency services agencies to share criminal and incident data. As mentioned in Section **9.2**, existing regular interaction among transportation and public safety agencies in the tri-state area led to a remarkably effective response by transportation personnel on September 11, 2001, even though the situation was chaotic and expected communications channels were not necessarily operational.

9.5.2.3 Inter-organizational Data Sharing

The amount of useful data shared among organizations is a useful measure of the degree of systems integration. Data sharing is what holds the integrated system together. However, the characteristics of the data to be shared may not be the same in every organization. In a transit example mentioned previously, video surveillance cameras provide data to the agency's safety, operations, and police units. Different agency departments have varying requirements for the timeliness of the video data. For example, the safety department may not require a continuous stream of video images, whereas security functions do.

The installation of a security system with the capability for data sharing among departments may encourage future data sharing. In one example, a transit communications manager responsible for the OCC predicted that the security department's new intrusion-detection system would be monitored centrally, rather than at a special purpose facility.

9.5.2.4 Construction and Installation

Coordination with the agency's construction department and maintenance of quality control throughout the installation process are critical to the success of the transit security project. The construction department is most concerned with completing its job as quickly as possible. This means department managers may not want to take the time to attend stakeholder meetings. One transit system was reported to have had a well-specified security system, but defects in the quality of the installation resulted in the communications channel being too noisy to be useful. Quality control throughout the process, as well as tight technical specifications, should help prevent a negative result.

To prevent tampering, project managers should also consider preparing security plans during construction and installation of the security system. Securing construction sites in general against crime, vandalism, and terrorist acts can help raise the security image of the transit network as a whole.

9.5.2.5 Systems Operations and Maintenance

A security system is only as good as the supporting training, personnel, policies and procedures. For example, in an access control system security goals may not be met if the database of currently employed personnel and their access privileges are not kept up-to-date with actual personnel events, such as terminations or promotions. Video images can go unmonitored and alarms unanswered. Data may be undigested, if the data have not been transformed into information that can be used for decision-support.

Although respondents stressed that transit operations personnel are not law enforcers, the National Research Council makes the point that the presence of transit operations personnel in transit systems make them deterrents and the true first responders with respect to terrorist attacks.[74] An integrated approach requires these personnel to receive extensive training on responding to alarms generated by automated systems or on making alarms through security systems.[75]

Transit facilities maintenance and systems maintenance operations should consider incorporating correct procedures for new equipment in their existing work packages. Maintenance personnel can be trained to inspect new equipment and to ensure that standard maintenance procedures pose no danger of damaging the equipment.

[74] National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* (Washington, D. C.: The National Academies Press, 2002).

[75] The American Public Transit Association (APTA) surveyed transit systems to determine their security needs. Among the most important operating needs reported by transit agencies were: training for security personnel including preparatory drills, security training for other personnel, joint transit/law enforcement training including preparatory drills. APTA, "Survey of United States Transit System Security Needs and Funding Priorities, Summary of Findings" April 2004.

9.6 Systems Integration and Project Management

The system engineering activity flow in Section **9.4.2** describes the milestones reached and the results produced as a project proceeds through beginning, middle, and end. Agencies know that no project exists in a vacuum. Processes occur before the "beginning" to define and fund a project, and processes occur after the "end" to deploy, operate, and maintain the final product.

This section looks at agency decisions relating to the overall project management capabilities of a transit agency, especially "high tech" security system projects. The section gives an institutional and methodological context to Section **9.5**, which presented technical and institutional factors a decision-maker should consider in relation to a particular project. Included in this section are strategies for maximizing a transit agency's ability to deploy integrated systems by creating a robust set of system development management processes. These include all processes needed for the system engineering activity flow (or system development life cycle) discussed in Section **9.4.2.2** to produce intermediate and final products.

System Development Management Processes

System development management processes include activities that are needed not only to develop a particular system, but also include activities to create consistent processes and procedures that can be re-used for any project. Every transit agency has a unique combination of needs and resources; some considerations listed here may be more applicable to some agencies than to others; each transit agency should determine which actions best meet its goals. To reach a high level of systems integration an agency should evaluate its size, staffing profiles, and management style, among other factors, to optimize the processes to its particular situation.

These are the actual processes that must be in place and executed in order to achieve the milestones, deliverables and results needed at each step of the system engineering activity flow for a particular development project. The system development management process groups include policy formation, capital budgeting and planning, process management, technical management, and acquisition and supply. **Table 9-2** aligns these groups with the system engineering and system development life-cycle steps given elsewhere in this chapter.

> The considerations present general approaches to managing system development, but each agency must identify its particular security needs to determine which approaches are appropriate.

System development management processes also include non-technical process groups, such as policy formation and capital budgeting. Integration issues are critical at these non-technical stages, because projects and their attendant constraints are typically defined as a result of these processes.

The considerations listed in the balance of this chapter summarize points made throughout this document and arrange the considerations by system development life cycle process group. Each agency must identify its particular security needs and determine which of these considerations are appropriate. They should, when consulting these considerations, consider the differences in threat levels and particular circumstances will differ among various geographic areas or facilities.

Table 9-2. System Development Management Process Groups and the System Development Life Cycle

Process Groups	EIA 632	"Vee" Model	System Engineering Activity Flow	PMBOK[76]: Processes				
				Initiate	Plan	Control	Execute	Close
Policy Formation								
Capital Budgeting and Planning								
Process Management	Technical Management Planning Assessment Control			■	■	■	■	■
Technical Management	Technical Evaluation Systems Analysis Requirements Validation Systems Verification	Validation	Verification Validation		■	■	■	
Acquisition and Supply	Acquisition and Supply Supply Acquisition	Procure Parts					■	
System Design	System Design Requirements Definition Solution Definition	User Requirements & Concept of Operations System Requirements & Architecture Component Design	Need Operational Concept Functional Requirements System Architecture Allocated Requirements Detailed Design			■	■	
System Implementation	Product Realization Implementation Transition to Use	[Procure,] Fabricate, & Assemble Parts Component Integration & Test	Implementation Test [& Verification] [Validation]			■	■	■

[76] A Guide to the Project Management Body of Knowledge (ANSI:/PMI 99-001-2000), Project Management Institute, p.38

Process Groups	**EIA 632**	**"Vee" Model**	**System Engineering Activity Flow**	**PMBOK[76]: Processes**				
				Initiate	Plan	Control	Execute	Close
		System-level Integration & Test System Demonstration & [Validation]						

Note:
Light-shaded processes are project precursors. These processes set up the policy and fiscal framework needed to begin a project.
Dark-shaded processes are supporting or methodological processes that are used to produce results at all stages of the system development life cycle.
Brackets indicate the [sub]process is included in another, more appropriate process group.

The system development management process groups described include:

- Policy formation
- Capital planning and budgeting
- Process management
- Technical management
- Acquisition and supply
- System design
- System implementation

9.6.1 Policy Formation

A policy represents a set of generalized principles that an organization uses to make decisions in specific instances to which the policy applies. With respect to the system development management processes discussed in this section, policy formation refers to the processes that an organization uses to decide which policies need to be created and which principles should be included within the needed policies.

The following considerations suggest ways in which a transit agency's policy formation agenda can be shaped by security systems integration concerns:

- Assigning responsibility for counter-terrorist security systems.
- Including security on every agency agenda.
- Creating in-house knowledge of technology.

Assign Clear Responsibility for Counter-Terrorist Security Systems

A transit agency should designate an organizational unit and a person within that unit to be in charge of security systems to counter terrorist activity and establish lines of authority and communication.

Even though transit operators have established or begun to establish organizational structures relating to emergency management and incident response, the responsible organizations for responding to a terrorist incident may not be the same as those charged with building security systems.

Including Security on Every Agency Agenda

An assessment of relevant security concerns should be a major component of all policy setting activities in the agency, even if the transit agency has determined that the risk to its riders, staff, and facilities from terrorist activity is low. With security always on the agenda, once a particular security systems project is underway, internal stakeholders will have a pre-existing foundation for substantive interaction around security-related issues and for ultimately reaching an integrated result.

Create In-House, Non-Specialized Knowledge of Technology and its Capabilities

The diverse functional capabilities of technology and the speed of technological change can leave non-specialists unaware of the wide range of available options. Creating non-specialized technical knowledge in-house will help system planners make the budget case for technology-based security, ITS, operations, and crime-prevention projects; acquire third-party consultants for generating usable system requirements; and prepare procurement specifications.

Even though agencies often disagree on the level of in-house technical expertise required, most practitioners recognize the need to have a clear understanding of the language and broad issues related to a particular technology.

9.6.2 Capital Planning and Budgeting

Transit agencies understand their capital planning and budgeting processes in relation to vehicles, facilities, and infrastructure. However, applying these processes to the acquisition of the equipment and services to produce an integrated high technology solution for transit security can present an added measure of complexity and uncertainty to the financial process group.

The budgeting process is an implicit project prioritization process that identifies which efforts must be started first. The following considerations suggest ways in which a transit agency's capital planning and budgeting can be shaped by security systems integration concerns. They include:

- Allocating resources for activities promoting integration
- Applying long-range planning processes
- Prioritizing security systems projects

Allocate Sufficient Resources for Activities Promoting Integration

A common complaint in systems development, especially in the public sector, is that budgets are not large enough to perform the job correctly. Project managers should prepare arguments for systems integration and for the activities needed to promote integration, such as stakeholder input to requirements determination and design, early testing, pilot programs, and demonstrations.

Apply Existing Long Range Planning Processes to Security Systems.

Transit agencies are experienced in long-term capital planning and budgeting and can apply these skills to security systems planning. However, security systems technology is constantly changing with more capability and functionality becoming available over time. Practitioners report that these technologies can be expected to become obsolete in a five-to ten-year period. Agencies should take upgrade paths into account in their long-range planning cycles.

Prioritize and Focus Security Systems Projects.

The capital planning and budgeting process determines the size and nature of new investments in transportation assets. By definition this process sets priorities among competing program demands for funds. Prioritizing and focusing transportation security projects will require system planners to identify clear benefits and justifications when deploying a particular system.

9.6.3 Process Management

System development managers create a framework within which every individual project is developed. The process management process group focuses on creating tools and executing the processes to plan, assess, and control development projects.

Strategies include:

- hiring consultants to coordinate stakeholders
- using system engineering methods
- training staff continuously

Hire a Third-Party Consultant to Coordinate Agency Stakeholders

Organizational units within an agency may need an outside party to bring them all together to define the process, identify integration opportunities and technologies, and minimize stovepiped behaviors.

Use Systems Engineering Methods (EIA 632)

Applying these method, which incorporate risk assessment and risk modeling, will facilitate increased systems integration and provide a holistic point of view that promotes systems integration.

Train Staff Continuously

Ultimately, agency staff must respond to information gathered and distributed by the integrated security system. For the response to be effective and appropriate, continuous training is necessary for all affected personnel.

9.6.4 Technical Management

Technical management is a process group that creates and deploys the methodologies and underlying techniques for system analysis and validation. A foundation of sound methodologies will improve the transit agency’s ability to implement an integrated transit security system.

Strategies include:

- Implementing a test program
- Using a phased implementation approach
- Using standards

Implement a Strong Test Program

Testing is considered a means of determining whether a system has achieved a sufficient level of integration. Testing should take place at all stages of the development life cycle and include:

- Modeling and simulation—including rehearsals, table top exercises, and systems analysis at all life cycle stages
- Validation and verification
- Operational testing

Use a Phased Implementation Approach

Transit agencies already have experience in implementing pilot projects that test a new device or method in a portion of the transit system, e.g., a new fare collection system, before full implementation. Transit agencies should consider leveraging this experience for the implementation of new security system technologies. It is equally important for transit systems to consider pilot projects as defined within a comprehensive multi-year plan to help avoid the proliferation of stand-alone pilots and ensure that the pilot can be integrated into a full system in the future.

Use Standards

Transit security system planners should evaluate standards relating to process, information technology, and communications for use in the security program. Using standards will increase the likelihood of higher levels of integration, not only for the current project but in future phases.

9.6.5 Acquisition and Supply

Any product, whether final or intermediate, has an acquirer; an organization that orders and receives the product, and a supplier, which creates or transfers the product to the acquirer. The product's supplier may be internal or external to the transit agency.

Even for internal transactions, well-defined agreements between acquirers and suppliers are needed. Since a critical relationship is the contracting relationship, agencies should consider the following strategies when forming partnerships with contractors:

- Writing well-specified procurement documents
- Finding the "right" partner
- Using third party experts

Write Well-Specified Procurement Documents

Transit agency personnel experienced in system development, networking, and communications warn that procurement documents are being written by non-specialists, who may not be aware of all the elements necessary to ensure that the acquisition has the desired result. In particular, the "low bid" environment can have adverse affects if the procurement does not specify the desired quality and functions of the service or device.

Attention to detail in the procurement process is critical, from the acquisition of initial consultant services through the procurement of security system devices. Peer transit agencies can provide advice based on their experiences with hiring consultants, with system development and integration services, and with selecting system hardware and software.

Search for the "Right" Partners

Agencies dependent on contractors may try to maintain relationships with trusted partners. However, one researcher reporting on large, complex technical projects recommends that agencies "[s]elect partners or subcontractors with a sound enterprise environment honed on projects of a similar scale and complexity. This may sound obvious but failure to heed this advice has been the cause of many project failures."[77]

Importance of expertise in procurements

Procurement documents are being written by non-specialists, who may not be aware of all the elements necessary to ensure that the acquisition has the desired result.

Use Third-Party Experts

Agencies should evaluate using third-party disinterested experts, such as university research centers, rather than vendor experts, to evaluate the potential devices, architectures, and technical approaches that are available, since technology vendors are not likely to provide truly unbiased evaluations of other approaches.

9.6.6 System Design

The system design process group includes all processes at the beginning of the system development life cycle, from the concept of operations and requirements through detailed component design. Creating the system architecture is a key step in this process group, as it shows the connections among the various sub-systems that form the overall system.

[77] Stephen C. Cook, "What the Lessons Learned from Large, Complex, Technical Projects Tell Us about the Art of Systems Engineering" in Proceedings and Oral Presentation of the INCOSE 2000 Conference, Systems Engineering: A Decade of Progress and A New Century of Opportunity, Minneapolis, Minnesota, USA, 16-20 July 2000, pp. 723-730; **http://www.unisa.edu.au/seec/pubs/00papers/cook-lessons.pdf**.

Processes include:

- Generating system requirements
- Using COTS
- Installing the appropriate kernel
- Layering security
- Securing digital networks
- Maximizing system robustness

Generate Well-Formed System Requirements

To develop an integrated system, developers need to know who requires what information, when, and for what purpose. Generating well-formed system requirements is critical for developing the core and ancillary functions for a particular security system. An excellent tactic for developing requirements is to examine how solutions were developed at other transit agencies, and the range of pre- and post-system development requirements. The transit agency cannot leave this exercise to its consultants, system developers, or integrators, because as the ultimate customer the agency must define the scope of the desired system at the outset to ensure that its needs are met.

> To develop an integrated system, developers need to know who requires what information, when, and for what purpose.

Use Proven Commercial Off-The-Shelf (COTS) Solutions

Technology specialists contributing to this document advise agencies to avoid proprietary solutions and to use solutions based on open architectures. COTS equipment can result in cost savings since equipment that is widely used in other industries has a proven track record. However, the system planner must verify that the COTS solution is based on open architectures (or at least architectures widely supported by many vendors) and provides an upgrade path as the technology incorporates new features over time. Transit security system planners recommend expediting the procurement process to prevent the acquisition of obsolete systems and requiring the vendor to provide product support for a specified minimum period of time.

Install the Appropriate Kernel

The kernel, or core function, is the minimum set of security applications that can make up the initial phase of an integrated transit security system installation. Installing the appropriate kernel of an integrated security system in part of the agency's facilities will depend on the service characteristics of the transit system.

Consider the following two examples of the minimum technical applications needed for new tunnel construction and for bus transit.

- **Example.** Core functions that are being implemented in new tunnel construction for one transit agency include:
  - Access control to rooms inside tunnels with data on usage and alarms transmitted to and recorded at the OCC.
  - CCTV with video image feeds to OCC and transit police department that provide visual verification of alarms generated by the access control system.
  - Intrusion detection to protect tunnels and other sensitive assets, with data transmitted to and recorded at the OCC.
- **Example.** For bus systems, AVL is the core application needed for integration with security, safety, and communications devices.

Layer Security to Protect Assets

Agencies should follow a layered approach to protect assets, including the security system itself. If a video surveillance system is installed with images monitored locally in a station and there is no transmission outside the local facility, there are no additional layers of protection available if station personnel are unable to view the monitors.

Secure Digital Networks

Security experts advise that both authentication and encryption techniques are needed to secure digital communications.[78] Strong, proven techniques exist to safeguard communications and should be built into security system design.

Maximize System Robustness

System robustness, or the ability of the system to remain operational under internal or external stress, is necessary for the system to survive not only day-to-day wear and tear and the inevitable system glitches, but also attacks or disasters. System robustness can be increased by including redundant and backup systems in the design and using hardened equipment.

9.6.7 System Implementation

System implementation refers to all of the steps needed to build the system using the architecture and detailed designs produced by processes in the system design process group. Operations and maintenance are also part of this process group.

[78] Authentication refers to information attached to a message that validates the identity of the sender. Encryption refers to methods of encoding a message so that it is meaningless, unless the recipient has a key needed to decode the message.

The outcomes of processes in this group that are especially critical for building integrated systems include:

- Planning for obsolescence
- Early involvement of construction and maintenance
- Technology testing

Plan for A Five-To Ten-Year Product Obsolescence Cycle

The ability to upgrade information technology and communications systems needs to be built into the planning and implementation of security systems projects. Transit security and information technology specialists report that products often become obsolete and require replacement within a five-to ten-year time frame.

Involve Construction and Maintenance Early in the Process

The construction and maintenance departments should be involved early in the system development process to ensure that all constraints on installation and subsequent maintenance are accounted for prior to installation.

Thoroughly Test Technologies

Transit agency officials place a premium on speedy construction and installation. A thorough testing program may appear to slow down the process and add to costs. However, because the technologies being implemented are new, it is especially critical for the product to be thoroughly tested through installation and into operations to avoid the major costs associated with reworking an inadequate product.

System security in relation to terrorism

The security of transit systems in relation to the emergent threat of terrorist activity is critical for two reasons:

- Transit is a likely target of terrorist activity, both as a primary or incidental target, and as a means of delivering a device to a separate target.
- After an attack, transit operations must continue to support emergency services logistics, to provide evacuation resources from areas affected by terrorist activity, and to maintain service in unaffected parts of the system.

9.7 Effective Transit Security: The Importance of Security Systems Integration

9.7.1 Transit Security

The events of September 11, 2001, brought security to the forefront of transit agency planning concerns, especially in larger cities. Although transit agencies had previously recognized the need to secure their facilities, the lack of any history of such attacks within the U.S., the low probability of an attack against any one transit property, and perennial budget pressures resulted in security countermeasures being given a relatively low priority. While these factors may still be relevant, transit managers must now explicitly address responses to terrorist attacks in their transit system security plans and projects. The focus on security as it pertains to terrorist attacks is closely related to, but does not entirely overlap with, the focus transit systems have maintained on security as it pertains to crime prevention, and safety.

One particular area of concern is that transit agencies need to develop better methods of communicating during emergencies both internally and with emergency responders.

> "To effectively do their job, public safety responders depend on sophisticated communication systems to relay mission-critical information in real time. They also require wireless systems that provide immediate channel availability. Today's wireless communications systems must support a growing set of missions, such as responses to weapons of mass destruction and domestic terrorism, requiring coordinated participation from agencies at all levels of government. Unfortunately, in many jurisdictions, public safety agencies operate and maintain largely independent radio systems. This type of deployment is often referred to as the "stovepipe model", where systems are installed to serve the mission of a single agency, and where the individual systems lack the capacity to support interoperability with surrounding support agencies. This type of system deployment can cause potentially dangerous situations that risks lives."[79]
>
> "The ability of the public safety community to provide a rapid coordinated response to criminal activities, fires, medical emergencies…natural disasters…terrorism…and mass-casualty tragedies…accentuate the importance of a coordinated response among public safety agencies from all levels of government."
>
> "Foremost among the obstacles that can hinder an effective multi-jurisdictional response is the lack of interoperability among public safety agencies. Wireless interoperability is simply the ability of public safety officials to communicate across different wireless systems when necessary. Radio communications are often public safety personnel's only lifeline when operating in a crisis environment. Without communications interoperability, both life and property are put at significant risk."[80]

The Capital Wireless Integrated Network (CapWIN) in the Washington, D.C. metropolitan area and the New York State Integrated Incident Management System (IIMS) are real-time systems to enhance data communications among transportation and public safety agencies systems, especially for the purposes of incident management. While these systems do not focus on transit, the methods

[79] The Role of States in Public Safety Wireless Interoperability, Public Safety Wireless Network Program.
[80] Ibid.

and results of these integration efforts are very similar to what would be needed in a transit context.[81]

9.7.2 Systems Integration and Security

In the past two decades, there has been both an evolution and a revolution in the application of technology to everyday life. The evolution is evident in the growing deployment of increasingly sophisticated electronic devices like CCTV, while the technological revolution is seen in the application of high levels of digital computing power, storage capacity, and communications bandwidth to all economic activity, including the transit industry.

As technology assumes a bigger role in various aspects of transit operations, the ability of systems to share information brings increasing benefits to operations as well as to transit security. As noted in Chapter 2, organizations of all kinds tend to build "stovepipe systems." However, a higher level of security is possible when agencies, personnel, and technical components work together.

Systems integration brings a synergistic and inclusive view to systems planning and implementation. The holistic perspective takes into account all of the physical, technical, operational, institutional, and procedural factors that comprise a security system.[82] Transit system managers can use these factors to:

- Integrate security devices into a coherent whole
- Integrate security devices into the transit system
- Integrate security and non-security functions
- Interface with non-transit agencies, such as emergency services and traffic management

Integration contributes to transit security by allowing security systems to generate data that can be used for real-time, system-wide decision support.

The three main benefits of systems integration to a transit security system include:

- **Improving communications**. An integrated system can communicate timely information to organizational units. The information used by or generated by integrated devices can be communicated to other devices and to decision-makers. With an integrated system, a person or technology is always collecting and transmitting information to other organizational units.
- **Leveraging resources.** One technological device or system can have multiple purposes. Integrated systems leverage the data being monitored, collected, and transmitted among multiple functions, and multiple organizations. These organizations

[81] For more information on CapWin, see http://www.capwin.org.
For more information on IIMS, see http://www.itspublicsafety.net/law_itsmanagement.htm.
[82] FHWA, Chapter 16, "Regional Integration," *Freeway Management and Operations Handbook*, (Publication Number FHWA-OP-04-003) http://ops.fhwa.dot.gov/Travel/traffic/freeway_management.htm.

can share the cost of system implementation and operation. For example, technology to deter, prevent, detect, and respond to terrorist attacks is related to technology applications for crime prevention and safety.

- **Promoting standards usage:** As discussed in Section 9.4.3, the need for systems integration promotes the use of standards, which produces other secondary benefits for the transit operator. Information technology and telecommunications standards are expected to lead to the interoperability and interchangeability of technical devices, facilitated upgrades to new technology, accurate data transfers, and lower long-term costs.

Appendix A. Chronology of Terrorist Attacks Against Public Transit

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
April 22, 1980	Israel	Grenade	Bus	No		
January 11, 1983	Tel Aviv, Israel	Grenade	Bus	No	12 injured	The PLO claimed that the bus was transporting troops
December 6, 1983	Jerusalem, Israel	Bomb	Bus	No	6 killed - 43 injured	
March 4, 1984	The West Bank	Shooting	Bus	No	6 injured	
March 7, 1984	Ashdod, Israel	Bomb	Bus	No	3 killed - 9 injured	
April 12, 1984	Gaza Strip	Hijacking and hostage-taking	Bus	No	30 kidnapped - 2 attackers killed in police raid	The attackers demanded the release of pro-Palestinian prisoners held in Israel
September 17, 1984	The West Bank	Shooting	Bus	No	5 injured	
December 1, 1984	Jerusalem, Israel	Grenade	Bus	No	3 injured	The PFLP claimed to be targeting Israeli soldiers on the bus
January 31, 1985	Hebron, Israel	Shooting	Bus	No	2 injured	
April 30, 1985	Israel	Incendiary grenades	Bus	No	1 injured (driver)	The injured was the driver
May 30, 1985	Afula, Israel	Bomb	Bus station	No		
June 12, 1985	Jerusalem, Israel	Bomb	Bus station	No		
June 24, 1985	Jerusalem, Israel	Bomb	Bus stop	No	1 injured	
July 8, 1985	Holon, Israel	Bomb	Bus station	No	5 injured	
September 5, 1985	Israel	2 gasoline bombs	Bus	No	(no passengers)	There were no passengers
September 9, 1985	Jerusalem, Israel	Firebomb	Bus	No		
September 19, 1985	Mt. Zion, Israel	Gasoline bomb	Bus stop	No		

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
September 25, 1985	Egged, Israel	Bomb	Bus stop	No	1 injured	
September 26, 1985	Gilo, Jerusalem	Bomb	Bus stop	No	7 injured	
November 8, 1985	Kafr Saba, Israel	Bomb	Bus station	No	Many	
November 13, 1985	Lebanon	Shooting	Bus	No	Several	
December 22, 1985	Erez, Israel	Bomb	Bus	No		
February 14, 1986	Jerusalem, Israel	Bomb	Bus	No	6 injured	
April 8, 1986	Jerusalem, Israel	Firebomb	Bus	No	9 injured	
April 16, 1986	Damascus, Syria	Coordinated bombs	Multiple buses	No		
July 3, 1987	Israel	Bomb	Bus	No	2 injured	
August 10, 1987	Mardan, Pakistan	2 bombs	Bus station	No	7 killed - 45 injured	
September 19, 1987	Rawalpindi, Pakistan	Bomb	Bus station	No	5 killed - 16 injured	
October 12, 1987	Peshawar, Pakistan	Bomb	Bus station	No	13 injured	The bombing happened while Peshawar was hosting the Cricket World Cup
November 18, 1987	Peshawar, Pakistan	Bomb	Bus	No	1 killed - 19 injured	
January 24, 1988	Pakistan	Bomb	Bus	No	10 killed - 19 injured	The bus was owned by the national government
March 7, 1988	Israel	Hijacking and hostage-taking	Bus	No	6 killed	The hostage-takers demanded the release of all Palestinian prisoners from Israeli jails. The hostage-takers were killed by Israeli commandos in a raid to re-take the bus (the commandos also killed two female hostages)
April 16, 1988	Charaadda, Pakistan	Bomb	Bus station	No	4 killed - 11 injured	
February 5, 1989	Quetta, Pakistan	Bomb	Bus station	No	3 killed - 5 injured	

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
April 7, 1989	Canada	Hijacking	Greyhound bus	No		The attacker demanded that the bus be driven to the Canadian parliament in Ottawa
April 30, 1989	Tel Aviv, Israel	Bomb	Bus stop	No		
July 4, 1989	Peshawar, Pakistan	Bomb	Bus	No	10 killed - 29 injured	
September 16, 1989	Evlak, Azerbaijan	Timed bomb	Bus	No	5 killed - 27 injured	
September 18, 1989	Peshawar, Pakistan	Bomb	Bus	No	3 killed - 2 injured	
October 10, 1989	Rawalpindi, Pakistan	Bomb	Bus station	No		
February 4, 1990	Cairo, Egypt	Grenades and shooting	Tourist bus	No	11 killed - 19 injured	The tourist bus was owned by an Israeli company and was transporting Israelis
February 18, 1990	Azerbaijan	Bomb	Bus	No	15 injured	
March 2, 1990	Tel Aviv, Israel	Bomb	Bus station	No		
May 21, 1990	Amman, Jordan	Shooting	Tourist bus	No	10 injured	The tourist bus was carrying French tourists
June 26, 1990	Jerusalem, Israel	Bomb	Bus stop	No	2 injured	
September 17, 1990	Tel Aviv, Israel	Bus	Bus station	No		
February 8, 1991	Israel	Grenade	Bus	No	3 killed - 4 injured	Those killed were the attackers
April 4, 1991	Corsica	Incendiary device	Bus	No		The device exploded under the bus
June 27, 1991	Sri Lanka	Bomb and shooting	Bus	No	14 killed - 9 injured	
July 6, 1991	Rome, Italy	Thrown explosive device	Tourist bus	No		The tourist bus was owned by a Spanish company

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
August 10, 1991	Athens, Greece	Arson	Tourist bus	No		The tourist bus was owned by a Turkish company
November 2, 1991	Assam, India	Bomb	Bus	No	6 killed	
February 7, 1992	London, England	Incendiary device	Subway track	No		
February 11, 1992	Solola, Guatemala	Shooting	Bus	No	5 killed - 15 injured	The attack took place immediately prior to a visit from the U.S. Secretary of Defense
February 21, 1992	Xinjiang, China	Timed bomb	Bus	No	6 killed - 20 injured	
February 28, 1992	Athens, Greece	Remote-controlled bomb	Bus	No	16 injured	The bomb was hidden in a metal container and magentically attached to a traffic pole
March 27, 1992	Lermontov, Russia	Hijacking	Bus	No		The hijackers were armed with machine guns and grenades and demanded freedom for two imprisoned burglars
May 12, 1992	Israel	Bomb	Bus	No		
June 5, 1992	Karachi, Pakistan	Bomb and shooting	Bus	No	2 killed - 24 injured	The bomb was tossed at the bus from a crowd
July 14, 1992	Egypt	Firebomb	Bus	No	1 injured	The tourist bus was transporting French tourists; the person injured was the tour guide
July 15, 1992	Santiago, Chile	Shooting	Bus	No		The bus was attacked while in the bus station
July 24, 1992	Peru	Shooting	Bus	No	2 killed	A German and a Colombian were singled out to be killed

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
July 30, 1992	Delhi, India	Timed bomb	Bus	No	1 killed - 26 injured	The bomb was hidden in a bag of cereal
August 26, 1992	Qena, Egypt	2 incendiary devices	Tourist bus	No	2 injured	The driver and tour guide were the injured
September 29, 1992	Pathankot, India	Bomb	Bus	No	6 killed - 50 injured	
October 16, 1992	Baykan District, Turkey	Ambush and kidnapping	Bus	No	7 passengers	The bus was set on fire and the passengers were kidnapped
October 22, 1992	Dayrut, Egypt	Shooting	Tourist bus	No	1 killed - 2 injured	A young boy stood watch and whistled to alert the attackers of the approach of the bus, which was carrying European tourists
November 12, 1992	Qena, Egypt	Shooting	Tourist bus	No	8 injured	
December 1, 1992	Ludihana, India	Hijacking and shooting	Bus	No	16 killed	
December 9, 1992	London, England	Bomb	Subway station	No		
December 23, 1992	London, England	Bomb	Subway station	No		The bombing was at rush hour
December 23, 1992	Bangkok, Thailand	Bomb	Bus station	No	4 killed - 1 injured	A second bomb on a bus failed to detonate
February 4, 1993	Cairo, Egypt	Malatov cocktail	Tourist bus	No		The bus was in use by a South Korean tour group
June 8, 1993	Egypt	Bomb	Tourist bus	No	2 killed - 21 injured	The bomb was placed inside an overpass and detonated as the bus drove through
August 18, 1993	Turkey	Grenade	Tourist bus	No	8 injured	The grenade was thrown under the bus as it waited outside a hotel

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
October 25, 1993	Lima, Peru	Bomb	Minibus	No	1 killed - 20 injured	The killed was the driver; the minibus was parked in the parking lot of Lima International Airport
December 27, 1993	Cairo, Egypt	Shooting and bomb	Tourist bus	No	15 injured	The bomb exploded near a café
April 6, 1994						
April 13, 1994	Afula, Israel	Car bomb	Bus	No	8 killed	
October 19, 1994	Hadera, Israel	Self-detonated explosives	Bus	Yes	5 killed	
October 23, 1994	Luxor, Egypt	Shooting	Tourist bus	No	1 killed - 3 injured	
December 15, 1994	Tel Aviv, Israel	Self-detonated explosives	Bus	Yes	22 killed	
December 21, 1994	New York City	Homemade bombs	Heavy rail	No		
December 25, 1994	West Jerusalem, Israel	Self-detonated explosives	Bus stop	Yes	12 injured	
January 3, 1995	New York City	Homemade bombs	Heavy rail	No		
January 15, 1995	Cambodia	Rocket attack	Tourist bus	No	1 killed - 2 injured	
March 20, 1995	Turkey	Shooting and grenade	Bus	No	2 killed - 22 injured	
April 9, 1995	Tokyo, Japan	Chemical attack	Subway, subway station	No	8 killed - 4700 injured	
April 9, 1995	Gaza Strip	Explosive-laden van	Bus	Yes	50 injured	
May 15, 1995	Chimbote, Peru	Ambush	Bus	No	Passengers were robbed at gunpoint	
July 14, 1995	Gaza Strip	Explosive-laden van	Bus	No	8 killed	
July 23, 1995	Belfast, Northern Ireland	Hijacking and firebombing	Bus	No	0 killed - 0 injured	
July 24, 1995	Punjab state, India	Bomb	Bus	No	3 killed - 25 injured	

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
July 25, 1995	Paris, France	Bomb	Subway, subway station	No	7 killed - 86 injured	
July 27, 1995	Ramat Gan, Israel	Self-detonated explosives	Bus	Yes	6 killed	
August 17, 1995	Paris, France	Nail-filled bomb	Subway station	No	17 injured	The bomb was placed in a trashcan near the entrance to the station
August 21, 1995	Paris, France	Timed bomb	Commuter rail, station	No	7 killed - 60 injured	
September 29, 1995	Jerusalem, Israel	Self-detonated explosives	Bus	Yes	4 killed	
October 1, 1995	Mexico City, Mexico	Shooting	Subway	No	3 killed - 6 injured	The shooter was an angry policeman
October 1, 1995	Georgia (CIS)	Hijacking	Bus	No	2 killed - 10 injured	
October 17, 1995	Laghouat, Algeria	Shooting	Bus	No	18 killed - 15 injured	
October 30, 1995	Paris, France	Bomb	Subway	No	24 injured	
December 1, 1995	Assam, India	Bomb	Bus, bus station	No	4 killed - 15 injured	
January 16, 1996	Trabzon, Turkey	Hijacking	Ferry	No	0 killed - 0 injured	The hijackers surrendered in Turkey
February 20, 1996	Lahore, Pakistan	Bomb	Bus	No	3 killed - 14 injured	The bomb was hidden in the luggage compartment
February 25, 1996	Jerusalem, Israel	Self-detonated explosives	Bus	Yes	26 killed - 80 injured	
February 26, 1996	London, England	Bomb	Bus	No	8 killed - 100 injured	The bomb may have detonated before it reached its intended target
March 3, 1996	Jerusalem, Israel	Self-detonated explosives	Bus, bus station	Yes	26 killed	
March 7, 1996	Jerusalem, Israel	Self-detonated explosives	Bus	Yes	19 killed	
April 8, 1996	Kashmir, Pakistan	Dynamite	Bus	No	4 killed - 5 injured	
April 27, 1996	Hebron, Israel	2 Firebombs	Bus	No	5 injured	

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
April 27, 1996	Modinager, India	Bomb	Bus	No	15 killed	The bombing took place during an election period
April 29, 1996	Mindinao, Philipines	Bomb	Minibus, bus station	No	2 killed - 11 injured	The two killed were children
May 4, 1996	Pakistan	Bomb	Private bus	No	40 killed	The bomb was hidden in the gastank of the bus
May 7, 1996	Tizi-Ouzou, Algeria	Homemade bomb	Bus stop	No	2 killed - 14 injured	The bus stop was located near an elementary school
May 22, 1996	Muhurraq, Bahrain	Bomb	Bus stop	No	2 injured	
June 3, 1996	Agra, India	Bomb	Bus	No	14 killed	
June 5, 1996	Caracas, Venezuela	Firebomb	6 buses	No	2 killed	The attack may have been associated with an increase in bus fares
June 11, 1996	Caracas, Venezuela	Firebomb	7 buses	No	0 killed - 0 injured	The attack may have been associated with an increase in bus fares
June 16, 1996	Moscow, Russia	TNT	Subway	No	4 killed - 12 injured	The TNT was attached to the underside of a subway seat
June 27, 1996	Punjab state, India	Bomb	Bus	No	2 killed - 15 injured	
July 11, 1996	Faizabad, Pakistan	Bomb	Bus station	No	3 killed - 5 injured	
July 12, 1996	Moscow, Russia	Homemade bomb	Trolley	No	5 injured	The bomb was hidden in a bag of vegetables; the driver was among the injured
August 13, 1996	Moscow, Russia	Bomb	Trolley	No	27 injured	The bomb was hidden in a bag; the attack took place during an election period

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
August 16, 1996	Gulu, Uganda	Landmine and ambush	Bus	No	14 killed	
September 23, 1996	Sivas Province, Turkey	Shooting	Bus	No	2 killed	One of the killed was a policeman
October 5, 1996	Bingol Province, Turkey	Kidnapping	Bus	No	3 kidnapped	The kidnapped were all foreigners
October 7, 1996	Piliscsaba, Hungary	Bomb	Bus	No	4 injured	
October 10, 1996	Ksar el Hirane, Algeria	Ambush	Bus	No	9 killed	
October 31, 1996	Hassi R'mel, Algeria	Ambush and knife attack	Bus	No	34 killed	The bus was stopped at a roadblock; the throats of the victims were slit
December 3, 1996	Paris, France	Bomb	Subway, subway station	No	4 killed - 86 injured	
December 3, 1996	Sydney, Australia	Bomb	Subway station	No		The bomb was placed in a public bathroom of the subway station
January 3, 1997	Benhamdani, Algeria	Ambush and knife attack	Bus	No	20 killed	The throats of the victims were slit
February 3, 1997	Damascus, Syria	Bomb	Bus	No	9 killed - 44 injured	
March 10, 1997	Jammu-Kashmir, India	Shooting	Bus	No	4 killed	
March 26, 1997	Seoul, South Korea	Kidnapping	Bus	No	34 hostages	Ended peacefully
April 6, 1997	Haryana, India	Bomb	Bus	No	1 killed - 18 injured	
May 14, 1997	Beijing, China	Bomb	Bus	No	2 killed - 100 injured	
June 6, 1997	Sauk, Albania	Shooting	Bus	No	2 killed - 6 injured	
June 27, 1997	Punjab state, India	Homemade bomb	Bus	No	2 killed - 14 injured	
July 1, 1997	Sri Lanka	Hijacking and arson	Ferry	No	Unknown	The ferry was Indonesian

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
July 14, 1997	Guangdong province, China	Bomb	Bus	No	5 killed - 6 injured	
August 5, 1997	Punjab state, India	Bomb	Bus	No	7 killed - 12 injured	
August 26, 1997	Algiers, Algeria	Bomb	Minibus	No	3 killed - 20 injured	
August 30, 1997	Delhi, India	Coordinated bombs	2 buses	No	12 killed - 13 injured	
September 18, 1997	Tursunzade, Tajkistan	Bomb	Bus terminal	No	2 injured	
September 18, 1997	Cairo, Egypt	Ambush	Tourist bus	No	10 killed - 8 injured	The bus was parked in front of a museum
September 22, 1997	Jammu-Kashmir, India	Bomb	Bus	No	25 injured	The bomb was hidden under the bus
September 28, 1997	Casamance Region, Senegal	Landmine	Bus	No	5 killed - 10 injured	The mine was detonated under the bus
September 29, 1997	Cairo, Egypt	Grenades and firebombs	Tourist bus	No	9 killed - 19 injured	Those killed were German tourists
October 3, 1997	India	Shooting	Bus	No	15 killed	
October 3, 1997	Tbilisi, Georgia (CIS)	Bomb	Bus	No	1 injured	
October 10, 1997	San Pedro Sula, Honduras	Grenade	Bus	No	7 injured	The bus was located near a police station
October 11, 1997	Southeast Turkey	Kidnapping	Bus	No	8 passengers kidnapped	The bus was stopped at a roadblock
December 30, 1997	Kampala, Uganda	Ambush	Bus	No	8 killed	
December 30, 1997	Southern India	Kidnapping	Bus	No	6 passengers kidnapped	
January 1, 1998	Oran region, Algeria	Ambush	Bus	No	33-50 killed - 20 bystanders injured	The bus was stopped at a roadblock

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
January 12, 1998	Delhi, India	Bomb	Bus	No	4 killed - 24 injured	
January 28, 1998	Moscow, Russia	Bomb	Subway, subway station	No	3 injured	The injured were transit employees
February 5, 1998	Moscow, Russia	Shooting	Tram	No	1 killed - 3 injured	
February 14, 1998	Algiers, Algeria	Bomb	Bus	No	4 killed - 22 injured	
February 23, 1998	Lahore, Pakistan	Bomb	Bus	No	1 killed - 16 injured	
March 5, 1998	London, England	Bomb	Bus stop	No	0 killed - 0 injured	
March 7, 1998	Wuhan, China	Bomb	Bus	No	16 killed - 30 injured	
March 25, 1998	Colombo, Sri Lanka	Bomb	Bus	No	28 killed - 235 injured	The bomb exploded while the bus traveled under a pedestrian bridge
April 7, 1998	Algiers, Algeria	Bomb	Bus station	No	12 injured	
July 26, 1998	Sukkur, Pakistan	Bomb	Bus station	No	1 injured	
July 28, 1998	Sukran, Pakistan	Bomb	Bus	No	5 killed - 20 injured	
August 25, 1998	Antioquia, Colombia	Ambush and shooting	Bus	No	17 killed	
November 2, 1998	Delhi, India	Bomb	Bus station	No	2 killed - 5 injured	
November 16, 1998	Sarajevo, Bosnia	Bomb	Bus	No	0 killed - 0 injured	
November 16, 1998	Uganda	Grenade	Bus	No	30 killed	The bus was on its way to Rwanda
November 19, 1998	Mindinao, Philipines	Coordinated bombs	2 buses	No	1 killed - 40 injured	
November 27, 1998	Delhi, India	Bomb	Bus station	No	25 injured	
December 7, 1998	Casamance Region, Senegal	Ambush	Bus	No	1 killed - 5 injured	
December 13, 1998	Mindinao, Philipines	Coordinated bombs	Bus, bus station	No	1 killed - 30 injured	The killed was the driver
April 11, 1999	Mindinao, Philipines	Bomb	Bus	No	1 killed - 11 injured	
June 23, 1999	Mindinao, Philipines	Shooting	Jitney	No	3 killed - 16 injured	

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
July 6, 1999	Sri Lanka	Coordinated bombs	Bus, bus station			
July 27, 1999	Kandy, Sri Lanka	Bomb	Bus	No	2 killed - 20 injured	The bomb was placed on the bus by a woman as she exited
September 4, 1999	Abkhazia region, Georgia (CIS)	Landmine	Bus	No	3 killed - 13 injured	
September 26, 1999	Kashmir, Pakistan	Bomb	Bus	No	7 killed - 19 injured	
October 20, 1999	Mindinao, Philipines	Grenade	Bus station	No	2 killed - 2 injured	
November 4, 1999	Mindinao, Philipines	Bomb	Bus	No	4 killed - many injured	
November 29, 1999	Badulla, Sri Lanka	Bomb	Bus	No	1 killed - 28 injured	
January 30, 2000	Muridke, Pakistan	Coordinated bombs	Bus stop, rail station	No	1 killed - 3 injured	
February 2, 2000	Hyderabad, Pakistan	Bomb	Bus	No	2 killed - 9 injured	
February 7, 2000	Mindinao, Philipines	Coordinated bombs	2 buses	No	0 killed - 0 injured	
February 8, 2000	Sri Lanka	Bomb	Bus	No	16 injured	
February 14, 2000	Yugoslavia	Antitank rocket	Bus	No	2 killed - 5 injured	
March 15, 2000	Sri Lanka	Coordinated bombs	2 buses	No	37 injured	
March 21, 2000	Sri Lanka	Coordinated bombs	2 buses	No	2 killed - 47 injured	
April 7, 2000	Algieria	Ambush and shooting	2 buses	No	16 killed - 30 injured	The buses were stopped at roadblocks
May 3, 2000	Mindinao, Philipines	Bomb	Bus, bus station	No	5 injured	
June 14, 2000	Lahore, Pakistan	Bomb	Bus station	No	15 injured	
June 21, 2000	Algeria	Ambush	Bus	No	19 killed	
July 7, 2000	Laos	Bomb	Bus	No	2 killed - 10 injured	
July 24, 2000	Sri Lanka	Rammed with an explosive-filled bicycle	Bus	Yes	2 killed - 8 injured	The bomb exploded prior to colliding with the bus

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
July 27, 2000	Rawalpindi, Pakistan	Bomb	Bus station	No	1 killed - 9 injured	
September 4, 2000	Lahore, Pakistan	Remote-controlled bomb	Minibus	No	1 killed - 4 injured	The bomb was placed under the bus and exploded while the bus was moving
October 5, 2000	Jalandar, India	Bomb	Bus	No	7 killed - 16 injured	
November 20, 2000	Duesseldorf, Germany	Fragmentation bomb	Subway station	No	9 injured	
November 22, 2000	Lahore, Pakistan	Bomb	Bus station	No	1 killed - 12 injured	
November 28, 2000	Abdijan, Ivory Coast	Bomb	Bus station	Not intentionally	4 killed - 7 injured	The bomb exploded while in the process of being hidden
December 6, 2000	Kfar Darom, Israel	Car bomb	Bus		11 killed	
December 18, 2000	Hadera, Israel	Car bomb	Bus		2 killed - 60 injured	
December 18, 2000	Sri Lanka	Landmine	Bus	No	7 killed - 20 injured	
December 30, 2000	Sri Lanka	Landmine	Bus	No	3 killed - 20 injured	
December 30, 2000	Nagaland, India	Bomb	Bus	No	4 died - 14 injured	
January 1, 2001	Algeria	Ambush and shooting	2 buses	No	20 killed	
March 27, 2001	Manila, Philipines	Bomb	Light rail, light rail station	No	9 killed - 60 injured	The bomb was timed to go off as the train pulled into the station
April 22, 2001	Quezon, Philipines	Bomb	Bus station	No	1 killed - 15 injured	
April 29, 2001	Netanya, Israel	Car bomb	Bus stop	Yes	60 injured	
May 25, 2001	Jerusalem, Israel	Self-detonated explosives	Bus	Yes	28 injured	
June 11, 2001	Jerusalem, Israel	Bomb	Bus	Yes	15 killed - 70 wounded	
July 16, 2001	Kfar Sava, Israel	Self-detonated explosives	Bus stop	Yes	1 killed - 60 injured	
November 29, 2001	Nablus, Israel	Car bomb	School bus	Yes	0 killed - 0 injured	

Date of Attack	Location of Attack	Type of Attack	Impacted Asset	Suicide Attack (yes/no)	Number of Casualties (if known)	Additional Comments
December 2, 2001	Hadera, Israel	Car bomb	Bus station	Yes	65 injured	
December 9, 2001	Binyamina, Israel	Self-detonated explosives	Bus stop	Yes	2 killed - 11 injured	
March 5, 2002	Hadera, Israel	Self-detonated explosives	Bus	Yes	3 killed - 9 injured	
March 17, 2002	Haifa, Israel	Self-detonated explosives	Bus	Yes	15 killed	
March 20, 2002	Haifa, Israel	Self-detonated explosives	Bus stop	No	30 injured	A second bomb was diffused
April 10, 2002	Afula, Israel	Self-detonated explosives	Bus	Yes	1 killed	
June 5, 2002	Jerusalem, Israel	Self-detonated explosives	Bus	Yes	0 killed	
October 21, 2002	Kfar Musmus, Israel	Self-detonated explosives	Bus	Yes	7 killed	
November 21, 2002	Haifa, Israel	Self-detonated explosives	Bus	Yes	8 killed	
March 5, 2003	Haifa, Israel	Self-detonated explosives	Bus	Yes	15 killed - dozens injured	
April 3, 2003	Grozny, Chechnya	Bomb	Bus	No	6 killed - 10 injured	
April 24, 2003	Kfar Sava, Israel	Self-detonated explosives	Train station	Yes	1 killed - 13 injured	
April 25, 2003	Algermissen, Germany	Hijacking	Bus	No	0 killed - 0 injured	
May 18, 2003	Jerusalem, Israel	Self-detonated explosives	Bus	Yes	7 killed - 20 injured	
May 22, 2003	Gaza Strip	Bomb	Bus	No	9 injured	The bomb was placed next to the bus.
June 5, 2003	Chechnya	Bomb	Bus	Yes	16 killed	
March 11, 2004	Madrid, Spain	Multiple bombs	Multiple trains	No	191 killed - 1500 injured	

Appendix B. Case Studies of Transit Security Initiatives

The following four case studies illustrate transit security initiatives. Three studies of large transit agencies examine threats, constraints, and issues that impact facility security, in particular access management. One study of a federal government agency examines how state-of-the-art security technology and detailed security procedures can keep unauthorized persons from entering a facility.

Case study researchers interviewed managers at each of the agencies and conducted an extensive literature search; sources are listed in the References appendix.

Case 1 - Transit Agency #1

Transit Agency #1 created a Terrorism/Security Task force shortly after September 11, 2001, made up of five agency managers and led by the head of security. The task force made 122 recommendations.

The agency is currently planning two small pilot programs; one with a company manufacturing chemical detection systems, the other with a research lab that uses technology to track the frequency of particulates present in subway stations. This agency is also working with an engineering firm on a cleanup system that will use electrically charged droplets, consisting of a mixture of bleach and water, for post-incident response after a chemical/biological incident or attack.

Table B-1 summarizes effective practices for access control in the OCC and rail maintenance facilities at Transit Agency #1. One key practice is training employees to be aware of threatening situations. Several community involvement programs have started to observe and report suspicious behavior occurring within the transit system. Surveillance cameras are a supplementary reporting source. In addition, all agency employees and vendors must carry and display identification badges in all agency buildings and facilities.

Another key practice is gate control. Although fences are used around the maintenance yards, there is no gate control. The transit agency police have roving patrols that cover the yard and maintenance facilities. There is also a police patrol at stations that focuses on the main system areas of the system, i.e. subways in the downtown business districts, and K-9 patrols are used throughout the system.

Table B-1. Effective Practices for Access Control – Transit Agency #1

Category	Practices
Policies / Procedures	Form Terrorism/Security Task Force to identify security improvements Include representation from all departments Ensure Police/Security Department review every new construction project to assess design aspects Apply CPTED and SCP principles and techniques Provide terrorism/security training for all employees Perform periodic safety/terrorism drills Share anti-terrorism training programs and briefings with other transit organizations
Credentials / Identification	Issue identification badges to all vendors, requiring Possession of permanent address Immigration clearance Separate picture ID Renew badges periodically Require all employees to carry and display identification badges in all buildings Perform background checks on all employees
Control Techniques	Install fencing around maintenance yards Emphasize need for attention to suspicious activity to all employees if gates are not controlled Ensure police patrol all stations Block gates' access at night, such as with a parked bus
Surveillance	Install surveillance cameras throughout stations and the rest of the system Implement "observe and report" programs with local community groups taking advantage of youth services where possible Use K-9 patrols
Sensors	Install chemical detection systems at major stations Install biological hazard detection systems at major stations Install sensors on trains for wider coverage
Information Processing / Systems Integration	Use radio frequency technology to communicate sensor data to Control Center

Case 2 - Transit Agency #2

Transit Agency #2 uses a smart card for access control to a number of facilities, including the revenue-processing center and headquarters. The same smart card technology is also used as one form of fare collection.

Table B-2 summarizes effective practices for access control. One key practice is using a dual access control system at the agency's revenue processing facility to transition to the new smart card system.

Other key practices include supplementing the smart card access control system with other measures, such as surveillance cameras, intrusion detection, security patrol activity, and employee awareness. Training is an important transit priority, along with emergency preparedness; a key practice is all employees must carry and display identification badges in all buildings and facilities.

The primary access control measure in minimizing risks in the transit paid areas is by training employees to be aware of threatening situations. This is supplemented with the use of surveillance cameras. Using smart fare cards, the movement of riders can be tracked for forensic purposes (at the risk of violating privacy).

Table B-2. Effective Practices for Access Control – Transit Agency #2

Category	Practices
Policies / Procedures	Use dual system to transition from present access control to new system Use separate compartmentalized access control systems for different facilities and/or functions Employ hardware and software methods Use same credential (smart card) for different functions, including facility access control, parking garage access control, and transit fare collection Use strict privacy guidelines to prevent unauthorized use of individual data Institute training programs Focus on emergency response measures
Credentials / Identification	Use smart card as the main individual credential Allow different levels of accessibility via smart card system Issue smart cards to all employees
Control Techniques	Use contactless radio frequency technology Use turnstiles with smart card readers
Surveillance	Install surveillance cameras at entrance and other critical locations Use surveillance cameras for multiple functions when appropriate
Sensors	Install intrusion detection system with sensors at critical locations such as on windows
Information Processing/ Systems Integration	Use Wiegand backbone for card management and control Integrate the security system with the fire system (presently fire signal sent to police monitor; in the future, the fire signal will automatically bring up camera)

Case 3 - Transit Agency #3

Transit Agency #3 uses a smart card for access control to a number of facilities, including their revenue processing center, headquarters, maintenance, and repair yard and training facility. The agency also uses the smart card to access their automatic fare collection (AFC) equipment for service, repair, and security checks. The facilities and AFC application represent different compartmentalized activities. The card systems at these facilities are separate and run independently with their own computer.

Table B-3 summarizes effective access control practices at the facility and for AFC applications. One key practice is using the smart card to provide enhanced security for entering sensitive areas, such as the revenue processing facility, headquarters, and training facility, supplemented with other measures, such as surveillance cameras, barrier gates, elevator control, security patrol activity, and employee awareness. Training and emergency preparedness are also important practices. All employees are required to carry and display identification badges in all buildings and facilities. Background checks are performed on all employees and strict card recovery procedures are in place for employees who leave the agency.

Since transit systems are open systems there is only minimal control of individuals into the paid area including stations, onboard railcars, and on buses. It is these areas where people tend to congregate that a terrorist attack would be most likely. The key practice in addressing this issue is training employees to be aware of threatening situations, supplemented by surveillance cameras to respond to crises and to be used in post-incident examinations (forensics).

Table B-3. Effective Practices for Access Control – Transit Agency #3

Category	Practices
Policies / Procedures	Use same credential (smart card) for different functions, including facility access control and fare collection system maintenance Use separate compartmentalized access control systems for different facilities and/or functions Use smart card for security / integrity investigations Recover cards when a person is discharged Remove account numbers from computer Impose fines for certain cards not turned in Retrieve cards in person if necessary Limit parking to fixed range from buildings Institute training programs Provide "eyes and ears" training for all employees Provide bomb training Use the Security Awareness Training CD from the National Transit Institute Focus on emergency response measures
Credentials / Identification	Use smart card as the main individual credential; include individuals' names and employee numbers Allow different levels of accessibility via smart card system Require decals on cars Perform background checks on all employees; include financial and educational checks Issue temporary cards Issue paper passes with sign in / sign out and escort for short term

Category	Practices
	Use hard plastic IDs for longer term but not for employees
Control Techniques	Allow only certain elevators to access sensitive floors Require elevator-key control to access sensitive floors Use barrier gates at sensitive facilities
Surveillance	Install surveillance cameras at entrance locations Use surveillance cameras for multiple functions when appropriate Pilot program using cameras to monitor mouths of tunnels
Sensors	Integrate state-of-the-art sensor systems through available contractors Alarm exits of tunnels
Information Processing/ Systems Integration	Make sure that facility access control systems that hard-wired and self-contained

Case 4 - United States Governmental Agency

The U.S. agency case study is an example of a highly sensitive facility using state-of-the-art security technology and detailed security procedures to keep unauthorized persons from entering. The current integrated security system combines embedded Wiegand-wire technology identification credentials and readers with various barriers and perimeter security.

Table B-4 summarizes effective practices for access control at the U.S. agency. One key practice is using a layered approach to access management. All automobiles and delivery vehicles must pass through a manned perimeter-screening location. Pop-up or portable barriers are used on the access road to prevent unauthorized vehicles from simply driving past the perimeter screening.

The current access control system at the entrances to the agency's building and to the garage uses embedded Wiegand-wire access credentials. The entrances are laid out so that a person must first display their badge to security personnel for verification then present their credential to the turnstile reader for entrance to the restricted area. Persons in autos must present their credential to security personnel at the parking garage entrance for access. Visitors are first screened outside the facility, signed in by their escort, and again screened in detail by metal detectors and x-ray machines. An authorized person can then escort the visitor through the turnstiles into the secure area. Visitor badges are simple paper badges and require an authorized escort.

The U.S. agency is currently in the process of replacing the Wiegand-wire credential technology with smart card technology and a supporting access control system. The smart cards can be equipped with a microprocessor chip, a fingerprint scan biometric, a variable image, and a picture of the cardholder, and will be color-coded. The smart card will also be used for Public Key Infrastructure and computer logical access using the GSA Smart Card Interoperability Specification. These various identification devices provide redundancy in access control and allow varying levels of authentication. For example, the smart card can be used for entry at turnstiles by simply inserting the card into a reader, but a person's fingerprint will be read at an interior portal to a more sensitive area.

New visitor system badges will be magnetic stripe technology. Future procedures for escorting visitors will link the escort and the visitor in the computer system. The escorts will use their smart cards and the visitors their magnetic cards in tandem at the turnstiles for visitor entry. If readers are installed within the building at various portals, this procedure will show the movement of both the escort and the visitor.

The facility is also equipped with an extensive surveillance system. Numerous cameras observe all entry and exit points as well as the grounds, garage, and building interior. The surveillance system includes an advanced digital video monitoring system that records all video cameras at all times. The state-of-the-art system allows security personnel to control recording at the time of an incident and to review specific video after the incident.

The building is equipped with a command center that is the central point for all access management, surveillance, and intrusion detection systems, including workstations for all security sub-systems. From the command center, the appropriate staff can monitor and respond to security situations.

Another key practice is using an extensive security force at all perimeter access locations, the building entrance, visitor check-in desk, and the turnstiles. Other secured areas within the building requiring card entry may have additional security personnel.

Table B-4. Effective Practices for Access Control – U.S. Agency

Category	Practices
Policies / Procedures	Use a layered approach to security, with security measures at the perimeter, at entry/egress points, and within the facility Implement and update thorough identification and pass procedures Deploy extensive security force throughout the facility to augment technologies used
Credentials / Identification	Use Wiegand technology for access control system (current) Use smart card technology for employee/contractor cards, and Magnetic Stripe for visitor cards (future) Perform background checks on all non-visitor personnel Perform criminal background checks on visitors with the new system Allow different levels of accessibility via smart card system
Control Techniques	Use technology as primary means to verify personnel access at readers Use visual inspection as secondary means to verify personnel access at readers Install barriers at all entry/egress points Use X-ray and metal detector equipment at entry/egress points Require escorts for all visitors

Category	Practices
Surveillance	Use surveillance cameras extensively throughout facility Use state-of-the-art digital video recording system
Sensors	Implement extensive intrusion detection system throughout the facility
Information Processing/ Systems Integration	Arrange for dual computer system for card management and control provides, for redundancy Designate the command center as the central point for all security systems

This page left intentionally blank

Appendix C. Performance Measures

Performance measures consist of:

- Inputs
- Efficiency/Effectiveness
- Adoption
- Outputs
- Extensiveness
- Quality
- Impact
- Usefulness

Inputs

Inputs are the resources used in providing services. Agencies might begin by asking whether there are adequate operating resources (funding and personnel) to achieve the goals, and whether the technology infrastructure (cameras, access control devices, etc.) are sufficient to ensure adequate response. In addition, the following should be considered:

- Financial indicators (funding level, budget)
- Number/cost of security force officers
- Cost of protection equipment
- Maintenance, testing costs
- Training costs

Efficiency/Effectiveness

Efficiency and effectiveness measures how well the security system or program meets objectives and productivity gains. The following should be considered:

- Degree to which the timeliness of access is increased
- Work/activity levels
- Loss reductions (assets)
- Number of crime related events
- Number of lawsuits
- Amount of court time for officers
- Number of officers necessary to conduct surveillance of public areas
- Percent of clearance errors; time to process clearance
- Percent of security violations

- Security violations per audit
- Percent of audits conducted on schedule
- Percent of security equipment checked per schedule
- Number of security problems identified by management versus total security problems identified
- Security violations by department/facility
- Number of security suggestions
- Results of screening
- Ridership
- Level of absenteeism
- System down time; average time for equipment repairs
- Service recovery times
- Time to detect
- Number of entries (attempts by undefined users; successes by undefined users; violations by undefined users)
- Number of alarms; average response time to alarm; number of false alarms; time spent on response to false alarms
- Percentage of workers in compliance with training standards
- Response force communication time

Adoption

This measures the extent to which security policies, programs and countermeasures are incorporated into organizational or individual activities. Indicators in this group:

- Compliance (employee breaches)
- Enforcement
- Complaints / Suggestions

Outputs

Outputs are indicators of the products or services resulting from the use of resources. They include:

- Number of credentials issued, revoked
  Training performed
- Inspections performed
- Security drills conducted
- Covert tests conducted
- Performance tests conducted

- Physical security audits conducted (e.g., barriers, locks, alarms, communications, response times/procedures)
- Access control policies/procedures/ processes reviewed/audited (e.g., visitors, vendors, temporary employees, key control)
- Reports produced
- Number of investigations / results of investigations (prosecutions/convictions)
- Results of conducting daily security checks - signs of tampering, other unusual situations
- Work/activity levels

Extensiveness

The following evaluate how much of a service is provided and the completeness of coverage:

- Activity levels by time periods
- Number of entries
- Number of facilities/doors coved by access control systems
- CCTV coverage area

Quality

The following help to measure how well security services/activities are performed and how well the security system functions:

- Number of denials of legitimate access
- Successful entries
- Time between user contact request and system response
- Customer complaints/suggestions – customer needs/satisfaction
- Legal and policy conditions affecting agency (e.g, - provisions for accessibility for persons with disabilities, safety regulation compliance)
- Level of availability (e.g., 24 hours, 7 days a week)
- Detection/alarm system accuracy

Impact

Measures should also assess how a service makes a difference in some other activity or situation. Are impacts positive, negative or both? Do positive impacts outweigh negative impacts? Can negative impacts be remedied or otherwise addressed?

Usefulness

To what degree are the services useful or appropriate and how well are the needs of users (security force, employees, patrons, management) met? This might be measured by:

- Comments, surveys and focus group results

- Increases in user productivity
- Degree to which security system information is incorporated into other tasks inside and outside the agency
- Requests for information from security systems

Appendix D. Vehicle Barrier Types and Effectiveness

This appendix describes the following barrier types:

- Natural material and cosmetic barriers
- Fabricated barriers

Natural Material and Cosmetic Barriers

Natural and cosmetic barriers are effective if integrated into security planning, new construction, or renovation projects. Natural obstructions such as hills, outcroppings, lakes, and ponds can be used to stop, deter, or slow a vehicle trying to enter a facility. Natural materials, wood, dirt, and rock, can be used to build berms and walls that prove to be effective barriers, yet do not detract from the aesthetics of the site landscaping.

Factors to take into account include:

- Vegetation
- Water
- **Terrain**

Vegetation

Vegetation along standoff zone perimeters and on off-road approaches to the perimeters can deter aggressors from approaching the protected facility from that route. Vegetation may also slow the approach of vehicles by providing obstacles to direct approach. Closely spaced plants in multiple, overlapping rows with trunk diameters greater than 5 inches are the best deterrents to stationary vehicles. Perimeter barriers capable of stopping moving vehicles can be integrated with plantings of vegetation for aesthetics purposes. Because mature plants are the most effective deterrents, the required plant material should be provided by retaining existing vegetation where possible.

Water

The effectiveness of bodies of water used as barriers to moving vehicles has not been quantified, but their value in slowing vehicles and as a deterrent is obvious. Water that is deep enough to submerge the exhaust pipes of vehicles will provide an effective barrier. Lesser depths may only slow vehicles. For example, cars and light trucks will be limited to speeds of approximately 25 miles per hour by large bodies of water only 6 inches deep. Bodies of water 3 feet deep would act as barriers to moving vehicles. If the body of water floor is uneven or contains several deep trenches, the effectiveness as a barrier increases significantly.

Terrain

Terrain features such as ditches, berms, hills, or large rocks may provide effective barriers to vehicles. Rocks or groups of rocks that have a collective mass equal to approximately twice that of the threatening vehicle make effective barriers. To be effective, rock ditches, and berms must span the approach route to block it. Those of lesser extent or such features of a size too small to stop a vehicle can be used as obstacles to slow vehicle approaches. In designing terrain obstacles, circuitous, off-road approach routes are far more effective than direct routes. As an example, the use of inclines can slow vehicle approaches by limiting their ability to accelerate.

Fabricated Barriers

The types of fabricated vehicle barriers include:

- Concrete (Jersey)
- Portable water/sand-filled
- Chain link/gate reinforcement
- Cable
- Drum and cable
- Dragnet
- Bollard
- Removable nuisance
- Guardrail
- Traffic control island
- Motorized barricade
- Hydraulic barricade
- Electronic barrier gate
- Tire penetrating
- Portable roadblock

Concrete Barrier (Jersey Barrier)

Barriers can be erected from either precast tongue and groove sections or cast in place with special concrete-forming equipment. These barriers can be used around a fixed site as a perimeter vehicle barrier. Barriers can also be arranged to direct and slow traffic flow into a site. This gives the security personnel at the gate more time to react to a potential threat.

Portable Water/Sand-Filled Barriers

Plastic water or sand-filled barriers can be effective, as well as being easily moved without the need for heavy equipment.

Chain Link Gate Reinforcement

Wire ropes are fastened to gates and anchored on either side of the gate. For a relatively weak gate, the reinforcement transfers the force of a vehicle impact to a more substantial anchor system. It can be used on many different gate applications.

Cable Barrier

Cable is fastened to each post with U-clamps at a height of 30 inches and is periodically anchored. The cable is typically ¾-inch diameter or larger aircraft cable mounted between chain link fabric and upright posts. The barrier prevents light vehicles from crashing through a standard chain link fence. One disadvantage is that the cable can be covertly cut when installed along the outermost perimeter.

Drum and Cable Barrier

Standard 55-gallon drums are filled with dirt, rock or concrete—weighing about 900 to 1,200 pounds—attached by a ¾-inch aircraft cable to another drum or fixed object. Requires minimal setup time and expense. This can be a cost-effective application since empty storage drums, dirt and rock are readily available.

Dragnet

This consists of a chain link "net" assembly with arresting cables attached to an energy absorber that is attached to the anchor system. In the open position, the dragnet is suspended above the access road. When a vehicle hits the dragnet in the closed (dropped) position, the energy form the impact is transferred through the arresting cables to an energy absorber that brings the vehicle to a controlled stop.

Bollard

A bollard is a post made of concrete, stainless steel, aluminum, cast iron, or other durable material, that creates an aboveground obstacle. Bollards can be fixed or retractable. At the high end, bollards are constructed to completely stop most vehicles.

Removable Nuisance Barrier

A 3-inch pipe driven into the ground and fastened with $^{3}/_{16}$-inch coil chain, is used to channel traffic and create marked isolation zones around sensitive areas, equipment, and buildings. It can be set up and removed quickly and easily.

Guardrail

Standard highway guardrails or median barriers; cable, W-beam, or box beam guardrails are used as a perimeter barrier. They are not designed to prevent head-on penetrations but can immobilize a lightweight vehicle attempting an intrusion.

Traffic Control Island with Vehicle Barriers

Standard guard post, with two automatic gates, a custom base, platform curb assembly with three pass-throughs, and 16 barrier posts provide protection for security personnel stationed at vehicle entrance.

Motorized Barricade

This refers to a steel barricade with standard height of 13 inches, and a maximum height of 30 inches. Several activation options are possible, such as by remote switch or card reader. These barricades provide a steel barrier that can be deployed to close off vehicle access in approximately three seconds.

Hydraulic Barricade

Upon major impact, the lifting mechanism absorbs the shock. In emergency situations, a steel barricade closes off vehicle access in just one second.

Electronic Barrier Gate

Chain link gates and turnstiles used for vehicle and personnel entrances, electronic barrier gates may be activated by remote switch, numerical code, or card reader.

Tire-Penetrating Traffic Barrier (One-way Tire Trendles)

A row of $^{3}/_{8}$-inch steel teeth that are unidirectional, spring-loaded, are embedded in the road. The barrier punctures the tires of an intruding vehicle, while allowing passage of vehicles in the opposite direction.

Portable Roadblock Tire-Puncturing Device

Hollow stainless steel spikes mounted on aluminum scissors action arms expand to stretch across a vehicle access. Anchors hold the scissors in place. The system expands to cover 21 feet and folds into a case weighing 35 pounds. When an intruding vehicle passes over the system, the spikes imbed into the vehicle’s tires and detach from the aluminum frame. This opens several "tubes" which cause rapid uniform deflation and prevent the holes from sealing. Since the air loss is uniform from all times, the operator is more likely to maintain control of their vehicle. These devices are most effective against light vehicles with standard ¾-inch thick rubber tires.

Appendix E. Vehicle Barrier Selection and Implementation Considerations

This appendix provides details on:

- Barrier selection considerations
- **Implementation issues** in selecting barriers
- **Crash performance data** for active and passive barriers

Barrier Selection

Threat /Desired Use

Select the level of security that is required for a particular facility based on a threat and vulnerability assessment. Barriers can be used to protect against several common aggressor tactics including: bombs in moving vehicle, bombs in stationary (parked) vehicle, or forced-entry attacks.

Degree of Protection/Crash Rating

Determine the degree of protection (range of physical restraint) required. To do this, knowledge of the setback, vehicle speed, vehicle approach angle, vehicle weight, and size of explosive package is required. Table E-1 lists test results of different types of active and passive barrier testing. For a list of specific make/models of Department of State (DOS) certified anti-ram vehicle barriers refer to **http://www.statebuy.state.gov/compad/documents/CertifiedVehicleBarriersRevA-02-04-05.doc**

Barriers are tested and certified to perform to specific Federal criteria (a specific level of anti-ram protection). In selecting barriers, it is important that transit agency security engineers consider the capabilities of these systems to protect against the threats specific to the facility. For crash-rated barriers, the weight and speed of the crashing vehicle are specified as well as the "allowed movement" of the barrier upon impact. There is a wide range of weights and speeds based on anticipated threat and physical approach.

Refer to the following documents for a list of standards and requirements that a potential product must satisfy to become qualified: Department of State (DOS) standard, SD-STD-02.01 (latest revision) – *Specification for Vehicle Crash Test of Perimeter Barriers and Gates*, and 12 FAH 5 – *Foreign Affairs Handbook – Physical Security Handbook*.

Table E-1. Tested Barrier Design – Test Results

		Vehicle		**Protection Level** **(0-10)**
		Weight	**Speed**	0 10
Passive Barrier Test Results	Concrete filled steel bollards	4,500	30	1
	Jersey Barrier	4,000	50	2.6
	Straight Retaining Wall	15,000	30	3.6
	Sloped Back Retaining Wall	15,000	40	6.4
	Concrete Planter / Retaining Wall	15,000	50	10
Active Barrier Test Results	Cable - Beam Barrier	10,000	15	0.6
	Retractable Bollards	15,000	30	3.6
	Portable Barriers	15,000	40	6.4
	Drum Type Barriers	15,000	50	10
	Sliding Gate	15,000	50	10

Source: Military FM 5-114

Passive vs. Active

Passive barriers can be used at entry points if traffic flow is restricted or rarely used. Passive barriers are normally used for perimeter protection.

Portability

What is involved if the barrier needs to be moved/repositioned? Some barriers are massive and heavy, requiring the use of heavy equipment for placement. Once placed, these barriers can only be moved by bringing in heavy lifting equipment, and cannot be quickly changed to allow access status for authorized vehicles. If portable, how easy is the barrier to carry, transport, stack, store, and put together/interlock? What is the time needed to deploy?

Width / Load Capacity

Are the appropriate widths available to fully protect while allowing passage of almost every type of vehicle?

Barrier Activation Mode

For high traffic entries, vehicle barriers are normally open and closed only upon detection of a threat. For "low flow" or "high threat" conditions, barriers are normally closed in order to stop vehicle flow and are lowered only after authorization has been approved (this is the more secure mode). For automated vehicle access systems the barrier should automatically return to the closed/protected position once a sensor has detected vehicle passage and should not allow tailgating. Whether the barrier can be locked in the up or down position should also be noted.

Access Control Options

Control for vehicles can include either automated or semi-automated access control, or manual access control. In automated or semi-automated access control, the driver of the vehicle will use a machine-readable device to open the barrier, or present suitable identification via CCTV to a remote monitoring station. In a manually controlled situation, a security person is stationed at the point of entry to monitor access. Ensure that the barrier selected can be operated by a variety of control systems to satisfy your current and future needs, including needs for card and proximity readers, for keypads, for inductive loops, and for intercom. The ability to operate the system locally and/or by remote control should also be considered in the selection process.

Compatibility with Other Security Components

Active barriers should be compatible with other security equipment installed at the site (IDS, CCTV, etc.) and with the available power source.

Operation

Barriers can be operated manually, electrically, pneumatically, or hydraulically. Can the system operate individually and in groups? Is there a manual override? Can the system work in manual operation in the event of power failure? Barrier direction should be instantly reversible at any point in its cycle from the control station(s).

Consider Options / Alternate Approaches

Options exist for reconditioning, refurbishing, or covering existing barriers. It is also possible to initiate an evolutionary plan in which the perimeter is progressively covered or where the entire perimeter is covered with something that can evolve to a higher level of protection over time. The difficulty of making site modifications (e.g., relocating truck deliveries away from the protected facility) that would to make vehicle barrier unnecessary or a lesser-rated barrier acceptable should also be assessed.

Barricade Speed / Response Time

The barrier system must contain sufficient time delay after activation to allow the vehicle to enter or exit the parking area.

Cycle Time/Pass-through Rates

Ensure that the device pass-through rate is consistent with the desired vehicle processing (3 to 15 seconds is suitable for most inspection and identification station requirements).

Environment

Not all barriers will be suited to all locations. Barrier components may require protection from excessive heat/cold, dirt, humidity, sand, high water table, or require additional maintenance.

Reliability / Maintenance

Reliability is an important factor in selecting active barriers. Most manufacturers offer maintenance contracts. If a facility requires an active vehicle barrier, the company selected can provide adequate service. Will it require painting and is it resistant to corrosion? Know what, where, when, and how maintenance will be done. Evaluate the system's failure modes to ensure that the barrier will fail in the predetermined position (open or closed) based on the security and operational requirements. Backup generators or manual override provision are needed to ensure continuous operation during power failures or equipment malfunction. Reliability and maintainability data are available from most manufacturers.

Safety Options / Features

Active barrier systems are capable of inflicting serious injury, even when used for their intended purposes. Warning devices (visible colors and patterns, reflectors, lighting, warning lights, and safety signals) should be used to mark the presence of a barrier and enhance its visibility to drivers. Vehicle detector safety loops and road plates checkered for good traction can also enhance safety.

Mounting / Foundation Requirements

Consider the costs of sitework for mounting or foundations:

- *Surface Mounted* – quick installation in difficult locations such as parking structure ramps or areas with sub-surface drainage problems.
- *Shallow Foundation* – sub-surface conditions that negate extensive excavations and obviate the concerns of interference with buried pipes, power lines, and fiber optic communication lines; reduces installation complexity, time, materials, and corresponding costs.
- *Sub Surface* – can require extensive excavations and the need to work around buried pipes, power lines, and fiber optic communication lines.

Aesthetics

What range of visual dissonance is acceptable? An attractive appearance is usually desirable, but can contribute to the cost. The aesthetic components include color, texture, shape, and live material (plantings).

Liability

Liability issues resulting from death or injury due to normal operation or inadvertent use/ malfunction should be considered.

Budget

What range of financial resources is available? It is important to ensure that the total cost is anticipated in the preliminary planning stages. In addition to the actual cost of the barrier product, whether purchased or fabricated on site, there may be freight, placement, equipment rental, utility modification, site-work, clean up, or other related expenses. Reliability, availability, and maintainability requirements will affect the cost of the system.

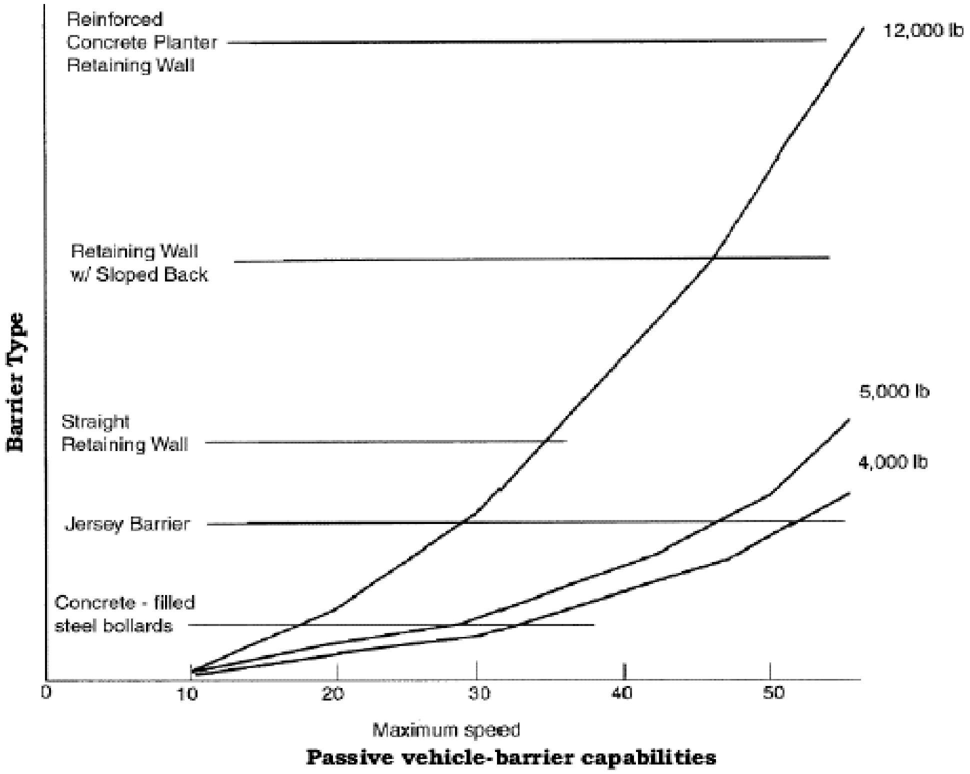
Implementation Issues

- Plan appropriate space if vehicle inspections are to take place. Locate the inspection area at the appropriate standoff distance from the facility. If possible use separate entrances for employees, visitors, and deliveries. If this is not possible, multiple lanes (for employees and others) can help to maintain maximum employee traffic flow. Clearly mark visitor/delivery entrances and lanes.
- Place active barriers away from inspection areas to reduce the required guard reaction time.
- Locate barrier support equipment (e.g., hydraulic power, generator, etc.) on the secure side away from guard posts to lower the threat of sabotage and injury to security personnel.
- Tamper switches should be installed on all vehicle barrier access doors, controllers, and hydraulic systems. Tamper switches should be connected to a central alarm station.
- Mark active barriers once they are installed and channel pedestrian traffic away from the system.
- Design barriers installed in clear zones so that they will not provide a protective shield or hiding place.
- Consider the use of barriers to stop vehicles from entering the wrong way via exit lanes.
- Ensure that buttresses, counterweights, and road plates do not obstruct authorized pedestrian or vehicular traffic.

- Plan for the appropriate use of safety equipment, such as traffic lights, inset warning lights, appropriate signage ("stop", "no entry", or "warning"), and safety buffers. Use clear signage and traffic control lights with active barriers.
- Provide operator training to prevent injury, reduce liability, and prevent equipment damage caused by improper operation.

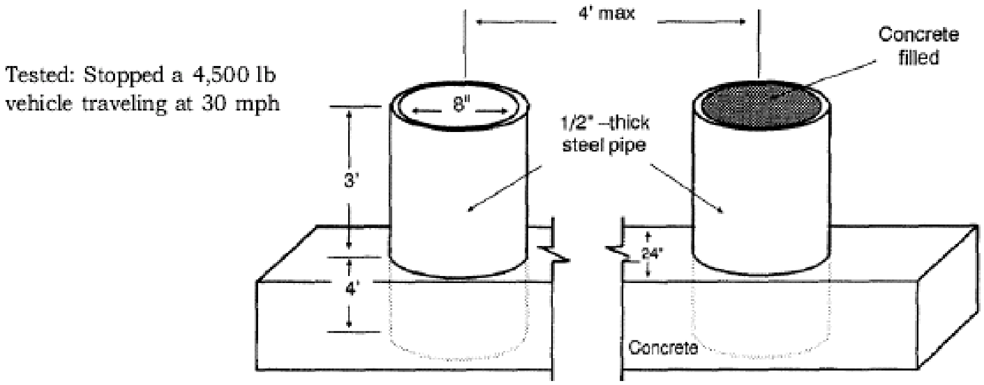
Crash Performance Data

The following diagrams showing crash performance data for a variety of passive and active barriers Data is from *Military Field Manual FM 5-114*.



Source: Military FM 5-114

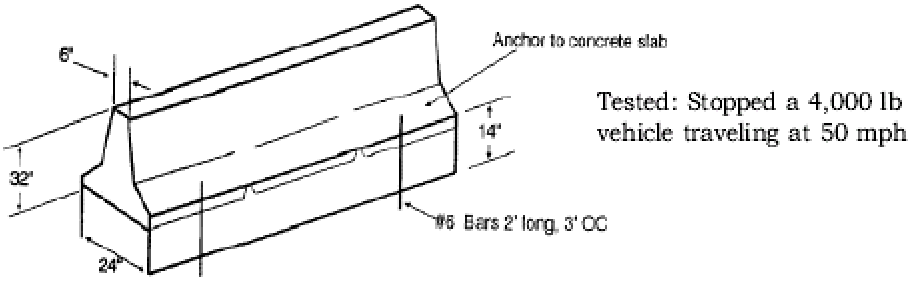
Figure E-1. Passive Vehicle-Barrier Capabilities



Tested: Stopped a 4,500 lb vehicle traveling at 30 mph

Source: Military FM 5-114

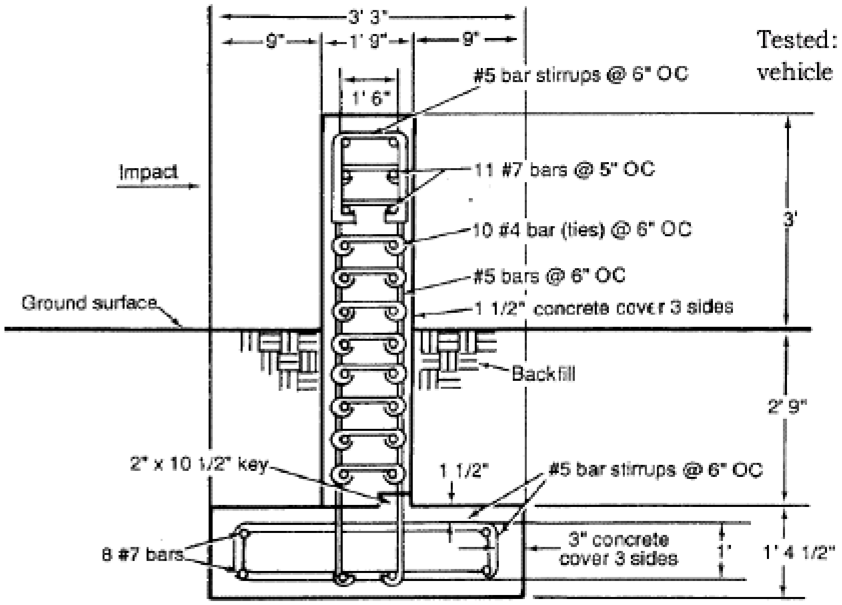
Figure E-2. Concrete Filled Steel Bollards



Tested: Stopped a 4,000 lb vehicle traveling at 50 mph

Source: Military FM 5-114

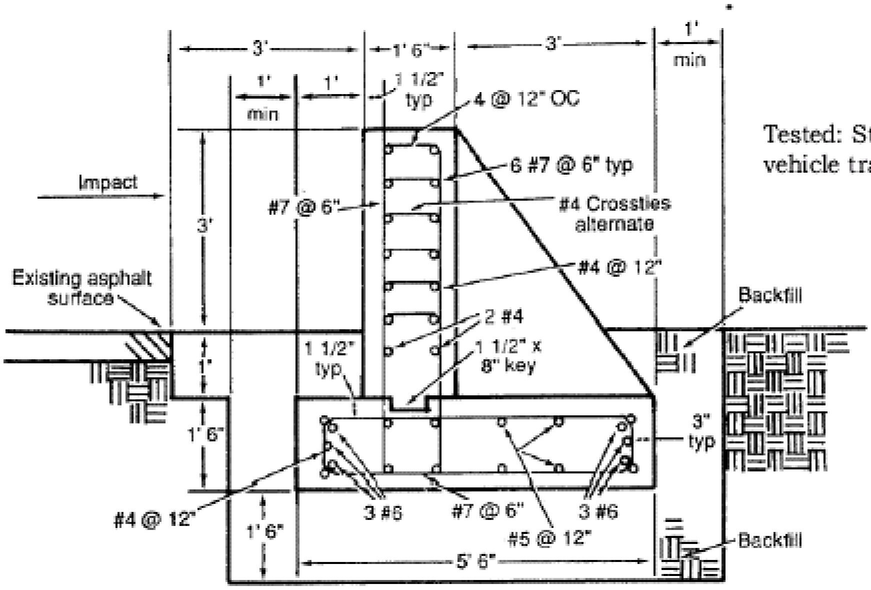
Figure E-3. Jersey Barrier



Tested: Stopped a 15,000 lb vehicle traveling at 30 mph

Source: Military FM 5-114

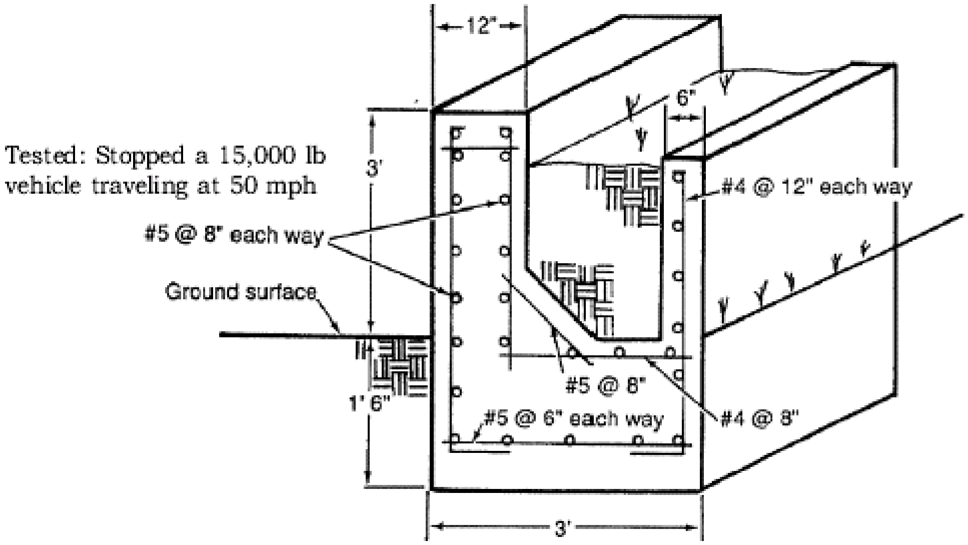
Figure E-4. Straight Retaining Wall



Tested: Stopped a 15,000 lb vehicle traveling at 40 mph

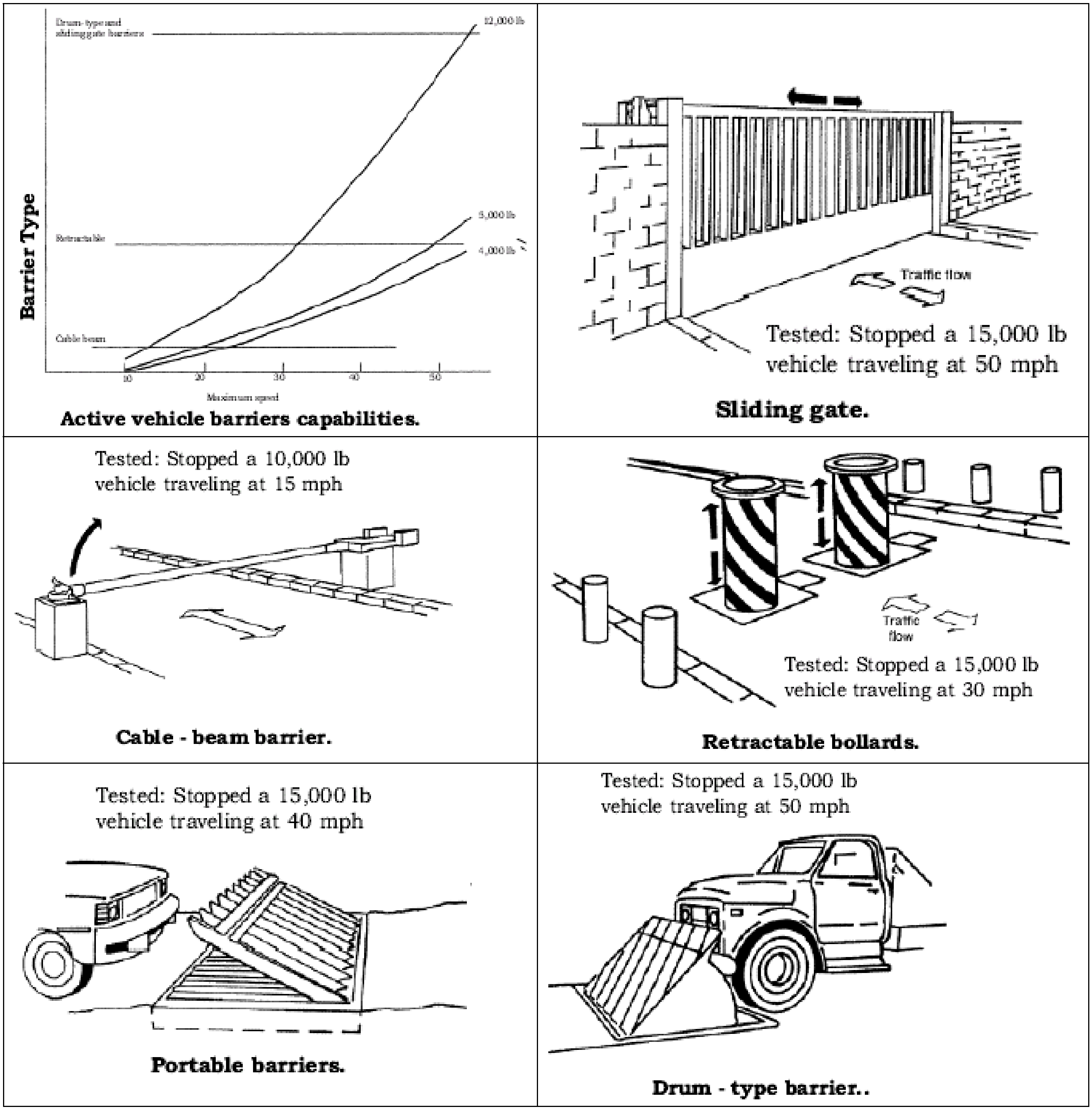
Source: Military FM 5-114

Figure E-5. Sloped-Back Retaining Wall



Note: Each wall must be calculated based on soil conditions at that site. Concrete: f'c = 3,000 psi. Reinforcement steel bars: fy = 60 ksi. 1 ½-inch concrete cover all around, except as noted.
Source: Military FM 5-114

Figure E-6. Reinforced Concrete Planter/Retaining Wall



Active vehicle barriers capabilities.

Tested: Stopped a 15,000 lb vehicle traveling at 50 mph

Sliding gate.

Tested: Stopped a 10,000 lb vehicle traveling at 15 mph

Cable - beam barrier.

Tested: Stopped a 15,000 lb vehicle traveling at 30 mph

Retractable bollards.

Tested: Stopped a 15,000 lb vehicle traveling at 40 mph

Portable barriers.

Tested: Stopped a 15,000 lb vehicle traveling at 50 mph

Drum - type barrier..

Source: Military FM 5-114

Figure E-7. Active Barrier Test Results and Examples

Appendix F. Codes and Standards

Appendix F lists codes and standards for:

- Infrastructure
- Buses

Appendix F1. Infrastructure

This section provides details on infrastructure codes and standards for:

- Facilities
- Emergency response
- Materials
- **Electrical**
- **Mechanical**
- **Plumbing**
- **Fire protection**
- **Fuels**

Facilities

American Society of Civil Engineers; standards. **http://www.pubs.asce.org/**

American Association of State Highway and Transportation Officials (AASHTO); *Standard Specifications for Highways and Bridges*

International Code Council; *International Building Code*

National Fire Protection Association (NFPA), *502 Standard for Road Tunnels, Bridges, and Other Limited Access Highways.* **http://www.nfpa.org/**

NFPA; *130 Standard for Fixed Guideway Transit and Passenger Rail System*

NFPA; *88A Standard for Parking Structures*

Masonry Advisory Council; building codebooks

Research Council on Structural Connections; structural connections standards. **http://www.boltcouncil.org/**

Truss Plate Institute; metal plate connected wood truss standards. **http://www.tpinst.org/my_standards.html**

Emergency Response

International Code Council; international performance codes. **http://www.iccsafe.org/cs/**

NFPA 101; *Life Safety Code*

NFPA 101A; *Guide on Alternative Approaches to Life Safety*

NFPA 101B; *Code for Means of Egress for Buildings and Structure*

Materials

American Concrete Institute (ACI) 318; *Building Code Requirements for Reinforced Concrete.*

ACI 530; *Building Code Requirements for Masonry Structures and Specifications for Masonry Structures & Commentaries.*

American Institute of Steel Construction (AISC) *Specification for Structural Steel Buildings-Allowable Stress Design and Plastic Design.*

AISC; *Load and Resistance Factor Design Specification for Structural Steel Buildings.*

American Forest and Paper Association; *National Design Specification for Wood Construction.*

Aluminum Association; aluminum industry standards. **http://www.aluminum.org/**

American Architectural Manufactures Association; fenestration (window) performance standards. **http://www.aamanet.org/**

American Hardboard Association; **http://www.pbmdf.com/**

American Iron and Steel Institute; **http://www.steel.org/**

American Institute of Timber Construction; glued laminated timber standards. **http://www.aitc-glulam.org/**

American National Standards Institute; **http://www.ansi.org/**

American Plywood Association; engineered wood products standards. **http://www.apawood.org/**

American Society for Testing Materials; **http://www.astm.org/**

American Wood Preservers Association; **http://www.awpa.com/**

American Welding Society; welding standards. **http://www.aws.org/**

Canadian General Standards Board; **http://www.pwgsc.gc.ca/cgsb/**

Canadian Standards Institute; **http://www.csa.ca**

Cedar Shake and Shingle Bureau; **http://www.cedarbureau.org/**

Canadian Wood Council; wood product and wood building codes. **http://www.cwc.ca/**

Gypsum Association; **http://www.gypsum.org/**

Hardwood Plywood and Veneer Association; **http://www.hpva.org/**

National Concrete Masonry Association; **http://www.ncma.org/**

National Institute of Standards and Technology; **http://www.nist.gov/**

Rubber Manufacturers Association; **http://www.rma.org/**

Steel Joist Institute; **http://www.steeljoist.com/**

U.S. Department of Commerce; **http://www.commerce.gov/**

U.S. Department of Transportation; **http://www.dot.gov/**

U.S. Consumer Product Safety Commission; voluntary consumer product standards. **http://www.cpsc.gov/**

Western Red Cedar Lumber Association; **http://www.wrcla.org/**

Electrical

Electronics Industries Alliance; **http://www.eia.org/**

ICC International Electrical Code; **http://www.internationalcodes.net/**

NFPA 70; *National Electrical Code*

Mechanical

American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE); *ASHRAE Handbook, 2003 HVAC Applications*

International Association of Plumbing and Mechanical Officials (IAPMO); *Uniform Mechanical Code*

International Code Council (ICC), *International Mechanical Code*

NFPA *90A Standard for the Installation of Air-Conditioning and Ventilating Systems*

NFPA *90B Standard for the Installation of Warm Air Heating and Air-Conditioning Systems*

NFPA *91 Standard for Exhaust Systems for Air Conveying of Vapors, Gases, Mists, and Noncombustible Particulate Solids*

U.S. Department of Transportation; *Subway Environmental Design Handbook Volume 1 Principles and Applications*

U.S. Department of Transportation; *Subway Environmental Simulation Computer Program*

Plumbing

IAPMO, *Uniform Plumbing Code*:

ICC, *International Plumbing Code*: International Code Council

ICC, *International Private Sewage Disposal Code*

Plumbing-Heating-Cooling Contractors Association, *National Standard Plumbing Code*

Fire Protection

International Code Council, *International Fire Code*

NFPA 1; *Uniform Fire Code*

NFPA 10; *Standard for Portable Fire Extinguishers.*

NFPA 13; *Standard for the Installation of Sprinkler Systems*

NFPA 14; *Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems*

NFPA 72; *National Fire Alarm Code*

Underwriters Laboratories

Fuels

International Code Council; *International Fuel Gas Code*

NFPA 30A; *Code for Motor Fuel Dispensing Facilities and Repair Garages*

NFPA 52; *Compressed Natural Gas (CNG) Vehicular Fuel Systems Code*

NFPA 54; *National Fuel Gas Code*

NFPA 55; *Standard for the Storage, Use, and Handling of Compressed Gases and Cryogenic Fluids in Portable and Stationary Containers, Cylinders, and Tanks*

NFPA 57; *Liquefied Natural Gas (LNG) Vehicular Fuel Systems Code*

NFPA 58; *Liquefied Petroleum Gas Code*

NFPA 59; Utility LP-Gas Plant Code

Appendix F2. Buses

This section provides details on bus statutes, regulations, and codes and standards:

- Statutes

- Regulations
- Codes and standards

Statutes

Clean Air Act, Amendments, 1990, Title II, Provisions Relating to Mobile Sources, Public Law 101-549.

Energy Policy Act of 1992 (EPACT), Public Law 102-486.

Alternative Motor Fuels Act of 1998 (AMFA), Public Law 100-494.

Regulations

29 CFR, Part 1910 - Occupational Safety and Health Standards (OSHA).

29 CFR, Section 1910.103, Subpart H: Hydrogen.

40 CFR, Part 86 – Control of Air Pollution from New and In-Use Motor Vehicles and New and In-Use Motor Vehicle Engines: Certification and Test Procedure.

49 CFR, Part 171 - Hazardous Materials Regulations.

49 CFR, Part 571 - FTA Regulation on Bus Testing

49 CFR, Part 573 - FMCSA Federal Motor Carrier Safety Regulations.

49 CFR, Part 571 - NHTSA Federal Motor Vehicle Safety Standards in.

Superfund Amendments and Reauthorization Act (1986), SARA Title III. (U.S. EPA)

Codes and Standards

This section bus codes and standards for the following organizations:

- ANSI
- ASME
- EPRI
- ICC
- ISO
- NFPA
- SAE
- UL

American National Standards Institute (ANSI)

ANSI-CSA NGV2-2000 and NGV2a-2001. Basic requirements for compressed Natural Gas Vehicle (NGV) fuel containers. In 2005 hydrogen will also be included

ANSI-CSA PRD-1. Basic requirement for pressure relief devices for natural gas fuel containers. In 2005 hydrogen will also be included.

ASME

Boiler and pressure vessel codes

Electric Power Research Institute (EPRI)

Electric Bus Technical Specifications

ICC

Building and fire codes (hydrogen being added)

International Organization for Standardization (ISO)

ISO Standard 6469 Parts 1, 2, and 3; *International Guidelines For Wiring, Safety Issues, and Electrical Isolation*

National Fire Protection Association (NFPA)

NFPA 30A; *Automotive and Marine Service Station Code*. This standard applies to automotive and marine service stations and to service stations located in buildings.

NFPA 50A; *Standard for Gaseous Hydrogen Systems at Consumer Sites* (1994 Edition).

NFPA 50B; *Standard for Liquefied Hydrogen Systems at Consumer Sites* (1994 Edition).

NFPA 52; *Standard for Compressed Natural Gas (CNG) Vehicular Fuel Systems*. This standard applies to the design and installation of compressed natural gas (CNG) engine fuel systems on vehicles of all types including aftermarket and Original Equipment Manufactures (OEMs) and to their associated fueling (dispensing) systems. Beginning in 2005 NFPA 52 will cover infrastructure for compressed and liquid hydrogen but will not cover vehicles.

NFPA 54; *National Fuel Gas Code*. This code is a safety code that shall apply to the installation of fuel gas piping systems, fuel gas utilization equipment, and related accessories.

NFPA 57; *Standard for Liquefied Natural GAS (LNG) Vehicular Fuel Systems*, 2002 Edition. (beginning 2005 part of NFPA 52)

NFPA 58; *Standard for the Storage and Handling of Liquefied Petroleum Gases*. This standard describes the minimum requirements that LPG facilities and vehicles must meet to ensure safety.

NFPA 59A; *Standard for the Production, Storage and Handling of LNG,* 2002 Edition.

NFPA 70; *National Electric Code.* The purpose of this code is the practical safeguarding of persons and property from the hazards arising from the use of electricity.

NFPA 72; *National Fire Alarm Code*, 2002 Edition

NFPA 88A; *Standard for Parking Structures.* This standard covers the construction and protection of, as well as the control of hazards in, open, enclosed, basement, and underground parking structures. This standard does not apply to one- and two-family dwellings.

NFPA 88B; *Standard for Repair Garages.* This standard covers the construction and protection of, as well as the control of hazards in, garages used for major repair and maintenance of motorized vehicles and any sales and servicing facilities associated therewith (now part of NFPA 30A).

NFPA 497A; *Recommended Practice for Classification of Class I Hazardous (Classified) Location for Electrical Installations in Chemical Process Areas.* This recommended practice applied to locations where flammable gases or vapors, flammable liquids or combustible liquids are processed for handled and where their release to the atmosphere may result in their ignition by electrical systems or equipment.

Society of Automotive Engineers (SAE) Recommended Practices

J406: *Recommended Practice CNG Powered Medium and Heavy Duty Trucks*

J1718; *Measurement of Hydrogen Gas Emission From Battery-Powered Passenger Cars and Light Trucks During Battery Charging*

J1742; *Connections for High Voltage On-Board Road Vehicle Electrical Wiring Harnesses*

J759; *Hydrogen Fuel System Safety* (light duty but could be useful for medium- heavy duty). To be published end of 2004

J1766; *Recommended Practice for Electric and Hybrid Electric Vehicle Battery System Crash Integrity Testing*

J1673; *High Voltage Automotive Wiring Assembly Design*

J1797; *Packaging of Electric Vehicle Battery Modules.*

J1798; *Performance Rating of Electric Vehicle Battery Modules*

J2293; *Energy Transfer System for Electric Vehicles*

J2344; *Guidelines for Electric Vehicle Safety*

J2600; *Fueling Nozzles and Connectors*

J2711; *Vehicle Emissions Testing* (update to J1711)

J2758; *Fuel Cell Vehicle Safety* (Light duty)

Underwriter's Laboratories (UL)

UL 50; *Standard for Enclosures for Electrical Equipment*

UL 991; *Standard for Tests for Safety-Related Controls Employing Solid State Devices*

UL 1244; *Electrical and Electronic Measuring and Testing Equipment*

UL 1439; *Determination of Sharpness of Edges on Equipment*

UL 1998; *Standard for Safety-Related Software*

UL 2202; *Electric Bus Charging System Equipment*

UL 2231; *Personnel Protection Systems for Electric Bus Charging Circuits*

UL 2251; *Plugs, Receptacles, and Couplers for Electric Vehicles*

Appendix G. Lessons Learned from Transit Communications Emergencies

Transit agencies can use communications experiences from real-world emergencies not only to respond better during times of crisis, but also to improve communication during day-to-day operations.

Two recent emergencies that transit agencies can learn from include the September 11, 2001 terrorist attacks on New York City and Washington, D.C., and the August 14, 2003 blackout that occurred across the Northeastern United States.

This appendix describes how transit agencies responded to the:

- September 11, 2001 terrorist attacks
- **August 14, 2003 blackout**

Summary

Communications lessons learned from these two emergencies include:

- A single point of failure can disrupt the entire communications system.
- It is important for an agency to maintain backup power for all segments of its communications network.
- The need for interoperable communications among agencies increases during emergency situations.
- It is important for an agency to have multiple forms of communications technology at its disposal.
- The problems experienced with communications technology in one emergency may be very different in the next emergency. An agency needs to be prepared for a changing set of circumstances.
- The public can now obtain information from multiple sources, including e-mail alerts, Internet updates, cell phones, and radio technologies.
- A communications system will experience an unusually high demand during an emergency, exactly when it may be the most vulnerable. Agencies should take advantage of federally sponsored emergency communications programs to ensure they are able to maintain communications during such times.

September 11, 2001 Terrorist Attacks

- New York City
- **Washington, DC**

New York City

In New York City, vital communications links were damaged or overwhelmed by demand. The damage included the loss of electrical power, and the destruction of landline communications facilities and radio towers.

Backup Power

New York City Transit's (NYC Transit) response to the Con Edison Washington Heights blackout in the summer of 1999 had confirmed the value of emergency power generators. Since that time the agency had been purchasing a fleet of trailer-mounted diesel generators.

On September 11, these trailers were dispatched to Lower Manhattan and were used to provide power to pump out the underground subway stations and tunnels, as well as the telephone and utility vaults located near the World Trade Center. The Mayor's Office of Emergency Management (OEM), the New York Police Department (NYPD), and the New York Fire Department (FDNY) also relied on these emergency generators to maintain emergency communications services in Lower Manhattan.

Redundancy

Both NYC Transit and the Port Authority of New York and New Jersey (Port Authority) maintain separate landline telecommunications systems independent of the commercial phone company. On September 11, the Port Authority's system was destroyed, but NYC Transit's system remained functional and was used by the emergency response agencies to maintain communications.

Both NYC Transit and NJ Transit had "mobile" communication centers (40-foot transit buses equipped with satellite communication and computer technology), which were used as command posts for communications and decision-making. NYC Transit also monitored some of its subway stations from its mobile command post using CCTV. Both agencies provided and maintained vital communications links and services for transit as well as federal, state and city emergency command posts through their mobile communications units.

Communication with the Public

Aware of the need to keep the public informed of their transportation options, NYC Transit took the key step of informing both the media and the riding public about constant service changes the first two weeks after September 11.

During the first three days of the disaster, NYC Transit made over 40 changes to subway service; these changes were announced using service notices (Take Ones) and maps handed out by transit employees. Information was also disseminated on the transit agencies' respective web sites. The Metropolitan Transportation Authority (MTA) reported 10 million web hits on its web site on one day after the September 11 attack, five times the normal volume.

Other Findings

Several agencies found that certain communications alternatives proved successful in the emergency response efforts for, particularly for internal information dissemination. Agencies reported that interactive pagers, such as the Blackberry pager, were extremely useful on September 11, when other forms of communication were unavailable.

The NYPD maintains the largest public safety mobile radio system in North America and it remained operational at all times. Nonetheless, it also experienced problems: available channels were extremely crowded, and there were interoperability problems when responders using incompatible radio equipment (operated in different bands) were unable to talk to one another.

At the FCC's Public Safety National Coordination Committee's General Meeting in November of 2001, the NYPD highlighted the fact that because they operate a substantial portion of their own communications infrastructure, they were able to keep E-911 call-taking and dispatching operating. This was an important point to make, because some public safety organizations have been urged to use commercial services to provide their public safety communications. The NYPD felt that September 11 highlighted the critical need for exclusive public safety communications systems that ensure secure quality transmission and reception.

The FDNY learned hard lessons about its audio communications abilities. Their mobile radio system temporarily lost the ability to transmit after the first tower collapsed. The incompatibility of their mobile communications system with that of the Police Department also prevented the agencies from communicating directly with each other. The critical issue of interoperability is being addressed by changing over from VHF to UHF, which will give the FDNY the ability to communicate within its own agency as well as with the NYPD and the Emergency Medical Services (EMS).

Washington, D.C.

In Washington, D.C., The Washington Metropolitan Area Transit Authority (WMATA) operates Metrorail rapid transit lines and an extensive Metrobus transit service throughout the region. Metrorail and Metrobus maintain separate command centers, but in major emergencies, their functions are consolidated into a single, central command post. On September 11, Metrobus drivers could not be notified of all service changes at once since the radio system required that dispatchers call drivers individually.

Telephones were the main communications technology used on September 11 at Washington, D.C.'s command center. But when circuits jammed on the East Coast, the center switched to mobile devices and global satellite phones, instant messaging, and e-mail.

Command Center

Even before the attack on the Pentagon, WMATA had set up a special command center following the attacks in New York, which monitored operations and remained open for much of the day. The command kept in close contact with the FBI, fire departments, and other law enforcement agencies in the region. The center heightened system surveillance, alerted tactical police, and sent sniffing dogs to find suspected explosives at stations, noting that WMATA received tips of suspicious packages seen in the system.

Emergency Preparedness

WMATA considers itself to be well prepared to deal with emergencies because of training, drills, and spot checks. Emergency preparedness is an important priority at WMATA because Washington is a prime target for terrorist attacks; the agency assumes that additional attacks on the nation's capital are inevitable.

August 14, 2003 Blackout

The August 2003 blackout caused a large portion of the Northeast and Great Lakes region to lose electrical power just as the evening rush hour was commencing (see Figure G-1). A major obstacle facing transit agencies and other government agencies in dealing with the blackout was the loss of communications. Activities such as vehicle evacuations had to be conducted without effective central coordination from the OCC. A NYC Transit dispatcher was quoted as saying in the transit agency's newsletter, "For transportation, I think the blackout was worse than 9/11. And the reason is, no communication." Communication problems included technology failures, as well challenges with disseminating timely information within an agency, among agencies, and to the general public.

Technology Failures

When designing a communications system to function during an emergency, it is crucial that the system be designed to eliminate single points of failure. Several transit agencies lost their radio communications because of a failure in at least one portion of its network. One agency's backup power did not work, resulting in inoperable radio communications; another agency had its antennas fail due to a loss of power. Repeaters failed to work on emergency backup or ceased operations after the battery power ran out. The NYPD's radio system experienced brief outages during the initial hours of the event.

Kathy Willens / AP

Figure G-1. Subway evacuation during the 2003 blackout

It is important for a transit agency to understand which segments of its communications system depend on external systems and resources.

New York City's 911 emergency telephone system experienced failures because of the loss of power at the phone company's switching stations. It also experienced the highest demand in its history on August 14, and the phone company's queuing capacity was not sufficient to handle the call volume. NYC Transit's paratransit operations were able to maintain power throughout the blackout, but some of its contracted vendors lost power. As a result, the vendors lost communications with the central operations center and had to resort to manually picking up trip manifests from the central offices.

Most agencies were not prepared for such a long loss of power as the one that occurred during the August blackout. Most backup batteries installed on the towers and repeaters were designed to work for approximately four to six hours. Cell phones and Nextel direct connect radios eventually lost power after several hours when their batteries died. Communications capabilities degraded as their reserve power supplies were exhausted.

Many problems faced during the blackout were not the same as past events. The Port Authority had implemented redundant means of communications, relying especially on text messaging technology, including e-mails and Blackberries, which are personal assistants with access to e-mail, phone, and web information. After its Operations Center lost power, the Port Authority's Internet system went down and text messaging was severely constrained.

Technology Changes

There were several examples of technological changes implemented as a result of lessons learned from September 11 that helped agencies better respond to the blackout. For example, NJ Transit established a dedicated 1-800 telephone number for key staff to be able to communicate the details of the agency's response plan.

References

A Guide to the Project Management Body of Knowledge (ANSI:/PMI 99-001-2000), Project Management Institute, p.38.

American Public Transportation Association. 2004. *Survey of United States Transit System Security Needs and Funding Priorities, Summary of Findings.* [Online]. Available: **http://www.apta.com/services/security/security_survey.cfm**. [2004, October 25].

Americans with Disabilities Act of 1990. Department of Justice. [Online]. Available: **http://www.usdoj.gov/crt/ada/pubs/ada.txt**. [2004, October 25].

Arunski, Karl, Brown, Phil, Buede, Dennis, et al. 1999. *Systems Engineering Overview.* Adapted from the presentation given to the Texas State Board of Professional Engineering. [Online]. Available: **www.incose.org/ntexas/meetings/0004what_is_se.ppt** [2004, October 25].

Balog, J.N. Bromley, Strongin, J.B., et al. *K9 Units in Public Transportation: A Guide for Decision Makers.* TRB TCRP Report 86: Public Transportation Security. Transportation Research Board National Research Council Volume 2: 2002. Available online: **http://trb.org/publications/tcrp/tcrp_rpt_86-v2.pdf**.

Balog, N. John, Boyd, Annabelle, Caton, James E. 2003. *The Public Transportation System Security and Emergency Preparedness Planning Guide.* [Online] Available: **http://transit-safety.volpe.dot.gov/Publications/security/PlanningGuide.pdf**. [2004, October 25].

Comparisons of American, British, French and German Standards for Flame, Smoke and Toxicity of Elastomeric Materials, Rick Hopf, Carol Stream, Emily Witthaus.

Cook, Stephen C. 2000. *What the Lessons Learned from Large, Complex, Technical Projects Tell Us about the Art of Systems Engineering.* [Online] Available: **http://www.unisa.edu.au/seec/pubs/00papers/cook-lessons.pdf**. [2004, October 25].

Cunningham, William C., Taylor, Todd H. June 1985. *The Hallcrest Report I: Private Security and Police In America.* National Institute of Justice.

Department of Defense. July 1999. *DOD Ammunition and Explosives Safety Standards.* DOD 6055.9-STD. [Online]. Available: **http://www.dtic.mil/whs/directives/corres/pdf/d60559_072996/d60559p.pdf** [2004, October 25].

Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health. May 2002. *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks.*

Department of the Army. *Engineer Operations Short of War.* FM 5-114. July 13, 1999. [Online]. Available: **http://globalsecurity.org/military/library/policy/army/fm/5-114/**. [2004, October 25].

Department of Transportation Strategic Plan 2003 – 2008: Safer, Simpler, Smarter Transportation Solutions. September 2003. [Online]. Available: **http://www.dot.gov/stratplan2008/strategic_plan.htm#_Toc52257030**. [2004, October 25].

Federal Emergency Management Agency. *FEMA 426 – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. [Online]. Available: **http://www.fema.gov/fima/rmsp426.shtm**. [2004, October 25].

Federal Emergency Management Agency. *FEMA 427 – Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*. [Online]. Available: **http://www.fema.gov/fima/rmsp427.shtm**. [2004, October 25]

Federal Highway Administration. *Freeway Management and Operations Handbook*. [Online]. Available: **http://ops.fhwa.dot.gov/Travel/traffic/freeway_management.htm**. [2004, October 25].

Federal Transit Administration. *Advanced Public Transportation Systems: The State of the Art Update 2000*. 2000. [Online] Available: **http://www.itsdocs.fhwa.dot.gov//JPODOCS/REPTS_TE//13583.pdf**. [2004, October 25].

Federal Transit Administration. *Public Transportation System Security and Emergency Preparedness Planning Guide (2003)*. [Online]. Available: **http://transit-safety.volpe.dot.gov/Publications/security/PlanningGuide.pdf**. [2004, October 25].

Federal Transit Administration. *Transit Threat Level Response Recommendation*. [Online]. Available: **http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/ThreatLevel/default.asp**. [2004, October 25].

Fire Safety Analysis for Rolling Stock, Mark A. Davis; Material *Toxicity Test Issues in Rolling Stock Procurements*, Mark Davis, Balaji Krishnamurthy, Peter Katsumata.

General Services Administration, Information Technology Service. 1996. *Telecommunications: Glossary of Telecommunications Terms*. [Online] Available: **http://www.its.bldrdoc.gov/fs-1037/**. [2004, October 25].

Institute of Electrical and Electronics Engineers IEEE P1362. *IEEE Guide for Concept of Operations Documents*, Draft 3.1. New York, NY. January 4, 1998.

Institute of Electrical and Electronics Engineers. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York, NY: 1990.

Jenkins M. Brian. December 1997. Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks. [Online] Available: **http://transweb.sjsu.edu/publications/terrorism/Protect.htm**. [2004, October 25].

Lawrence Livermore National Laboratory (LLNL). *Evaluation of an Expedient Terrorist Vehicle Barrier*. [Online]. Available: **http://www-eng.llnl.gov/tsd/movies/barrierfnlrpt.pdf**

Lewis, A. James. 2002. *Security and Surveillance*. Center for Strategic and International Studies. [Online]. Available: http://inet2002.org/CD-ROM/lu65rw2n/papers/g10-b.pdf. [2004, October 25].

Montgomery and Ward. 1993. Facility Damage and Personnel Injury from Explosive Blast.

National Institute for Occupational Safety and Health (NIOSH). Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks. (May 2002). [Online]. Available: http://www.cdc.gov/niosh/bldvent/2002-139.html. [2004, October 25].

National Institute of Standards and Technology. *Government Smart Card Interoperability Specification. Version 2.1*. [Online]. Available: http://csrc.nist.gov/publications/nistir/nistir-6887.pdf. [2004, October 25].

National ITS Architecture 5.0. U.S. Department of Transportation. [Online]. Available: http://itsarch.iteris.com/itsarch/html/user/usr24.htm. [2004, October 25].

National Nuclear Security Administration, Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT). [Online]. Available: http://transit-safety.volpe.dot.gov/security/pdf/protect_factsheet.pdf. [2004, October 25].

National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D. C.: The National Academies Press, 2002.

Public Transportation Security Volume 1: Communication of Threats: A Guide. TCRP Report 86 (2002); Public Transportation Security Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers. TCRP Report 86 (2002).

Rittenhouse, Todd. 1995. *Designing Terrorist-Resistant Buildings*. [Online] Available: http://www.wai.com/AppliedScience/Blast/blast-fireeng.html. [2004, October 25].

Federal Transit Administration. *Subway Environmental Design Handbook*.

Testimony Before the National Commission on Terrorist Attacks Upon the United States. (2003). *Transportation Security: Post-September 11th Initiatives and Long-Term Challenges*. Report No. GAO-03-616T [Online] Available: http://www.gao.gov/new.items/d03616t.pdf. [2004, October 25].

The Illuminating Engineering Society of North America. IESNA, The Lighting Authority. [Homepage of IESNA], [Online]. Available: https://www.iesna.org/shop/. [2004, October 25].

Transit Security Handbook. 1998. Report No. FTA-MA-90-9007-98-1. Washington, DC: U.S. Department of Transportation, Federal Transit Administration.

Transportation Research Board. Public Transportation Security, Volume 4: Intrusion Detection for Public Transportation Facilities Handbook [Online]. Available: http://trb.org/publications/tcrp/tcrp_rpt_86v4.pdf. [2004, October 25].

Transportation Security Administration. TSA TWIC Program. [Online]. Available: http://www.tsa.gov/public/display?theme=68. [2004, October 25].

UFC 4-101-01, Department of Defense, *Minimum Antiterrorism Standards for Buildings*, (31 July 2002).

United States of America Department of Transportation, Federal Transit Administration. *Master Agreement*. [Online] Available: **http://www.fta.dot.gov/library/legal/agreements/2004/ma.html**. [2004, October 25].

WG8. ISO/IEC 14443, Proximity Cards (PICCs). [Online]. Available: **http://www.wg8.de/sd1.html#14443**. [2004, October 25].

WG8. ISO/IEC 15693, Vicinity Cards (VICCs). [Online]. Available: **http://www.wg8.de/sd1.html#15693**. [2004, October 25].

White, C.S., The Scope of Blast and Shock Biology and Problem Areas in Relating Physical and Biological Parameters. *Annals of the New York Academy of Sciences, 1968*. 152: p. 89-102.

Acronyms

ADA	Americans with Disabilities Act
ANSI	American National Standards Institute
APTA	American Public Transportation Association
AORA	Areas of Response Assistance
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ASTM	American Society for Testing and Materials International
AVL	Automatic Vehicle Locator
BRT	Bus Rapid Transit
CapWIN	Capital Wireless Integrated Network
CBNR	Chemical, Biological, Nuclear, Radiological
CBR	Chemical, Biological, Radiological
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control
CDPD	Cellular Digital Packet Data
CFR	Code of Federal Regulations
CNG	Compressed Natural Gas
ConOps	Concept of Operations
COTS	Commercial Off The Shelf
CPTED	Crime Prevention Through Environmental Design
DCS	Distributed Control Systems
DHHS	Department of Health and Human Services
DOD	Department of Defense
DOS	Department of State
EMI	Electro-Magnetic Interference
FAH	Foreign Affairs Handbook
FCRA	Federal Fair Credit Reporting Act

FTA	Federal Transit Administration
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information Systems
GPA	Grade Point Average
GPS	Global Positioning System
GSA	General Services Administration
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESNA	Illuminating Engineering Society of North America
IETF	Internet Engineering Task Force
IIMS	Integrated Incident Management System
INS	Immigration and Naturalization Service
ISP	Internet Service Provider
ISO	International Organization for Standardization
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
MDT	Mobile Data Terminals
MVR	Motor Vehicle Record
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Agency
NIOSH	National Institute of Occupational Safety and Health
NRC	National Research Council
NTCIP	National Transportation Communications for ITS Protocol
NTI	National Transit Institute
NYCTA	New York City Transit Authority
NYCT	New York City Transit

OCC	Operations Control Center
OEM	Office of Emergency Management (New York Mayor's Office)
OTS	Off-the-Shelf
PA	Public Address
PD	Probability of Detection
PDA	Personal Digital Assistant
PIDS	Perimeter Intrusion Detection System
PIN	Personnel Identification Number
PROTECT	Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism
PSI	Pounds per Square Inch
RF	Radio Frequency
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Development Organization
TCIP	Transit Communications Interface Protocols
TCRP	Transit Cooperative Research Program
TNT	Trinitrotoluene
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSWG	Technical Support Working Group
TV	Television
TVA	Threat and Vulnerability Assessment
TWIC	Transportation Worker Identification Credential
UHF	Ultra High Frequency
US	United States
VHF	Very High Frequency
VMS	Variable Message Sign
WiFi	Wireless Fidelity

WPS	Wireless Priority System
WMD	Weapons of Mass Destruction

Working Group Members

Transit Security Working Group

Susannah Kerr Adler, Parsons Brinckerhoff

David Capozzi, The Access Board

Agapito Diaz, ACS, Inc

Dorothy Dugger, Bay Area Rapid Transit (San Francisco)

Jose Fernandez, Long Island Rail Road

Greg Hull, American Public Transit Association

Chris Kozub, National Transit Institute

Jim McLaughlin, Los Angeles County Metropolitan Transit Authority

Paul Messina, New York City Metropolitan Transit Authority

Roger Mowrey, Southern California Regional Rail Authority

William Neilson, City of San Francisco

Stephan Parker, Transportation Research Board

Chris Zeilinger, Community Transportation Association of America

Systems Integration Working Group

Karen Antion, Antion Consulting

Rob Ayers, ARINC Consulting

Maureen Bertocci, Port Authority (Allegheny County)

Robin Cody, Bay Area Rapid Transit (San Francisco)

Greg Cook, Ann Arbor Transit

Len Diamond, New Jersey Transit

John Fayos, Critical Link

Greg Hull, American Public Transit Association

Joe Kinchen, Alameda-Contra Costa Transit

Paul Larrousse, National Transit Institute

Jerry Lutin, New Jersey Transit

Rick Schonbachler, Orbital TMS

Issac Takyi, New York City Metropolitan Transit Authority

Credentialing Working Group

Sherry Anderson, Transportation Security Administration

Diane Bates, AMTRAK

Paul Christian, Transportation Resources Associates, Inc.

Susan Chiaroni, Golden Gate Transit

Bill Fleming, Massachusetts Bay Transportation Authority

Gary Gee, Bay Area Rapid Transit (San Francisco)

William T. Gibson, Bay Area Rapid Transit (San Francisco)

Richard Hibbs, Golden Gate Transit

Jim Hill, Transportation Resource Associates, Inc.

Greg Hull, American Public Transit Association

Paul Hunter, Transportation Security Administration

Jim Lair, Golden Gate Transit

Kevin McConvile, New York City Metropolitan Transit Authority

Chris McKay, Transportation Security Administration

Jim O'Donnell, New York City Metropolitan Transit Authority

Stephan A. Parker, Transportation Research Board

Robert Phillips, Transportation Security Administration

John Seltzer, Barton Transportation Services

Rick Schonbachler, Orbital TMS

Jim Sharp, Transportation Security Administration

Gene Walker, Golden Gate Transit

Chris Zeilinger, Community Transportation Association of America

Access Management Working Group

Sherry Anderson, Transportation Security Administration

Diane Bates, AMTRAK

Ron Bollhoffer, Milwaukee County Transit System

Bernard L. Buckner, Greater Cleveland Regional Transit Authority

Mike Burress, Community Transit Association of America

Susan Chiaroni, Golden Gate Transit

Paul Christian, Transportation Resources Associates, Inc.

Len Diamond, New Jersey Transit

Linda Fice, Toronto Transit Commission

William Fleming, Massachusetts Bay Transit Authority Police Department

Greg Garback, Washington Metropolitan Area Transit Authority

Gary Gee, Bay Area Rapid Transit (San Francisco)

William T. Gibson, Bay Area Rapid Transit (San Francisco)

Robert Emmet Hertan, Municipal Transportation Agency (San Francisco)

Richard Hibbs, Golden Gate Transit

Jim Hill, Transportation Resource Associates, Inc.

Greg Hull, American Public Transit Association

Paul Hunter, Transportation Security Administration

Frank Jennings, Dallas Area Rapid Transit

John Joyce, Greater Cleveland Regional Transit Authority

Jim Lair, Golden Gate Transit

Clark Lynch, Bay Area Rapid Transit (San Francisco)

Chris McKay, Transportation Security Administration

John P. O'Grady, Toronto Transit Commission

Laura Ray, Metro Atlanta Rapid Transit Authority

Stephan A. Parker, Transportation Research Board

Robert Phillips, Transportation Security Administration

John Seltzer, Barton Transportation Services

Jim Sharp, Transportation Security Administration

Gene Walker, Golden Gate Transit

Rick Schonbachler, Orbital TMS

Surface Infrastructure Working Group

Bernard Buckner, Greater Cleveland Transit

Victor Burke, Dallas Area Transportation Authority

Greg Hull, American Public Transit Association

Frank Jennings, Dallas Area Transportation Authority

John Joyce, Greater Cleveland Transit

John O'Grady, Toronto Transit Commission

Stephan A. Parker, Transportation Research Board

Laura Ray, Metro Atlanta Rapid Transit Authority

John Sepulis, Toronto Transit Commission

Susan Reed Tanaka, Toronto Transit Commission

Mike Wehr, Milwaukee County Transit System

Chris Zeilinger, Community Transportation Association of America

Tunnel Infrastructure Working Group

Dan Hall, Washington Metropolitan Area Transit Authority

Robert Emmett Hertan, Municipal Transportation Agency (San Francisco)

Greg Hull, American Public Transit Association

Harold Levitt, Port Authority Trans-Hudson

Clark Lynch, Bay Area Rapid Transit District (San Francisco)

William Morange, Metropolitan Transit Authority (Loas Angeles)

Stephan A. Parker, Transportation Research Board

Chris Zeilinger, Community Transportation Association of America

Bus Vehicle Working Group

Mark Brager, Orion Buses

Frank Jennings, Dallas Area Rapid Transit

Greg Hull, American Public Transit Association

Joyce Olson, Community Transit Association of America

Stephan A. Parker, Transportation Research Board

Allen Pierce, Orange County Transportation Authority

Paul Smith, New Flyer

Lurae Stuart, American Public Transit Association

Bonnie Todd, Miami Dade Transit

Phil Wallace, Washington Metropolitan Area Transit Authority

John Walsh, New York City Metropolitan Transit Authority

Chris Zeilinger, Community Transportation Association of America

Rail Vehicle Working Group

Michael Chinn, Municipal Transportation Agency (San Francisco)

Chester "Ed" Colby, Washington Infrastructure Services

Ray Friem, St. Louis Metro

Jean François Matte, Baultar Composite Inc.

Greg Hull, American Public Transit Association

Nigel Jones, Alstom

Charles Joseph, Sound Transit (Seattle)

Peter Katsumata, Booz Allen Hamilton

Paul Messina, New York City Metropolitan Transit Authority

Stephan A. Parker, Transportation Research Board

Jim Price, Utah Transit Authority

Dave Phelps, American Public Transit Association

Navin Sagar, Washington Group International, Inc

Sid Sparks, Siemens

Cesar Vergara, Jacobs Engineering Group, Inc.

Emily Witthaus, Rogers Corporation

Len Woolgar, Baultar Composite Inc.

Communications Working Group

Len Diamond, New Jersey Transit

Dorothy Dugger, Bay Area Rapid Transit (San Francisco)

Jose Fernandez, Long Island Rail Road

David Goodman, Maryland Transit Administration

Lt. Brian Heanue, Washington Metropolitan Area Transit Authority

Greg Hull, American Public Transit Association

Paul Lennon, Metropolitan Transit Authority (Los Angeles)

Steve McLaird, Metro Transit (Minneapolis)

Dave Martin, Department of Homeland Security

Stephan A. Parker, Transportation Research Board

Chief Gene Wilson, Metro Atlanta Rapid Transit Authority

Industry Review Working Group

Terry Andrews, Chief Constable, Toronto Transit Commission

Jeff Arndt, Vice President/ Chief Operating Officer, Metropolitan Transit Authority of Harris County

Cameron Beach, Chief Operating Officer, Sacramento Regional Transit

Robert Hertan, Director of Security Programs/ Chief of Transit Police, San Francisco Municipal Transportation Agency

Rich Hanratty, Chief Officer, Rail Transportation, SEPTA

Greg Hull, Director-Operations, Safety & Security Programs, American Public Transportation Association

Paul Lennon, Managing Director-Intelligence & Counter Terrorism, Los Angeles County Metropolitan Transportation Authority

William Mooney, Vice President of Bus Operations, Chicago Transit Authority

Gene Wilson, Chief of Police, MARTA

Paul Harvey, MARTA

Chris Zeilinger, Asst Director, Governmental Affairs & Training, Community Transportation Association of America (CTAA)