

Transit Security Handbook

Prepared for the:

Volpe National Transportation Systems Center

March 2, 1998

Submitted by



402 Greenwood Farms Road
Barboursville, VA 22923
(804) 985-1033

Table of Contents

1. INTRODUCTION.....	1
1.1 Purpose of Security Handbook.....	1
2. SECURITY AND FTA S STATE SAFETY OVERSIGHT RULE	3
2.1 Phase I: Establishing the Oversight Agency and Oversight Capability	4
2.1.1 The Oversight Agency	5
2.1.2 The Rail Fixed Guideway System.....	6
2.2 Phase II: Integrating Security into the Oversight Program	6
2.2.1 Including Passenger and Employee Security in the Program Standard	7
2.2.2 Require, Review and Approve, and Monitor Security Plan Implementation.....	9
2.2.3 Integrating Security into the Three-year Safety Review	9
2.2.4 Integrating Security into the Internal Safety Reporting Requirements	10
2.2.5 Integrating Security into FTA Certification and Annual Report.....	10
3. SYSTEM SECURITY APPROACH.....	12
3.1 The Provision of RFGS Security.....	13
3.2 System Security Program Plan Implementation.....	16
3.2.1 Crime Levels and Patron Perceptions	17
3.2.2 Environmental Design Solutions.....	17
3.2.3 Technology Solutions.....	18
3.2.4 Personnel Deployment Solutions	18
3.2.5 Terrorism Prevention Activities	18
3.2.6 Data Collection.....	19
4. THE SYSTEM SECURITY PLAN	20
5. CRIME LEVELS AND PATRON PERCEPTIONS.....	24
5.1 Crime Levels	24
5.1.1 Types and Occurrences of Rail Fixed Guideway System Crime	25
5.1.2 Types and Occurrences of Motor Bus Crime.....	33
5.1.3 Comparison of Motor Bus and RFGS Crime	43
5.2 Patron Perceptions.....	45
6. SECURITY BY DESIGN	46
6.1 Foundation of Environmental Crime Prevention	46
6.2 Principles of Crime.....	47
6.2.1 Participant Principle	48
6.2.2 Behavior Settings Principle.....	48
6.2.3 Flow Principle	48
6.3 Crime Prevention Through Environmental Design and Situation Crime Prevention	49

6.4	Using CPTED and Situation Crime Prevention to Reduce Crime	51
6.4.1	Increasing Perceived Effort	51
6.4.2	Increasing Perceived Risks.....	53
6.4.3	Reducing Anticipated Rewards	54
6.4.4	Inducing Guilt or Shame	55
6.5	Implementation Periods of Situational Crime Prevention.....	57
7.	SECURITY TECHNOLOGY IN THE TRANSIT ENVIRONMENT	62
7.1	Access Control Systems	63
7.1.1	Electronic Access Control Systems.....	63
7.1.2	Intrusion Detection Systems	67
7.1.3	Motion Detectors.....	68
7.1.4	Other Systems to Control Access.....	68
7.2	Closed Circuit Television Surveillance Systems	70
7.2.1	CCTV Utilization	70
7.2.2	Cameras and Networks.....	73
7.2.3	Housings and Accessories	75
7.3	Emergency Communications Systems	76
7.4	Security Materials Technology	78
8.	RAIL FIXED GUIDEWAY SYSTEM SECURITY PERSONNEL DEPLOYMENT	83
8.1	Deployment to Reduce Passenger Fear.....	84
8.2	Proactive Deployment	85
8.3	Determining Tactics	89
9.	RAIL FIXED GUIDEWAY SYSTEM TERRORISM PREPAREDNESS	90
9.1	Definition of Terrorism and Background Information.....	90
9.2	Mitigation and Preparation for Rail Fixed Guideway System Terrorism	92
9.2.1	Key Planning Prerequisites	92
9.2.2	Beginning the Planning Process.....	94
9.2.3	Resolving Identified Risks and Threats	96
9.2.4	Integrating Terrorism Response	97
9.2.5	Incident Command System Management Concepts.....	99
9.3	Responding to Transit Terrorism	100
9.3.1	Responsibilities for Incident Management.....	102
9.3.2	First Responder Considerations	102
9.3.3	Developing an Incident Action Plan	103
9.3.4	Reconciling Crisis and Consequence Management	103
9.3.5	Federal Emergency Management Agency Emergency Support Functions.....	105
9.4	Recovery.....	105
10.	DATA COLLECTION	106
10.1	Dispatch Logs.....	109
10.2	Rail Fixed Guideway System Operator Reports	110
10.3	Incident Report Forms.....	110

List of Figures

Figure 1: Integration of State Safety Oversight into RFGS Security Activities	16
Figure 2: Rail Fixed Guideway System Crimes by Type, 1996.....	26
Figure 3: Rail Fixed Guideway System Crimes per 10 Million Passenger Trips by System Size, 1996.....	26
Figure 4: Rail Fixed Guideway System Quality of Life Crimes, 1996.....	27
Figure 5: Rail Fixed Guideway System Quality of Life Crimes by Location, 1996.....	28
Figure 6: Rail Fixed Guideway System Quality of Life Crimes by System Type (Per 10 Million Passenger Trips)	28
Figure 7: Rail Fixed Guideway System Property Crimes, 1996.....	29
Figure 8: Rail Fixed Guideway System Property Crimes by System Type (Per 10 Million Passenger Trips).....	30
Figure 9: Rail Fixed Guideway System Property Crimes by Location, 1996.....	30
Figure 10: Rail Fixed Guideway System Violent Crimes, 1996.....	31
Figure 11: Rail Fixed Guideway System Violent Crimes by System Type (Per 10 Million Passenger Trips)	32
Figure 12: Rail Fixed Guideway System Violent Crimes by Location, 1996.....	32
Figure 13: Motor Bus Crimes by Type, 1996	36
Figure 14: Motor Bus Crimes per 10 Million Passenger Trips by System Size, 1996	36
Figure 15: Motor Bus Quality of Life Crimes, 1996	37
Figure 16: Motor Bus Quality of Life Crimes by System Size (Per 10 Million Passenger Trips).....	38
Figure 17: Motor Bus Quality of Life Crimes by Location, 1996	38
Figure 18: Motor Bus Property Crimes, 1996.....	39
Figure 19: Motor Bus Property Crimes by System Size (Per 10 Million Passenger Trips).....	40
Figure 20: Motor Bus Property Crimes by Location, 1996.....	40
Figure 21: Motor Bus Violent Crimes, 1996	41
Figure 22: Motor Bus Violent Crimes by System Size (Per 10 Million Passenger Trips)	42
Figure 23: Motor Bus Violent Crimes by Location, 1996	42
Figure 24: Rail and Motor Bus Quality of Life Crimes per Ten Million Passenger Trips, 1996 ..	43
Figure 25: Rail and Motor Bus Property Crimes per Ten Million Passenger Trips, 1996	44
Figure 26: Rail and Motor Bus Violent Crimes per Ten Million Passenger Trips, 1996	44

List of Tables

Table 1: State Safety Oversight Implementation Phases	4
Table 2: Phase II Security Oversight Activities.....	7
Table 3: CPUC Security Component of Program Standard.....	7
Table 4: PTSB Security Program Standard.....	8
Table 5: Safety and Security Review Checklist Categories.....	11
Table 6: Partial Listing of Security Organizations Used at Affected RFGS.....	13
Table 7: Bus and Rail Passenger Trips on SSO-Affected Systems, 1996.....	15
Table 8: Violent Crimes in Municipalities and Rail Fixed Guideway Systems, 1995.....	34
Table 9: Situational Crime Prevention.....	51
Table 10: Security by Design.....	58
Table 11: New York City’s Port Authority Bus Terminal Renovations.....	60
Table 12: Changes by NYCT to Reduce Fare Evasion.....	61
Table 13: Bay Area Rapid Transit Access Control System	66
Table 14: Amtrak Access Control System	66
Table 15: Intrusion Detection Systems	67
Table 16: MARTA Closed Circuit Television System	73
Table 17: BART Closed Circuit Television System	74
Table 18: Emergency Communication System Technologies	77
Table 19: Materials Selections and Physical Features in the Transit Environment.....	80

1. Introduction

The prominence of rail transit and the large number of passengers who rely on this service ensure that *security* is a fundamental responsibility. To promote improved security capabilities at the nation's rail agencies, the Federal Transit Administration (FTA) has incorporated security as part of its State Safety Oversight Rule. This Rule covers thirty-two rail transit systems operated in nineteen states and the District of Columbia.

The FTA's State Safety Oversight Rule was prepared in response to section 3029 of the Intermodal Surface Transportation Efficiency Act (ISTEA), which directed FTA to issue regulations requiring that states oversee the safety and security of Rail Fixed Guideway Systems (RFGS). The enactment of Section 3029 reflected the growing concerns of Congress regarding the potential for catastrophic accidents and security incidents on rail transit systems; it was subsequently codified into the Federal Transit Act at 49 U.S.C. section 5330.

In response to section 5330, FTA issued a Final Rule on December 27, 1995 entitled "Rail Fixed Guideway Systems; State Safety Oversight." The Final Rule is codified at 49 CFR Part 659, and is referred to as the State Safety Oversight Rule or Part 659.

Provisions for passenger and employee security are included in FTA's State Safety Oversight Rule in recognition of the fact that safety and security risks are interrelated for rail transit passengers and employees. Part 659 has been designed to reduce all incidents that harm passengers and employees, whether these incidents are the result of unintentional occurrences (safety) or intentional acts (security).

1.1 Purpose of Security Handbook

To support on-going implementation of State Safety Oversight security requirements, FTA has prepared the *Transit Security Handbook*. This Handbook explains the security provisions specified in Part 659 and provides a comprehensive description of the *system security process*.

The Handbook provides both Oversight Agency and RFGS personnel with an overview of the rail security function, including:

- The development of a State Security Oversight Program,
- The establishment of a rail transit police or security department,
- The development of a System Security Program Plan (Security Plan),
- The deployment of uniformed and plainclothes police and security personnel,
- Crime Prevention through Environmental Design (CPTED) and Situation Crime Prevention (SCP) techniques for rail facility design and operation,

- The use and management of security technology, and
- Techniques for crime data collection and analysis.

Finally, this Handbook contains information that will support the efforts of rail transit agencies to comply with the requirements specified in Part 659.

2. Security and FTA's State Safety Oversight Rule

The State Safety Oversight Rule presents FTA's requirements for the first state-managed RFGS safety and security oversight program. Applying a collaborative and cooperative approach to oversight, Part 659 is intended to establish a partnership between:

- State Oversight Agencies, who must monitor and review RFGS system safety and security programs;
- RFGS, whose primary responsibility is to provide safety and security for rail passengers and employees; and
- FTA, whose principal role is to monitor the implementation of the State Safety Oversight Rule.

In FTA's State Safety Oversight Rule, safety requirements are specified in detail, while security requirements are referred to only in general terms. Specific security requirements are not issued in Part 659 because security is interpreted as part of the Oversight Agency's safety oversight program; thus, the tools developed to support RFGS safety oversight should also be used to support security oversight.

To provide for the gradual incorporation of security into each State's Oversight Program, FTA established a two-phase implementation schedule. During **Phase I**, the designated Oversight Agency must establish the capability to perform the seven key oversight functions specified in Part 659. **Phase II** requires the integration of security into these oversight functions.

As indicated in Table 1, Part 659 required **Phase I** activities to be completed by January 1, 1997. **Phase II** activities must be in place by January 1, 1998.

Part 659 Implementation Phases	Implementation Schedule
<p>Phase I: Safety Oversight</p>	<p>By January 1, 1997, the Oversight Agency must review and approve in writing the safety component of the System Safety Program Plan (SSPP) for each RFGS located within its jurisdiction. Further, by January 1, 1997, the Oversight Agency must make its Initial Submission to FTA. This Submission includes all procedures and practices that support the oversight capability of the Agency:</p> <ul style="list-style-type: none"> • The Program Standard • Review/approval process for the RFGS SSPP • Accident investigation, reporting, and notification procedures • Corrective Action Plan procedures
<p>Phase II: Integrating Security</p>	<p>By January 1, 1998, the Oversight Agency must review and approve in writing the security component of the SSPP for each RFGS located within its jurisdiction.</p>

Table 1: State Safety Oversight Implementation Phases

2.1 Phase I: Establishing the Oversight Agency and Oversight Capability

This section presents, in summary form, the requirements for **Phase I** of Part 659, including the following:

- The authorities and responsibilities of the *Oversight Agency* in developing the requirements and programs necessary to comply with FTA's State Safety Oversight Program, and
- The role of the *RFGS* in complying with the program developed by the Oversight Agency.

2.1.1 The Oversight Agency

During **Phase I**, the designated Oversight Agency is required by Part 659 to perform seven distinct functions. These functions constitute the core of FTA's State Safety Oversight Rule. By January 1, 1997, the Oversight Agency must:

- **Develop a Program Standard.** This written document defines the relationship between the Oversight Agency and the RFGS and guides the RFGS in developing its System Safety Program Plan (SSPP). The Program Standard must, at a minimum, comply with the American Public Transit Association's Manual for the Development of Rail Transit System Safety Program Plans (APTA Manual). [*§659.3*]
- **Require, review and approve, and monitor the implementation of an SSPP that complies with the Oversight Agency's Program Standard at RFGS.** By January 1, 1997, the Oversight Agency must review and approve, in writing, the RFGS SSPP. After the initial approvals, the Oversight Agency must review, as necessary, the RFGS SSPP and determine whether it should be updated. [*§659.33(a),(b),(c)*]
- **Establish procedures for conducting an on-site, formal Safety Review at each RFGS a minimum of every three years.** In a Safety Review, the Oversight Agency must assess whether the RFGS's actual safety practices and procedures comply with its SSPP. Once this Review is completed, the Oversight Agency must prepare a report containing its findings and recommendations, an analysis of the efficacy of the RFGS SSPP, and a determination of whether the SSPP should be updated. [*§659.37*]
- **Require each RFGS to report the occurrence of accidents and unacceptable hazardous conditions within a period of time specified by the Oversight Agency.** The Oversight Agency must investigate such events in accordance with established procedures. The Oversight Agency may conduct its own investigation, use a contractor to conduct an investigation, rely on the investigation conducted by the rail transit system or the National Transportation Safety Board (NTSB), or use a combination of these methods. [*§659.39*], [*§659.39*] and [*§659.41*]
- **Require each RFGS to implement a Corrective Action Plan.** The Oversight Agency must require each RFGS to minimize, control, correct, or eliminate, hazardous conditions identified during investigations, in accordance with a Corrective Action Plan drafted by the RFGS and approved by the Oversight Agency. [*§659.43*]
- **Require the RFGS to conduct safety audits according to the Internal Safety Audit Process detailed in the APTA Manual (Checklist Number 9).** In addition, the Oversight Agency must require the RFGS to compile and submit an Annual Audit Report for review. [*§659.35*]

- **Establish procedures for annual certification and reporting to FTA.** The Oversight Agency must annually certify its compliance with FTA’s State Safety Oversight Program and submit annual reports describing oversight activities. [*§659.45*]

A detailed discussion of each of these requirements can be found in Implementation Guidelines for State Safety Oversight of Rail Fixed Guideway Systems, available from:

Federal Transit Administration
 Office of Safety and Security
 400 Seventh Street, S.W.
 Washington, D.C. 20590
 Phone: (202) 366-0197
 Fax: (202) 366-7951

2.1.2 The Rail Fixed Guideway System

While the requirements in Part 659 are directed at the states and the Oversight Agencies, RFGS play a central role in the State Safety Oversight Program.

To comply with **Phase I** of Part 659, the Oversight Agency must, at a minimum, require each RFGS within its jurisdiction to perform the following activities:

- Develop an SSPP that complies with the Oversight Agency's Program Standard,
- Classify hazardous conditions according to the *APTA Manual Hazard Resolution Matrix*,
- Report, within the time frame specified by the Oversight Agency, any accident or unacceptable hazardous condition,
- Obtain the Oversight Agency's approval of a Corrective Action Plan and then implement the Plan to minimize, control, correct, or eliminate the particular unacceptable hazardous condition,
- Conduct safety audits that comply with the *Internal Safety Audit Process, APTA Manual (Checklist Number 9)*, and
- Draft and submit an annual report summarizing the results of the internal safety audit process.

2.2 Phase II: Integrating Security into the Oversight Program

Phase II activities require the Oversight Agency to integrate “*specific provisions for addressing passenger and employee security*” into the established Safety Oversight Program. During **Phase II**, the procedures and policies established during **Phase I**, should be expanded to include security. Table 2 presents these requirements.

Phase II Security Oversight Activities	
Include passenger and employee security in the Program Standard.	§659.31
Require, review and approve, and monitor the Implementation of a System Security Program Plan (Security Plan) at each rail transit system. The Security Plan can be Part of the SSPP, or it can be a separate document.	§659.33 (a),(b),(c)
Include security in the on-site Three-year Safety Review.	§659.37
Include security in the Internal Safety Reporting requirements.	§659.35
Include security activities in annual reporting to FTA.	§659.45

Table 2: Phase II Security Oversight Activities.

Each of these requirements is addressed in the following sections.

2.2.1 Including Passenger and Employee Security in the Program Standard

Part 659 references FTA’s Transit System Security Program Planning Guide as providing minimum requirements for the security component of the Program Standard. Integrating security into the Program Standard can be a relatively straightforward activity. For example, the California Public Utilities Commission (CPUC) updated its Program Standard to address security using the single paragraph presented in Table 3.

California Public Utilities Commission – Security Component of Program Standard
<p>“The system safety program plan shall address the personal security of the transit agency’s passengers and employees. The Federal Transit Administration’s final report FTA-MA-90-7001-94-1, <u>TRANSIT SYSTEM SECURITY PROGRAM PLANNING GUIDE</u>, January 1994 shall serve as a set of guidelines for preparation of the security portion of each transit agency’s system safety program plan. Procedural details that the transit agency classifies as confidential information to prevent or mitigate security breaches shall not be revealed in the system safety program plans. Each transit agency shall submit the security portion of its system safety program plan to the Commission for approval prior to January 1, 1998, or the date it begins operations, whichever is later.”</p>

Table 3: CPUC Security Component of Program Standard

Some Oversight Agencies may wish to provide additional guidance in specifying the requirements for the Security Plan. For example, as part of its revised Program Standard, the New York Public Transportation Safety Board (PTSB) issued a set of guidelines to direct the development of Security Plans at affected RFGS. (See below.)

New York Public Transportation Safety Board (PTSB) Security Program Standard

"The purpose of this section is to identify the tasks and responsibilities for system security; security's role in the overall operation of the system; the role management plays in enforcing it; and its effectiveness in the overall development of the property's system safety program planning process. Both short and long term goals should be included as well as the means to measure their effectiveness.

This section should be interfaced with those of other operating departments and explain the correlation to one another, especially with regard to safety. This section should discuss the security effects for potential danger considering the acceptance, control, and elimination of such dangers within the confines of the available resources.

Because of the confidentiality required with the security portion, much of the information may remain confidential and references as such, available for PTSB review in the event of a security breach in which the PTSB is solicited as a party to investigate the events.

- 22.1 Identify the purpose of the System Security Program Plan
- 22.2 Identify the goals of the system security plan
- 22.3 Describe the organizational structure and hierarchy of the Security Department (or organizational entity responsible for security) including, but not limited to discussion on such items as resources, service operations, operating environment, facilities and available equipment, existing capabilities and response measures.
- 22.4 Describe the role and authority of the property's security management with the other internal departments and external agencies (i.e., police, fire, ambulance, government agencies, etc.) including the policies and interfaces shared between them
 - 22.4.1 Interface with Safety Department
 - 22.4.2 Interface with Transportation Department
 - 22.4.3 Interface with Engineering Department
 - 22.4.4 Interface with Maintenance Department
 - 22.4.5 Interface with Maintenance of Way Department
 - 22.4.6 Interface with Capital Improvements Department
 - 22.4.7 Interface with Procurement Department
 - 22.4.8 Interface with Passenger Service Department
 - 22.4.9 Interface with other pertinent internal and/or external departments/agencies
- 22.5 Describe the responsibilities of each division of the Security Department
- 22.6 Describe the training, and responsibilities with regard for training, for each Security employee
- 22.7 Incorporate (by reference) the property's policies for threat and vulnerability identification, assessment, and resolution
- 22.8 Describe the update policy for the system security program plan

NOTE: Other additions to the current SSPP on file with the PTSB will be required in those sections in which references to security need to be addressed."

Table 4: PTSB Security Program Standard

2.2.2 Require, Review and Approve, and Monitor Security Plan Implementation at Each Rail Fixed Guideway System

The Oversight Agency must require, review and approve, and monitor the RFGS Security Plan for compliance with the Program Standard. The review and approval process may require considerable coordination with the police and/or security department at each affected RFGS. FTA encourages this coordination, since compliance with the requirements in Part 659 will focus more attention on security and will encourage the adoption of the systems approach to reducing the occurrences of criminal incidents, in the same manner in which this approach is currently applied in the safety field.

The Security Plan is intended to be a dynamic document that is used to manage security activities and assist agencies in achieving their security goals. FTA, therefore, has allowed for a great deal of flexibility in the security requirements for this document; however, as specified in the Transit System Security Program Planning Guide, a typical Security Plan must include, at a minimum, the following components:

- RFGS management commitment and policy regarding security,
- Introduction to the RFGS System Security Program,
- RFGS description
- Management of the Security Plan,
- Description of system security responsibilities,
- System security threat and vulnerability identification and resolution process,
- Security Plan implementation and verification, and
- Security Plan evaluation and modification procedures.

Using procedures established during **Phase I**, the Oversight Agency must approve this revised Plan, in writing, by January 1, 1998.

2.2.3 Integrating Security into the Three-year Safety Review

During **Phase II**, the Oversight Agency should modify its Three-year Safety Review procedures and checklists to ensure that the Security Plan, which is technically part of the RFGS's SSPP, is being evaluated.

The Three-year Safety Review:

- Allows the Oversight Agency to assess the effectiveness of the rail transit agency's SSPP and Security Plan and determines that they are being followed,
- Assesses the RFGS's commitment to ensuring safe and secure operations,
- Assists the Oversight Agency in identifying systemic safety and security issues affecting the public and system employees, and
- Ensures that the Oversight Agency maintains a proactive role in the safety/security process at the RFGS.

For example, the Florida Department of Transportation (FDOT) recently developed a "Safety Review Checklist" (see Table 5) that incorporates both safety and security. This Checklist updates the twenty-three categories in the APTA Manual to address security. FDOT has hired a contractor to develop the specific checklist forms and to conduct the actual Reviews.

2.2.4 Integrating Security into the Internal Safety Reporting Requirements

An essential component of each RFGS's implementation of its Security Plan is on-going performance reporting for all activities. During **Phase I**, each Oversight Agency should have developed safety reporting procedures for each RFGS in its jurisdiction.

For **Phase II**, the Oversight Agency should modify the reporting requirement to include security. For example, both the CPUC and the PTSB require information from the RFGS in their jurisdiction on security activities and performance. FTA recommends that the Oversight Agency allow the RFGS to submit existing security reports, schedules, and findings, prepared for RFGS management, to fulfill this requirement.

2.2.5 Integrating Security into FTA Certification and Annual Report

To integrate security in the Annual FTA Certification and Annual Report, the Oversight Agency should:

- Modify its Certification Form to include security, and
- Include a description of all security oversight activities performed in the Annual Report.

This report can be prepared especially for FTA, or can be an annual report developed by the Oversight Agency to satisfy its management and/or public information requirements.

Florida Department of Transportation (FDOT) – Safety and Security Review Checklist Categories

- Policy statement and authority of System Safety Program Plan (SSPP) and System Security Program Plan (SECURITY PLAN), as applicable,
- Description of purpose for the SSPP and SECURITY PLAN, as applicable,
- Clearly stated goals for requirements of the SSPP and SECURITY PLAN, as applicable,
- Identifiable and attainable objectives,
- System description and organizational structure,
- SSPP and SECURITY PLAN control and update procedures,
- Hazard/security risks identification and resolution process,
- Accidents, unacceptable hazardous conditions, security incidents, and unacceptable risk conditions, reporting, and investigation,
- Internal audit process,
- Facility inspections,
- Maintenance audits and inspections,
- Rules and procedures review,
- Training and certification reviews and audits,
- Emergency response planning, coordination, and training,
- System modification review and approval process,
- Safety/security data acquisition and analysis,
- Interdepartmental and interagency coordination,
- Configuration management,
- Employee safety and security program,
- Hazardous materials program,
- Drug and alcohol abuse programs,
- Contractor safety and security coordination, and
- Procurement.

Table 5: Safety and Security Review Checklist Categories

3. System Security Approach

As required by FTA’s State Safety Oversight Rule, the Oversight Agency’s Program Standard directs each RFGS to apply the *systems approach* to the provision of passenger and employee security. The system security approach is defined as:

“The application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.”¹

System security is a form of risk management that eliminates or controls threats and vulnerabilities through an ongoing threat and vulnerability resolution process. The system security approach identifies, evaluates, and controls security threats and vulnerabilities through all system life cycle phases. Security is addressed in the design, construction, and operation of the transit system. This proactive approach encourages both the design of features which “harden” system elements against criminal activity, and the implementation of security information monitoring systems, which identify and control new threats and vulnerabilities. This approach also identifies designs, technologies, and deployment strategies that assist in reducing patron fear.

A security program utilizing the systems approach offers the functional and integrated capability of protecting users and operators of the system, as well as the resources of the system. The basic elements of protection involve prevention or deterrence of acts or conditions threatening the safety or welfare of those persons or resources, and corrective or remedial action to limit the effects of such acts or conditions when they do occur.

The system security approach relies on threat and vulnerability management. This threat identification and resolution process includes a thorough examination of the role and interrelationship between the four elements of the system:

- Passengers and employees,
- Equipment and facilities,
- Procedures, and
- Environment.

Such an approach will assist in minimizing system threats while providing the highest level of security practical.

¹ John Balog, Anne Schwartz, Bernard Dyle. Transit System Security Program Planning Guide (Washington, D.C.: Federal Transit Administration), 1994, pg. xxix.

The coordination of security operations and emergency response activities with all appropriate local, state, and federal agencies is necessary to the success of the systems approach. This approach will assist each transit system in using limited resources more effectively and improving security performance.

3.1 The Provision of RFGS Security

Security at the thirty-two RFGS affected by Part 659 is provided by organizations with varying degrees of police powers operating under specialized conditions, including the following (see Table 6):

- Dedicated sworn police force with jurisdiction for the entire RFGS,
- Contracted non-sworn security,
- Contracted local law enforcement (off-duty police officers and formal contracts for municipal police services),
- Non-contracted local law enforcement, and
- Combinations of the above.

Agency-to-agency variations in design, equipment, policies, and procedures are significant, and influence security staffing and management. No single security organization description is adequate for all affected RFGS; each security program has evolved to address local conditions and resources.

Contract Security (non-sworn guards)	Local Law Enforcement (transit units of local police, contracted local police, or use of off-duty officers)	Sworn Transit Police
Denver RTD JTA Miami Metro-Dade	LACMTA Muni SDTI SRTD SCVTA CTA New Orleans RTA BSDA NYCT Portland Tri-Met	BART WMATA MARTA Maryland MTA MBTA NJT PATCO NFTA GCRTA PAT SEPTA DART

Table 6: Partial Listing of Security Organizations Used at Affected RFGS

Although transit agencies may differ in the resources available to support security, the systems approach to security allows for the maximization of security levels regardless of the agency-to-agency variations. Further, the successful implementation of the system security approach will address all aspects of the transit system and its environment.

Of the 32 affected RFGS, 29 also operate, and are managed, in a highly integrated fashion with bus services. Table 7 identifies transit systems that operate both rail and bus services. As demonstrated in the Table, motor bus operations represent a substantial amount of transit ridership at the affected transit agencies. Modern bus and rail terminals rarely rely on any single transport mode. Because of this reliance on multi-modal transportation, a rail agency's Security Program may directly, or indirectly, address the security concerns associated with motor bus operations. Motor bus and rail terminals share many characteristics, including the interrelationship between the four system elements described in the previous section. Due to this similarity in operations — especially between light rail and bus — as well as in threat identification and resolution, the application of the system security approach at many rail systems necessarily impacts bus operations.

The remainder of this Handbook is designed to provide both Oversight Agency and transit personnel with an overview of the rail transit security function. Oversight Agency personnel are encouraged to use these chapters as a reference to support the following activities:

- Modifying the Program Standard to address security,
- Requiring, reviewing and approving, and monitoring the RFGS Security Plan,
- Integrating security into the Three-year Safety Review,
- Integrating security into the Internal Safety Reporting requirements for each RFGS, and
- Integrating security into annual FTA certification and reporting.

This Handbook also contains information to assist RFGS operations and security personnel in their efforts to with Part 659. Finally, those security personnel with responsibility for bus operations are encouraged to examine these chapters to support their efforts to provide a safe and secure service for passengers and employees.

State	Transit System	Total Passenger Trips	% Rail	% Bus
CA	LA-LACMTA-Metro	361,820,182	7.4%	92.6%
	Sacramento-RT	24,802,430	30.9%	69.1%
	San Diego- The Trolley*	54,721,368	30.6%	69.4%
	San Francisco-BART	76,806,629	100.0%	0.0%
	San Francisco-Muni	136,240,993	34.0%	66.0%
	San Jose-SCCTD	48,793,258	12.6%	87.4%
CO	Denver-RTD	58,681,526	7.0%	93.0%
DC	Washington-WMATA	317,492,752	61.1%	38.9%
FL	Jacksonville-JTA	8,664,339	3.4%	96.6%
	Miami-MDTA	78,928,070	23.2%	76.8%
GA	Atlanta-MARTA	144,729,000	50.0%	50.0%
IL	Chicago-RTA-CTA	444,155,602	32.0%	68.0%
LA	New Orleans-RTA	60,469,683	8.8%	91.2%
MA	Boston-MBTA	278,858,502	63.7%	36.3%
MD	Baltimore-Maryland-MTA	94,682,427	18.9%	81.1%
MI	Detroit-DTC	2,048,852	100.0%	0.0%
MO	St. Louis-Bi-State	50,477,304	25.5%	74.5%
NJ	New Jersey Transit	130,814,467	3.1%	96.9%
	Philadelphia-PATCO	10,657,689	100.0%	0.0%
NY	Buffalo-NFTA	27,620,627	25.8%	74.2%
	NY-MTA-NYCTA	1,989,810,762	68.0%	32.0%
OH	Cleveland-RTA	64,608,589	21.5%	78.5%
OR	Portland-Tri-Met	70,743,969	14.2%	85.8%
PA	Johnstown-CCTA	1,458,804	9.7%	90.3%
	Philadelphia-SEPTA	280,881,771	44.5%	55.5%
	Pittsburgh-PAT	72,427,046	11.5%	88.5%
TN	Chattanooga-CARTA	2,450,534	18.9%	81.1%
	Memphis-MATA	11,913,793	5.5%	94.5%
TX	Dallas-DART	48,153,929	3.1%	96.9%
	Galveston-Island Transit	1,296,565	8.7%	91.3%
WA	Seattle-Metro	64,310,521	0.7%	99.3%
	Seattle Monorail	N/A	N/A	N/A
TOTAL		5,019,521,983	47.1%	52.9%
*Bus numbers reported by San Diego Transit N/A = not available				

Table 7: Bus and Rail Passenger Trips on SSO-Affected Systems, 1996²

² Source: Boyd, Maier & Associates analysis of 1996 National Transit Database data

3.2 System Security Program Plan Implementation

System security is a management process to encourage maximization of security resources through the inclusion of security in all RFGS life cycle phases. FTA’s State Safety Oversight Rule specifies a distinct approach to the implementation of system security at each affected RFGS. Figure 1 provides a graphical representation of this process.

As indicated in Figure 1, the Oversight Agency plays a central role in ensuring the application and appropriate functioning of the system security process. The modified Program Standard will guide this process, requiring that system security be incorporated at each RFGS. The Security Plan, required by the Oversight Agency, will document and support implementation of a System Security Program to integrate security functions and resources into a coherent and more effective program, as well as discuss the security management function. Oversight Agency review and approval of the Security Plan will further support efforts to enhance security coordination and to improve vital security management processes.

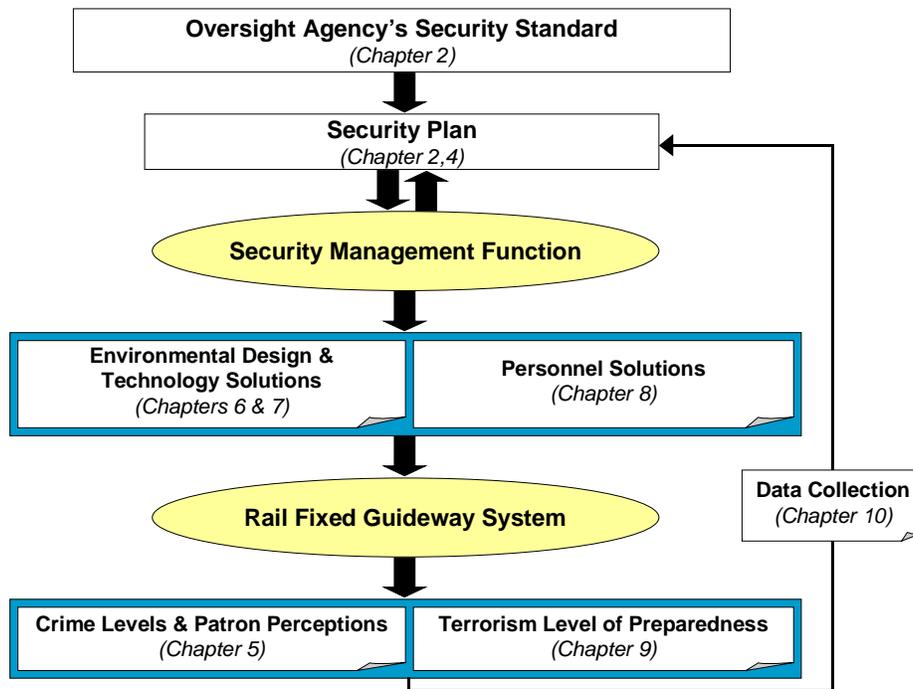


Figure 1: Integration of State Safety Oversight into RFGS Security Activities

Key security elements, as detailed in the Transit System Security Program Planning Guide, and as presented in Figure 1, will be coordinated to support the development and management of the Security Plan. These elements include the following:

- Design and modification of the RFGS environment,

- Security technologies,
- Security personnel deployment strategies,
- Terrorism prevention programs, and
- Security data collection activities.

The remainder of this chapter briefly summarizes each of the security function elements presented in Figure 1.

3.2.1 Crime Levels and Patron Perceptions

When designing security programs, RFGS typically first evaluate the levels and types of crimes experienced on their systems to determine security needs. RFGS security needs may depend on a number of related factors, including the following:

- Crime levels,
- Types of crime experienced,
- Types of ridership and trip purposes, and
- Geographic and jurisdiction considerations.

In addition to actual crime levels, passenger perceptions of security are particularly important for RFGS. Passenger perceptions of security, which research indicates do not correlate to actual crime rates, but rather to personal observations of public disorder, are difficult to measure and even more challenging to address.

Chapter 0 of this Handbook includes a detailed presentation of data describing the types and levels of crimes occurring at rail transit systems nationwide.

3.2.2 Environmental Design Solutions

Once crime and passenger fear levels have been established, the system security approach requires that security be addressed during the design, modification, and renovation of all RFGS facilities. To ensure that security is addressed throughout the planning and design of RFGS life cycle phases, many RFGS use Crime Prevention through Environmental Design (CPTED) and Situational Crime Prevention (SCP) techniques.

See Chapter 6 for a more detailed discussion of these techniques.

3.2.3 Technology Solutions

Generally, the technological approaches used by rail systems to ensure the security of passengers, employees, and systems can be categorized into four groups:

- Access Control Systems (ACS) technology which covers a broad range of security systems designed to protect one or more controlled access points into a restricted area;
- Surveillance equipment used to subject the criminal to the threat of being observed, increasing the chances of arrest;
- Communications systems ranging in complexity from simple telephones to sophisticated, satellite-based Automatic Vehicle Locators (AVL s); and incidents occurring on the system by manipulating the physical environment to produce effects that limit criminal behavior.

Chapter 7 provides a more detailed discussion of technology solutions.

3.2.4 Personnel Deployment Solutions

Some level of deployment of uniformed and undercover personnel in the transit environment is essential to prevent criminal occurrences on the system, to respond effectively to those incidents that do occur, and to reduce patron fear. The RFGS can deploy uniformed police, uniformed non-sworn security officers, and undercover police to perform the following functions:

- Maintain order on the system,
- Arrest offenders and collect and organize legal evidence to support the conviction of perpetrators,
- Support the security needs of passengers and employees, including the use of proactive techniques, such as community outreach and security problem-solving, and
- Support the development of Security Plan.

Security staffing alternatives available to RFGS, along with deployment options for these resources, are discussed in Chapter 8.

3.2.5 Terrorism Prevention Activities

In response to rising threat levels against RFGS nation-wide, terrorism prevention and emergency response programs have become an important part of overall security.

Chapter 9 provides a detailed discussion of these activities.

3.2.6 Data Collection

A properly designed and maintained data collection process serves as a valuable tool in countering transit crime. Data on crime levels, patron perceptions, and special conditions in the transit environment serve to:

- Guide policy development,
- Provide insights on current vulnerabilities,
- Assist in establishing priorities,
- Indicate possible trends or future problems,
- Evaluate the success of programs and technologies, and
- Focus personnel deployment.

Further information on data collection and analysis is detailed in Chapter 10.

4. The System Security Plan

As specified in the Transit System Security Program Planning Guide, the Security Plan should include the following sections:

- Introduction to System Security,
- Transit System Description,
- Management of the System Security Plan,
- Roles and Responsibilities,
- Threat and Vulnerability Identification, Assessment, and Resolution,
- Implementation and Evaluation of System Security Plan, and
- System Security Plan Modification.

The system security approach is documented in the RFGS Security Plan. This Plan should:

- Establish how security activities are organized at the RFGS,
- Specify employee responsibilities for security,
- Institute threat and vulnerability identification, assessment, and resolution methodologies, and
- Set security goals and objectives.³

To be effective in the transit environment, the system security approach, as documented in the Security Plan, requires increased efficiency in the ways in which the RFGS expends resources on security efforts. The system security process encourages transit operations, maintenance, and security personnel to identify critical RFGS security functions, including the following:

- Managing all calls requesting service,
- Providing patrols to deter criminal activity (violent crimes, pickpocketing, quality of life violations),
- Investigating serious criminal activity and combating crime through selective law enforcement techniques,

³ Balog et al, pg. 6.

- Providing protection for revenue collection personnel and safeguarding the revenues of the agency,
- Providing parking control and enforcement (uninsured and unlicensed private vans or jitneys, bus zones, and employee and agency facilities),
- Providing a system free from graffiti, and
- Providing a secure working environment for all employees.

In addition, this process integrates security activities into other functions performed to manage risk at the RFGS, including the following:

- Crowd control,
- Passenger medical emergencies,
- Fires,
- Accident investigation,
- Community outreach,
- Emergency response, and
- Anti- and counter-terrorism programs.

Finally, the Security Plan should identify security roles and responsibility for data collection and risk assessment methodologies being conducted at the RFGS, including the following:

- Site surveys (physical and planned),
- Technology acquisition and maintenance,
- Safety and security data collection and analysis (reporting to FTA's National Transit Database),
- Insurance and injury claims and records,
- Hazard identification and resolution process,
- Threat and vulnerability identification and resolution process,
- Safety and security reporting for RFGS management,
- Safety and security reporting for State Safety Oversight Agency, and
- Crime data collection and reporting for the Federal Bureau of Investigation (FBI).

The systems approach to security provides each transit system with a management tool to ensure that security functions are effectively integrated into system operations. The transit agency's Security Plan should address the concepts of the system security approach and outline specific steps for the proactive involvement of RFGS police, security personnel and local law enforcement in relationship to system security. The concepts and procedures outlined in the Security Plan must be communicated to those agencies involved in law enforcement activities, as well as system employees, as the application of some procedures may require specific training and coordinated drills with personnel from outside departments.

Although employees, security personnel, and local police forces share responsibility for maintaining a safe and secure transit system, the Security Manager retains ultimate responsibility for the management and oversight of the system security program plan, and for its success in keeping the system as safe and secure as possible. This Handbook uses the term *Security Manager* to refer to the person with ultimate responsibility for security at each transit system. The Security Manager may be the Chief of Police, the Director of Security, the Director of Safety, or may have some other title.

The Security Manager must provide the highest practical level of security in an environment of limited financial, staff, and material resources. Security is but one of the many transit system's needs; it must compete with operations, maintenance, and other departments for essential management and funding support. As a result of these and other limitations, Security Managers often make decisions based upon contingency and budgetary restrictions rather than by intentional design. Other challenges affect the ability of the Security Manager to design and implement an effective security program. Perhaps the most significant of these challenges is the rail transit environment itself.

Transit systems are attractive targets for criminals because they transport large numbers of passengers along scheduled routes. These systems serve a variety of neighborhoods with widely varying crime rates. Older stations, tunnels, and facilities, designed before architecture was commonly used as a tool for crime prevention, create an environment that may actually support crime and increase passenger fear. Management of these systems requires a security program that clearly identifies crime trends and potential risks, and subsequent responses, in an effort to keep the system as crime-free as possible. The typical Manager of modern transit security usually has three primary responsibilities:

- Meeting the actual and perceived security needs of the system's passengers,
- Protecting the system's employees, revenue, and property, and
- Maintaining order on the system.

The Security Plan should outline these responsibilities, as well as the role of the Manager in communicating security as a top priority to all employees.

A key to a successful Security Plan is the transit agency's ability to cooperate with the wide variety of other organizations. The Security Manager must work closely with personnel from other law enforcement agencies in roles that range from the exchange of information to preparing for multi-agency response to major incidents. In addition, coordination with law enforcement agencies regarding the effective use of resources will aid in the management of security personnel and deployment tactics, as discussed in chapter nine. Further, transit agencies must take a proactive role in developing working relationships with other outside organizations that enhance security and safety within the transit environment.

5. Crime Levels and Patron Perceptions

In 1979, the Southeast Michigan Council of Governments (SEMCOG) conducted a study of fifty-seven U.S. transit systems. The findings of this study suggest that crime on transit systems, while generally lower than in the neighborhoods surrounding the system, "is a national problem of major proportion that cannot be ignored in terms of the seriousness and/or frequency with which offenses are committed."⁴ Over the past two decades, researchers have demonstrated that transit crime patterns generally parallel crime patterns in the surrounding neighborhoods (i.e., a high incidence of transit crime is likely to occur in those geographical areas with a high incidence of street crime). In addition, research indicates that:

- Most violent or serious crimes that occur within the transit environment occur on large metropolitan transit systems
- Juveniles and young adults commit the majority of crimes on public transportation.⁵

Rail systems (heavy, light, and commuter) generally experience higher crime rates than bus systems, although crime reporting for bus operations tends to be less reliable than that for rail services. Transit systems, because they provide shelter and 24-hour availability, are also a favored location for the homeless, panhandlers, and with increasing frequency, low-level drug dealers. The crimes committed by these groups within the transit system impact patron perceptions.⁶ Research also reveals that crime against passengers is much more likely to occur in a transit station or bus stop, rather than on a moving train or bus.⁷

Past research on transit crime indicates that robbery, larceny, and serious assaults account for the majority of crimes committed against people, while vandalism, public drunkenness, and disorderly conduct constitute the majority of crimes against property.

5.1 Crime Levels

In 1995, the FTA modified its National Transit Database (NTD) reporting system to include an annual report on security incidents (Safety and Security Form 405). This form requests both rail and bus transit systems receiving grant money from the FTA to record and disclose the occurrences of Part I and Part II crimes (as defined by the Federal Bureau of Investigation) on their property.

⁴ Southeast Michigan Council of Governments (SEMCOG), *Crime and Security Measures on Public Transportation Systems: A National Assessment* (Washington, D.C.: U.S. Urban Mass Transportation Administration; Springfield, VA, 1979), pg. 14.

⁵ Henry DeGeneste and John Sullivan, *Policing Transportation Facilities* (Springfield, IL: Charles C. Thomas), 1994, pp. 3-27 and pp. 114-122.

⁶ DeGeneste and Sullivan, pp. 3-27.

⁷ DeGeneste and Sullivan, pp. 3-27.

While definitional and jurisdictional differences may limit the accuracy of this crime reporting, the NTD database provides a general picture of criminal activity in the transit environment. To provide a description of the types and level of crime occurring at affected RFGS, crime statistics from the 1996 NTD are presented below, organized according to three general crime categories⁸:

- Quality of Life Crimes. Quality of life crimes are minor crimes that degrade the overall quality of the transit service, interfere with the passengers using the system, and limit the ability to provide passengers with an inviting environment. This category includes issues that typically do not pose a physical threat to passengers, but may cause intimidation, increase the perception that the system is not secure, and reduce the likelihood that public transit will be used in cases where riders have other options. Crimes of this type include public drunkenness, vandalism, and disorderly conduct.
- Property Crimes. Property crimes include burglary and larceny (which includes pick pocketing, purse snatching, and thefts from motor vehicles), motor vehicle theft, and fare evasion.
- Violent Crimes. Violent crimes include homicide, robbery, assault, and rape. Although they are relatively infrequent, these offenses require extensive time and attention from police/security departments.

In each category, information is provided on crime levels by system type, as well as where crimes occurred (in stations, on vehicles, or on other transit property).

5.1.1 Types and Occurrences of Rail Fixed Guideway System Crime

According to the NTD database, RFGS reported 91,551 criminal occurrences in 1996. Figure 2 represents 1996 crime level data, as reported by RFGS for quality of life, property, and violent crime. Quality of life and property crimes account for over 93 percent of all crimes on RFGS. Violent crime occurs relatively infrequently, accounting for only 6.6 percent of all RFGS crime. Figure 3 shows the breakdown of crime by system type.

⁸ Source: Boyd, Maier & Associates analysis of 1996 National Transit Database data

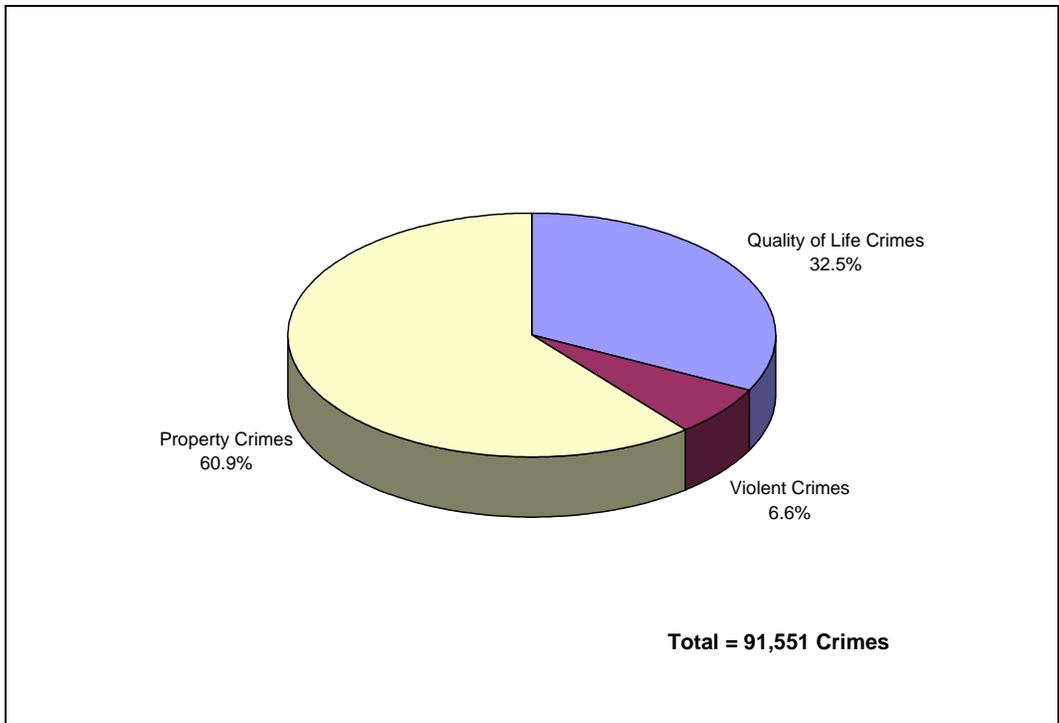


Figure 2: Rail Fixed Guideway System Crimes by Type, 1996

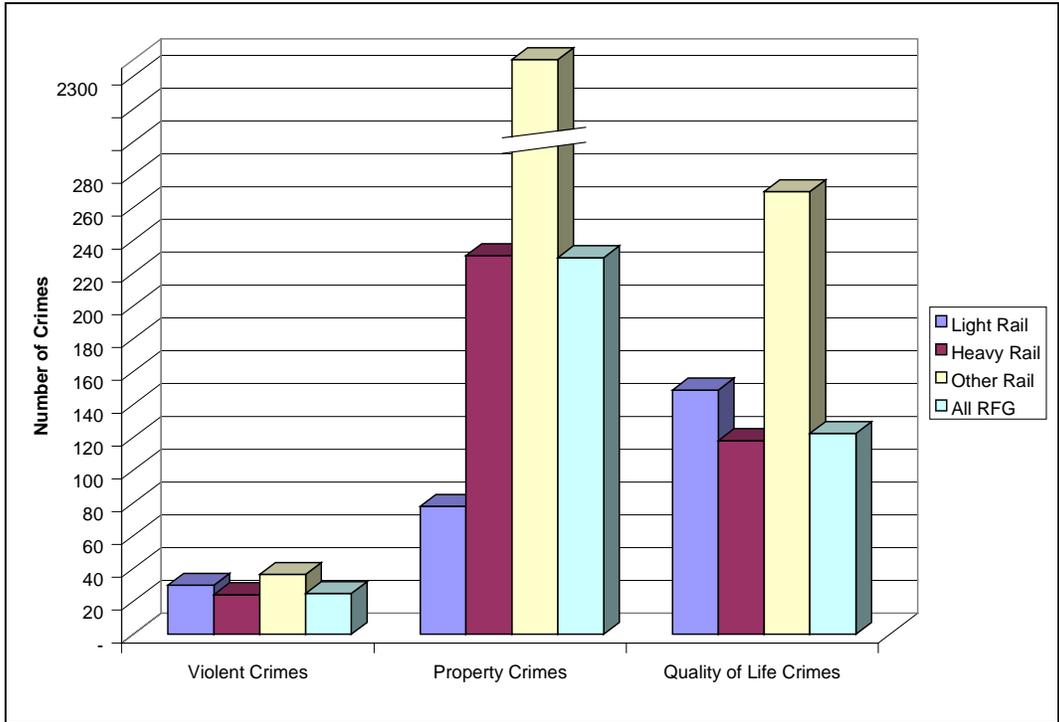


Figure 3: Rail Fixed Guideway System Crimes per 10 Million Passenger Trips by System Size, 1996

5.1.1.1 RFGS Quality of Life Crimes

Figure 4, Figure 5, and Figure 6 present data on quality of life (QOL) crime in RFGS. Key findings include:

- The most common QOL crimes are disorderly conduct and drunkenness, which account for nearly 80 percent of QOL crimes on RFGS,
- Trespassing and loitering account for 9.5 percent of QOL crimes,
- Most QOL crime arrests occur on trains (62.2 percent) with a smaller percentage in transit stations (31.1 percent),
- Heavy rail systems have the largest number of disorderly conduct crimes, significantly higher than the rate experienced on other RFGS modes,
- The rates of drunkenness and drug abuse violation were higher on light rail systems than on other RFGS systems, and
- Trespassing, vandalism, and loitering rates were significantly higher in the Other Rail category due to high rates on Automated Guideway systems.

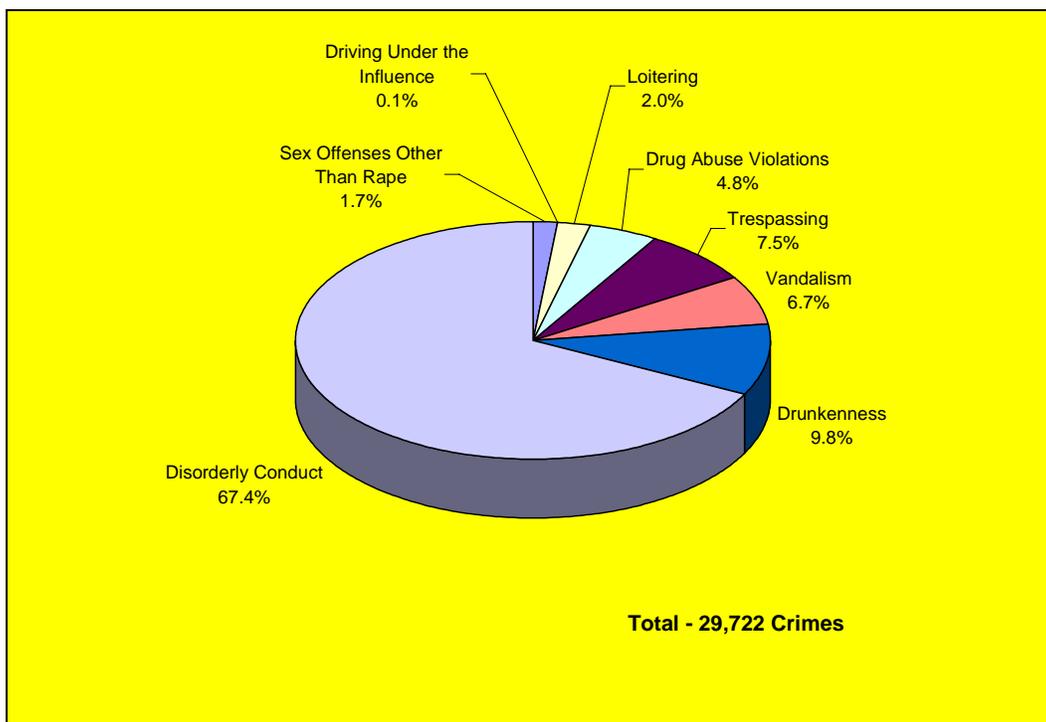


Figure 4: Rail Fixed Guideway System Quality of Life Crimes, 1996

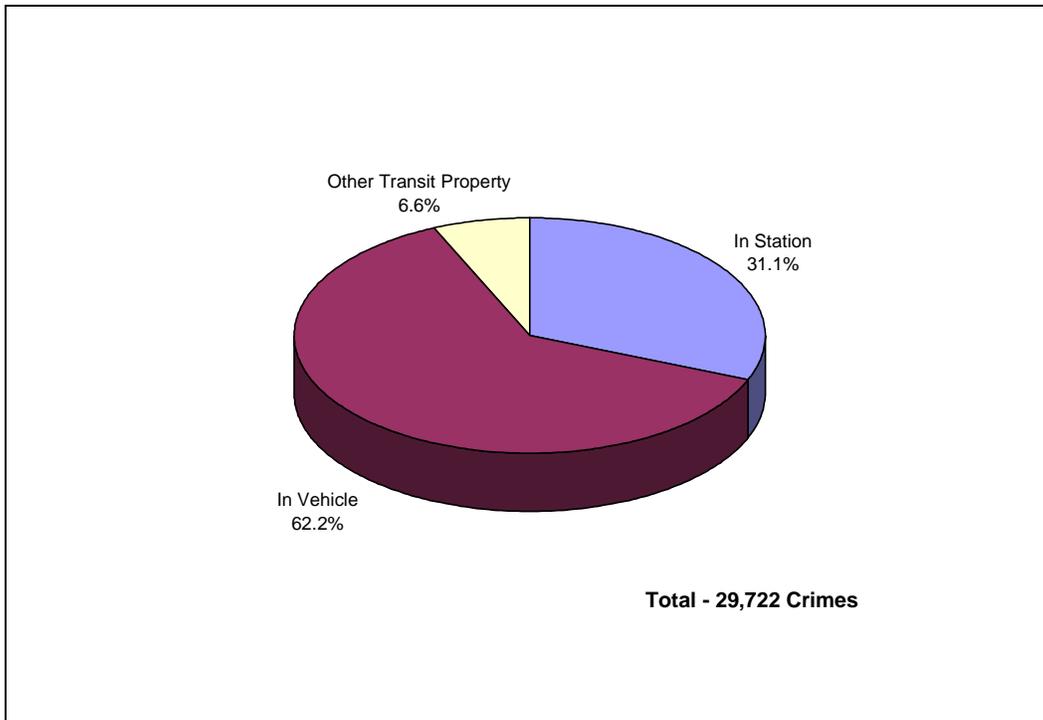


Figure 5: Rail Fixed Guideway System Quality of Life Crimes by Location, 1996

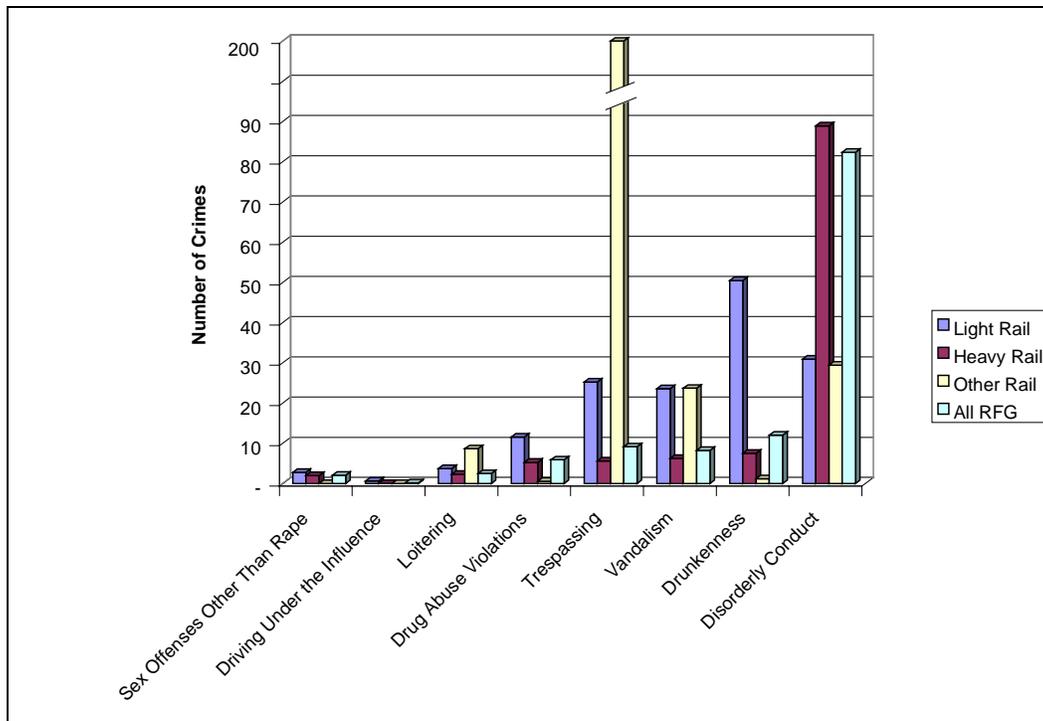


Figure 6: Rail Fixed Guideway System Quality of Life Crimes by System Type (Per 10 Million Passenger Trips)

5.1.1.2 RFGS Property Crimes

Figure 7, Figure 8, and Figure 9 present data on RFGS property crimes. Key findings include:

- Fare evasion accounts for over 80 percent of property crimes in the RFGS environment,
- Theft and burglary account for less than 20 percent of reported property crime offenses,
- Due to high numbers of incidents on automated guideway systems, the highest rate for fare evasion is in the Other Rail category (over 10 times the rate experienced on light and heavy rail systems),
- Heavy rail systems also experience a relatively high rate of fare evasion (180 per 10 million passenger trips),
- Rates for burglary, arson, and motor vehicle theft are low across all RFGS systems,
- Eighty percent of property crimes occur in stations, and
- Only 11.4 percent of property crimes occur in RFGS vehicles.

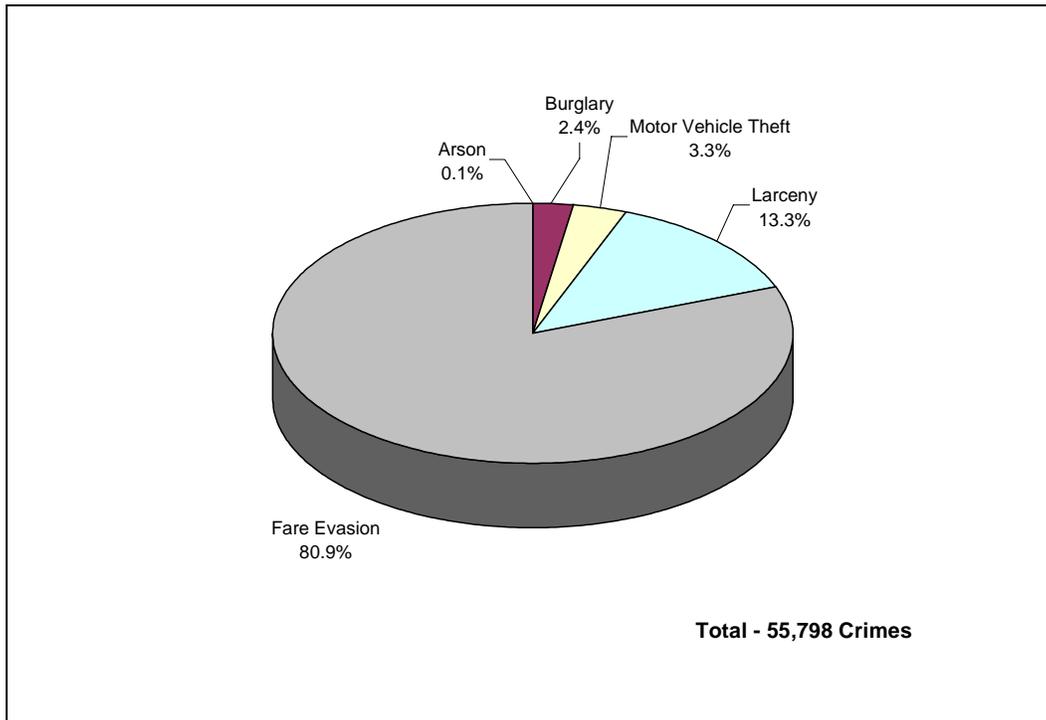


Figure 7: Rail Fixed Guideway System Property Crimes, 1996

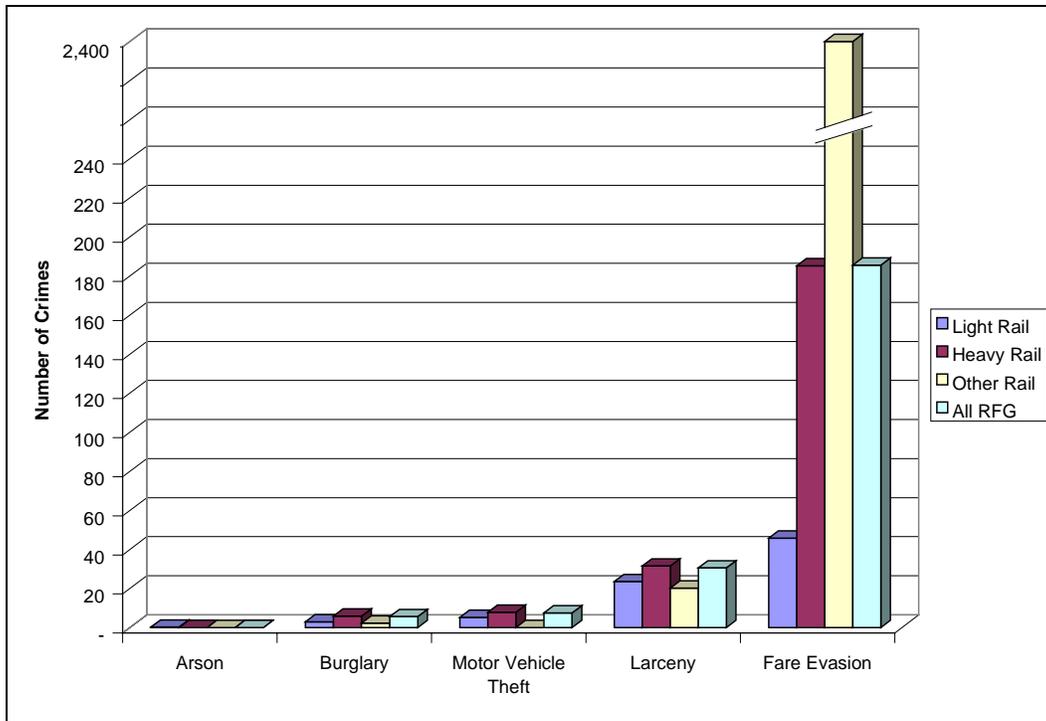


Figure 8: Rail Fixed Guideway System Property Crimes by System Type (Per 10 Million Passenger Trips)

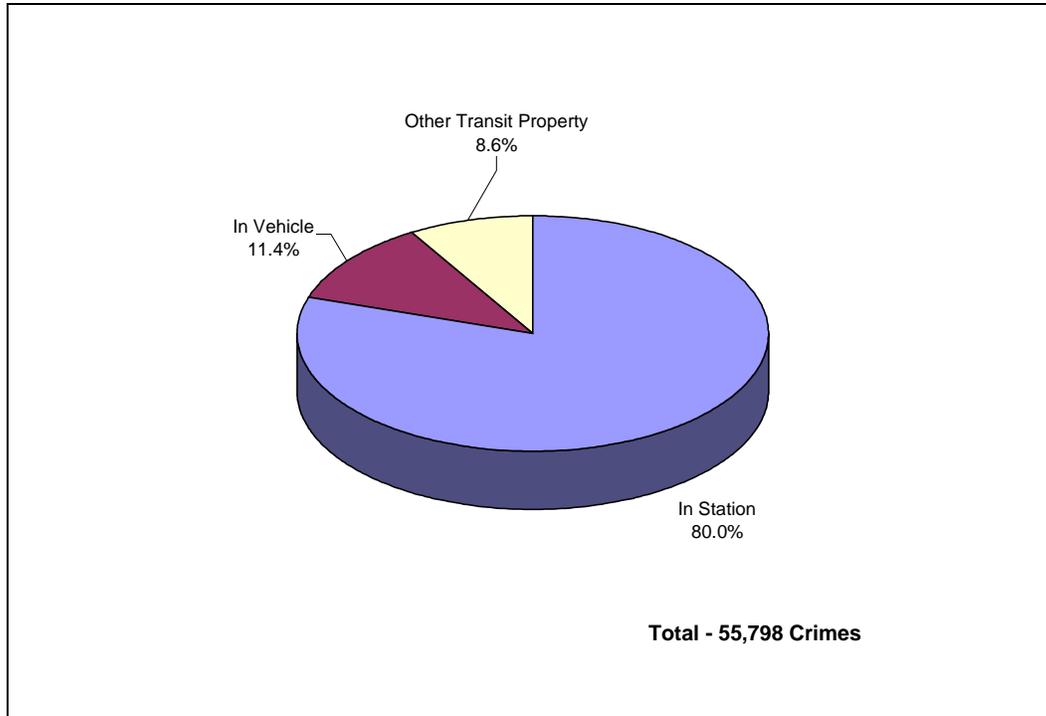


Figure 9: Rail Fixed Guideway System Property Crimes by Location, 1996

5.1.1.3 RFGS Violent Crimes

According to reported data from the affected RFGS, violent crimes occur relatively infrequently. Figure 10, Figure 11, and Figure 12 present data on RFGS violent crime. Key findings include:

- The most serious violent crimes (homicide and forcible rape) comprise less than one percent of the total incidents of violent crime occurring on RFGS property,
- Incidents of assault on operators and passengers account for almost 43 percent of the violent crime experienced,
- Robberies, the taking of items and money from victims using violence or the threat of violence, are a significant problem on RFGS, accounting for 56.8 percent of violent crimes,
- Light rail and other rail systems experience a higher rate of robbery and assaults than heavy rail systems,
- 65 percent of violent crimes occur in stations, and
- 27.7 percent of violent crimes occur in vehicles.

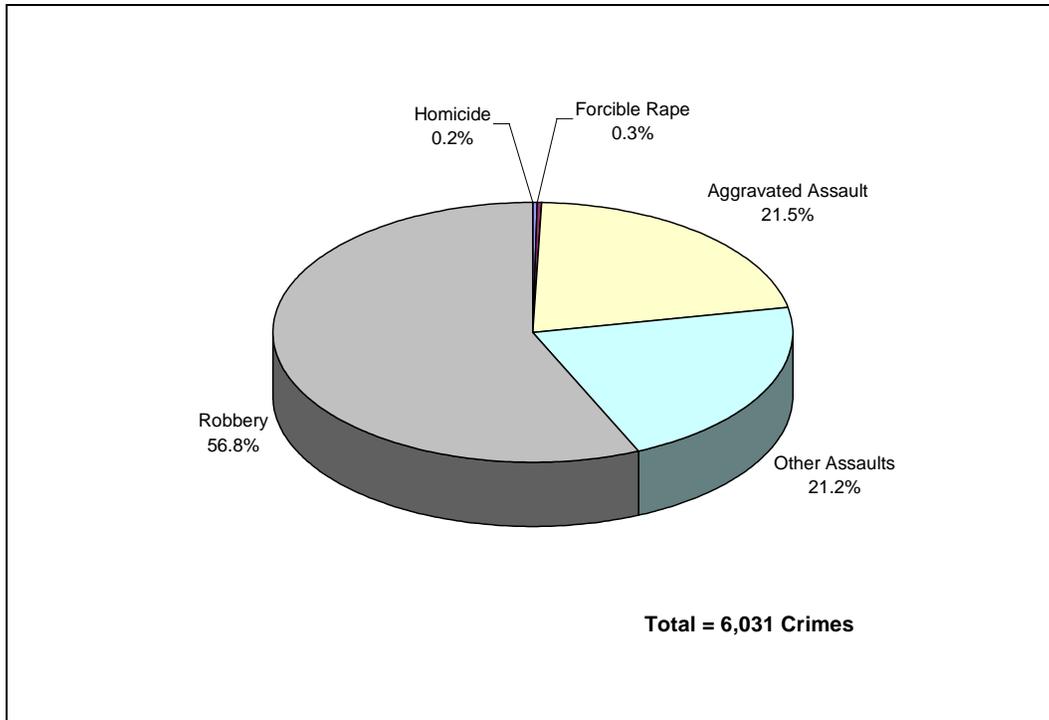


Figure 10: Rail Fixed Guideway System Violent Crimes, 1996

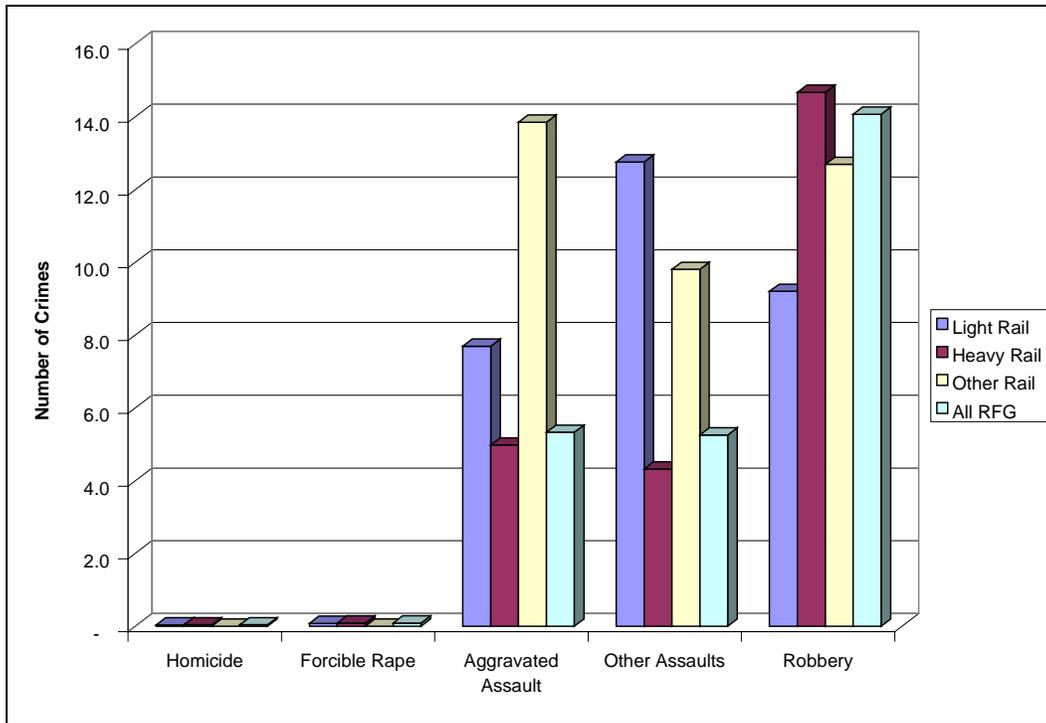


Figure 11: Rail Fixed Guideway System Violent Crimes by System Type (Per 10 Million Passenger Trips)

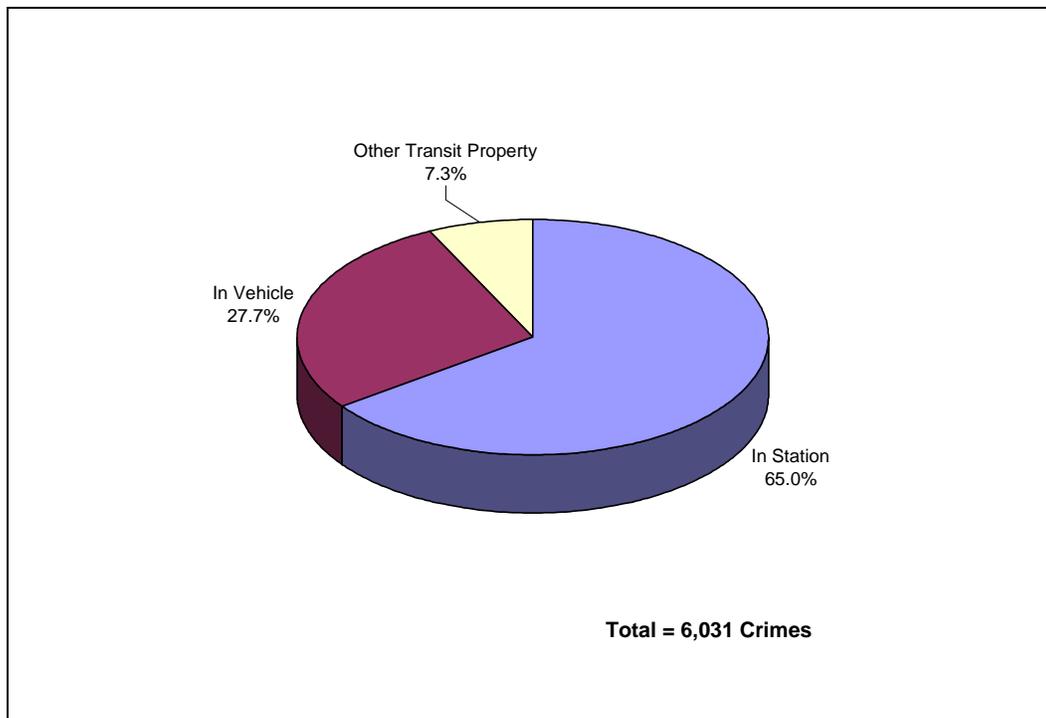


Figure 12: Rail Fixed Guideway System Violent Crimes by Location, 1996

RFGS violent crime occurrences, when compared to municipal violent crime, are minimal. For example, in 1995, the city of Los Angeles experienced more violent crime in a two-month period than *all affected RFGS reporting to the NTD during the entire year*. To place the occurrence of violent crimes at affected RFGS in perspective, Table 8 presents a breakdown of 1995 Part I Crimes as reported to the FBI by municipal police⁹ and to the FTA by transit police and security departments. This table demonstrates that rates of violent crime in the transit environment are considerably lower than rates in the municipal areas served by RFGS.

5.1.2 Types and Occurrences of Motor Bus Crime

RFGS generally experience higher crime rates than motor bus systems, and this is evidenced by motor bus systems reporting a total of 28,835 crimes in 1996. Quality of life crimes accounted for over 60 percent of these crimes (see Figure 13). Property crimes represented 21.7 percent and violent crimes represented 14.4 percent of the total. Crime levels for violent and property crimes were higher on larger systems (see Figure 14). Quality of life crimes were more prevalent on small motor bus systems.

⁹ Universal Reference Publications, Crime in America's Top-Rated Cities: A Statistical Profile 1995-96 (Boca Raton, FL), 1996.

City and RFGS	Part I Crimes		
	Violent Crimes against People	Property Crimes	Murders
Los Angeles, CA	83,701	205,249	846
LACMTA – all Transit	532	398	2
LACMTA RFGS Only	97	59	0
San Diego, CA	12,599	64,126	113
All Transit	185	82	0
RFGS Only	53	82	0
San Francisco, CA	10,837	51,023	91
BART – All Transit	242	3,210	2
Muni – All Transit	179	698	0
BART – RFGS Only	242	3,210	2
Muni – RFGS Only	39	49	0
Denver, CO	4,706	30,728	81
RTD - All Transit	90	45	0
RTD – RFGS Only	INA	INA	INA
Washington, D.C	15,177	47,967	399
WMATA – All transit	184	1,043	0
WMATA – RFGS Only	133	975	0
Miami, FL	12,969	52,298	115
MDTA – All Transit	91	326	0
MDTA – RFGS Only	59	299	0
Atlanta, GA	14,684	51,596	191
MARTA – All	161	966	1
MARTA – RFGS Only	144	902	1
Chicago, IL	60,000 ¹⁰	205,001	928
RTA-CTA – All	742	1,520	2
RTA-CTA – RFGS Only	449	1,159	1
New Orleans, LA	9,322	40,521	425
RTA – All	30	32	0
RTA – RFGS Only	11	12	0
Boston, MA	10,664	42,414	85
MBTA – All	447	478	1
MBTA – RFGS Only	330	265	1
Baltimore, MD	20,952	71,832	321
MTA – All	201	290	0
MTA – RFGS Only	69	229	0
Detroit, MI	27,000 ¹¹	94,356	541
DTC – All	10	9	0
DTC – RFGS Only	10	9	0

INA = Information Not Available

Table 8: Violent Crimes in Municipalities and Rail Fixed Guideway Systems, 1995

¹⁰ Estimate – final 1995 numbers not available

¹¹ Estimate – final 1995 numbers not available

City and Transit Agency	Part I Crimes		
	Violent Crimes against People	Property Crimes	Murders
Newark, NJ	INA	INA	INA
NJT – All	162	815	0
NJT – RFGS Only	26	13	0
Buffalo, NY	6,894	24,093	94
NFTA – All	36	120	0
NFTA – RFGS Only	22	53	0
Cleveland, OH	7,744	30,001	132
RTA – All	72	110	0
RTA – RFGS Only	56	68	0
Philadelphia	20,638	79,779	404
SEPTA – All	421	646	3
PATCO – All	8	85	0
SEPTA – RFGS Only	405	530	3
PATCO – RFGS Only	8	85	0
Pittsburgh, PA	4,105	22,245	64
PAT – All	68	198	0
PAT – RFGS Only	3	INA	0
Memphis, TN	9,855	51,538	159
MATA – All	3	INA	0
MATA – RFGS Only	1	INA	0

INA = Information Not Available

Table 8 (cont.): Violent Crimes in Municipalities and Rail Fixed Guideway Systems, 1995

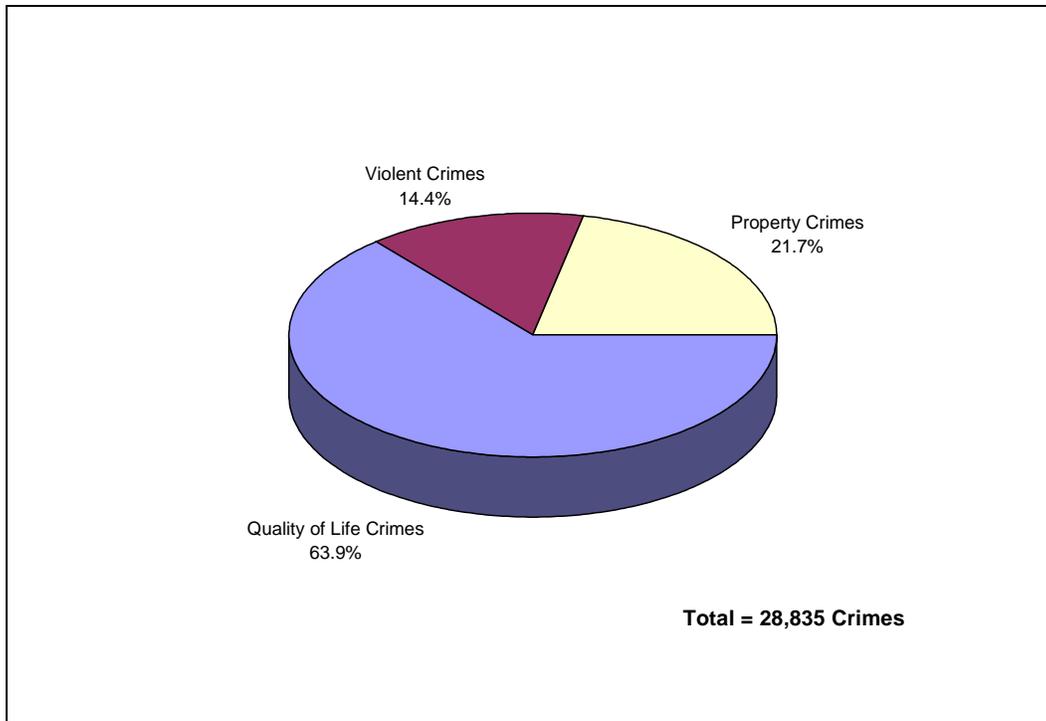


Figure 13: Motor Bus Crimes by Type, 1996

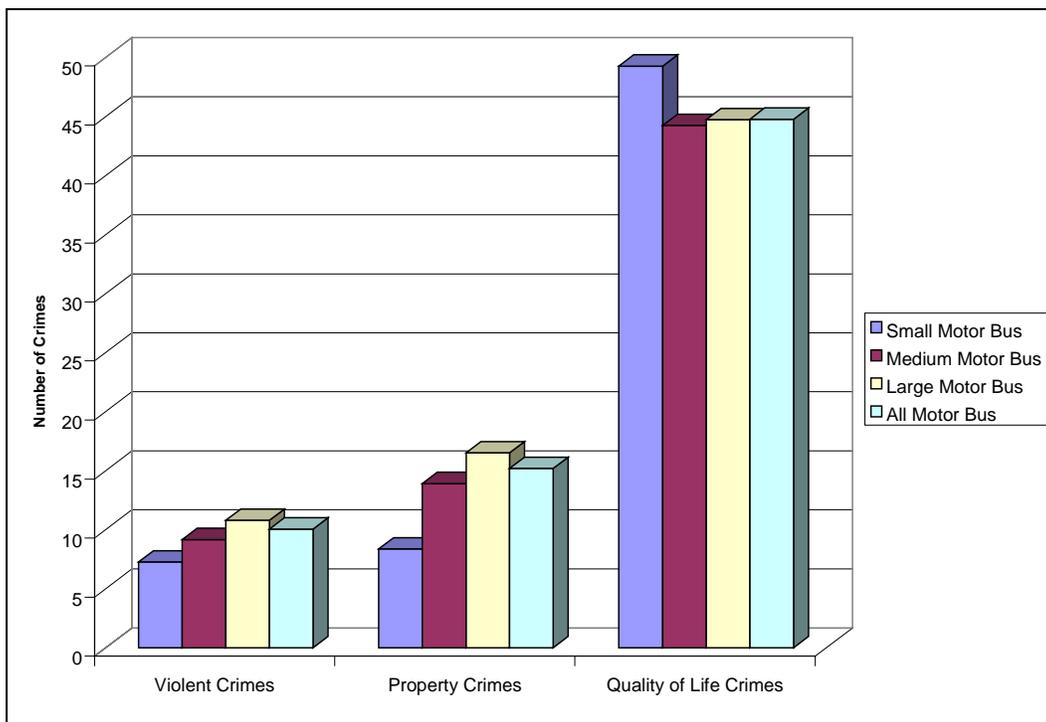


Figure 14: Motor Bus Crimes per 10 Million Passenger Trips by System Size, 1996

5.1.2.1 Motor Bus Quality of Life Crimes

Figure 15, Figure 16, and Figure 17 present information of Motor Bus quality of life crimes. Key findings include:

- Drunkenness and disorderly conduct account for nearly half of motor bus QOL crime,
- Vandalism (33.4 percent of QOL crimes) is a significant problem on buses,
- The rate of drug abuse violations was significantly higher on large motor bus systems than on other systems,
- Small and medium motor bus systems had a higher incidence of drunkenness arrests than large systems,
- Small systems also had a high rate of disorderly conduct crimes (18 per 10 million passenger trips), and
- 65.4 percent of motor bus QOL crimes occurred on buses.

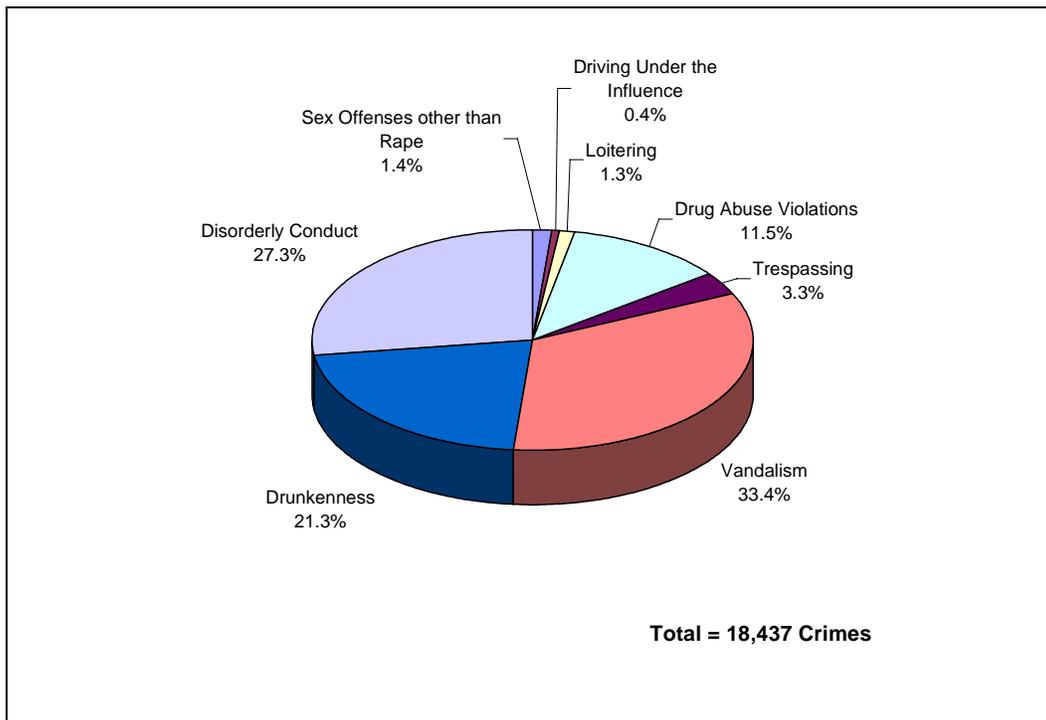


Figure 15: Motor Bus Quality of Life Crimes, 1996

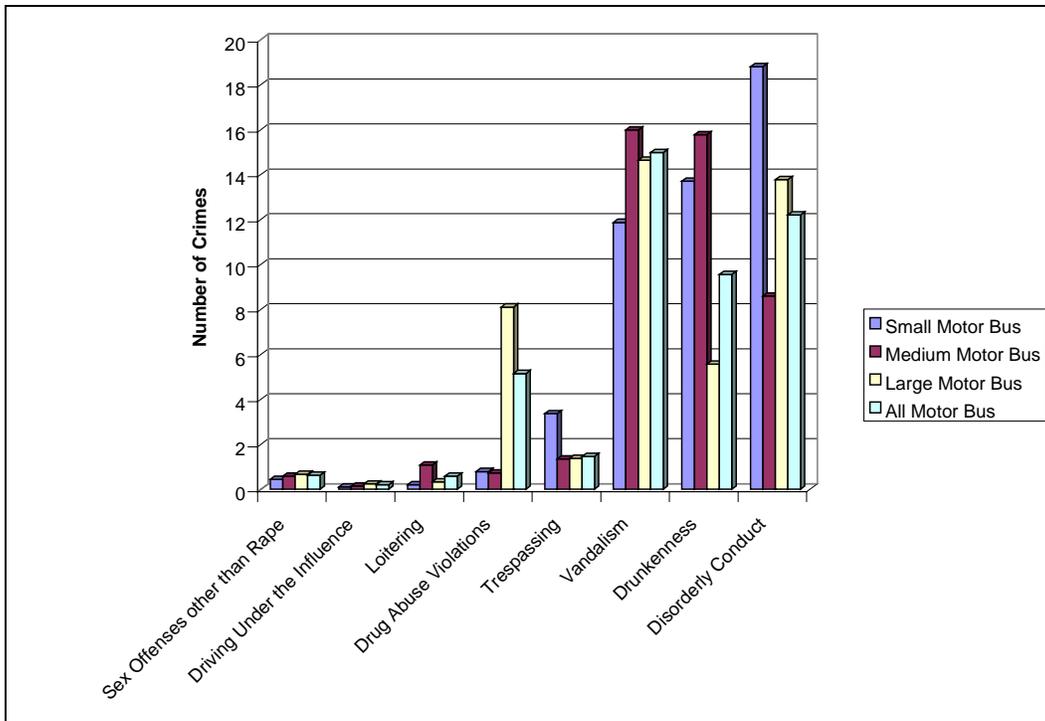


Figure 16: Motor Bus Quality of Life Crimes by System Size (Per 10 Million Passenger Trips)

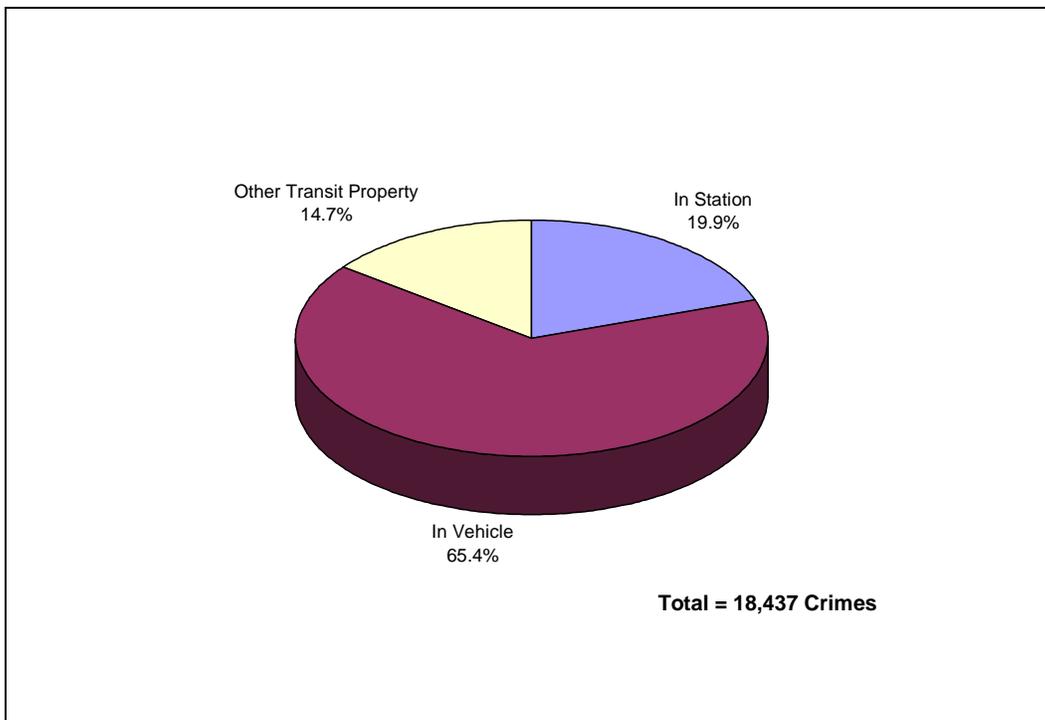


Figure 17: Motor Bus Quality of Life Crimes by Location, 1996

5.1.2.2 Motor Bus Property Crimes

Figure 18, Figure 19, and Figure 20 present data on motor bus property crimes. Key findings include:

- Larceny (54.5 percent) and fare evasion (37.9 percent) account for over 90 percent of property crimes,
- Larceny rates are highest on large systems,
- Fare evasion is most significant on medium motor bus systems,
- Rates for arson, burglary, and motor vehicle theft are relatively even across all size systems,
- 66.3 percent of property crimes occur on buses, and
- A large number (28.9%) of property crimes occur on transit property other than buses and stations.

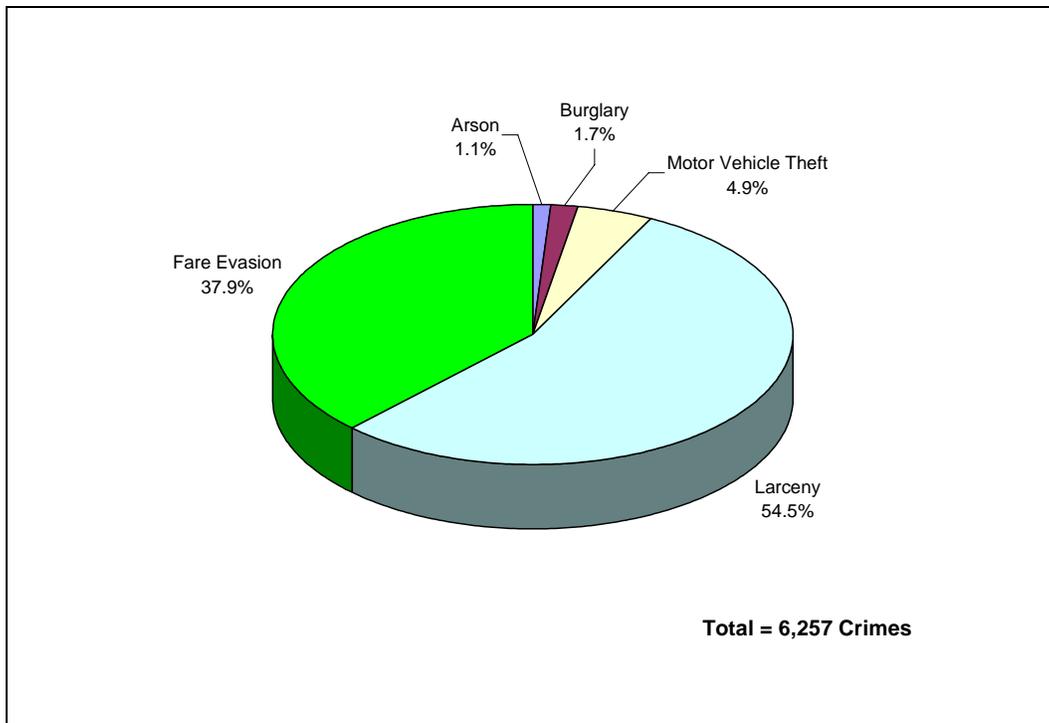


Figure 18: Motor Bus Property Crimes, 1996

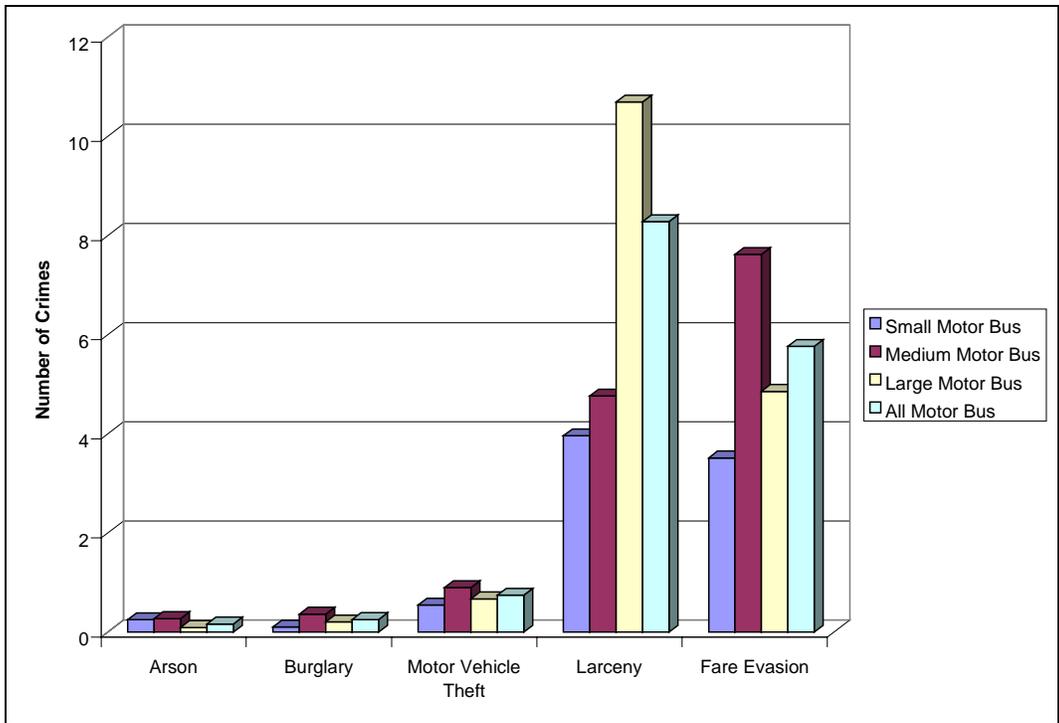


Figure 19: Motor Bus Property Crimes by System Size (Per 10 Million Passenger Trips)

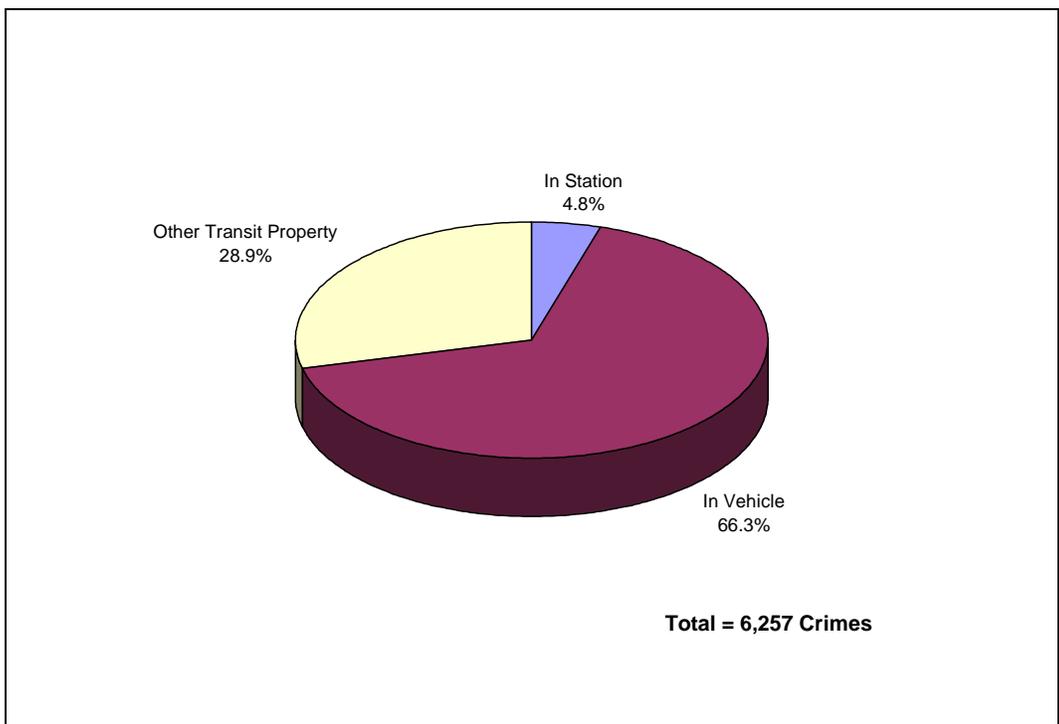


Figure 20: Motor Bus Property Crimes by Location, 1996

5.1.2.3 Motor Bus Violent Crimes

Figure 21, Figure 22, and Figure 23 present motor bus violent crime data. Key findings include:

- Assaults are the largest violent crime problem on motor buses, account for nearly eighty percent of violent crimes,
- Twenty percent of violent crimes on buses were robberies,
- Homicide and rape were very infrequent (a total of 9 homicides and 13 rapes were reported on motor bus systems in 1996),
- Assault rates were relatively consistent among small, medium, and large motor bus systems,
- Robbery is more frequent on larger systems, and
- Sixty-three percent of motor bus violent crimes were committed on buses.

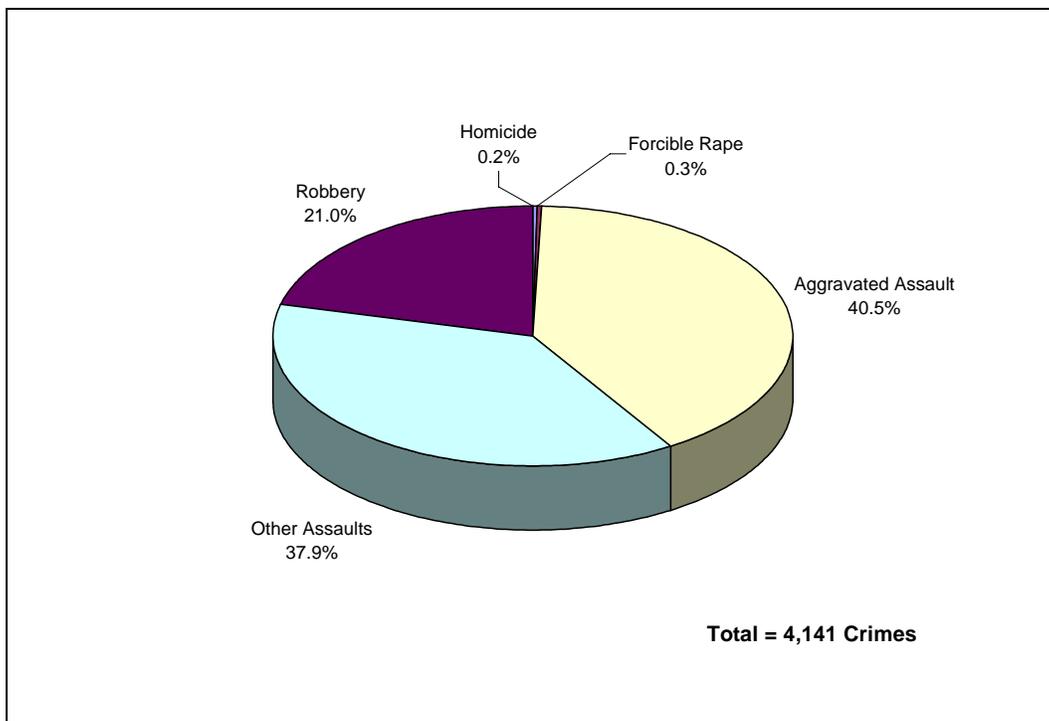


Figure 21: Motor Bus Violent Crimes, 1996

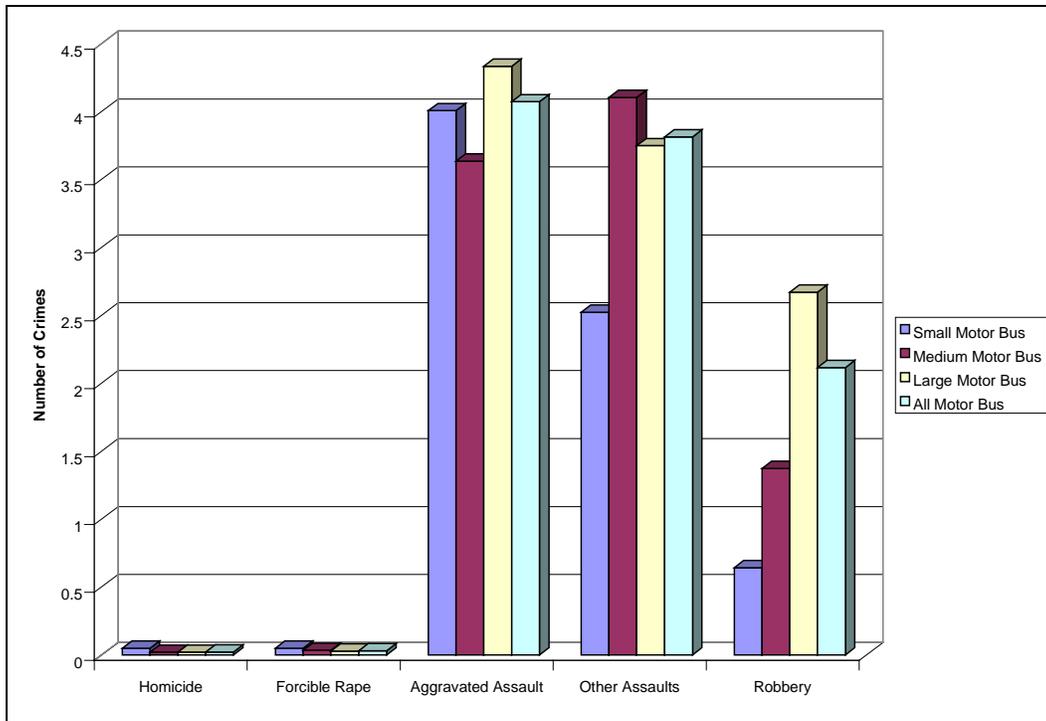


Figure 22: Motor Bus Violent Crimes by System Size (Per 10 Million Passenger Trips)

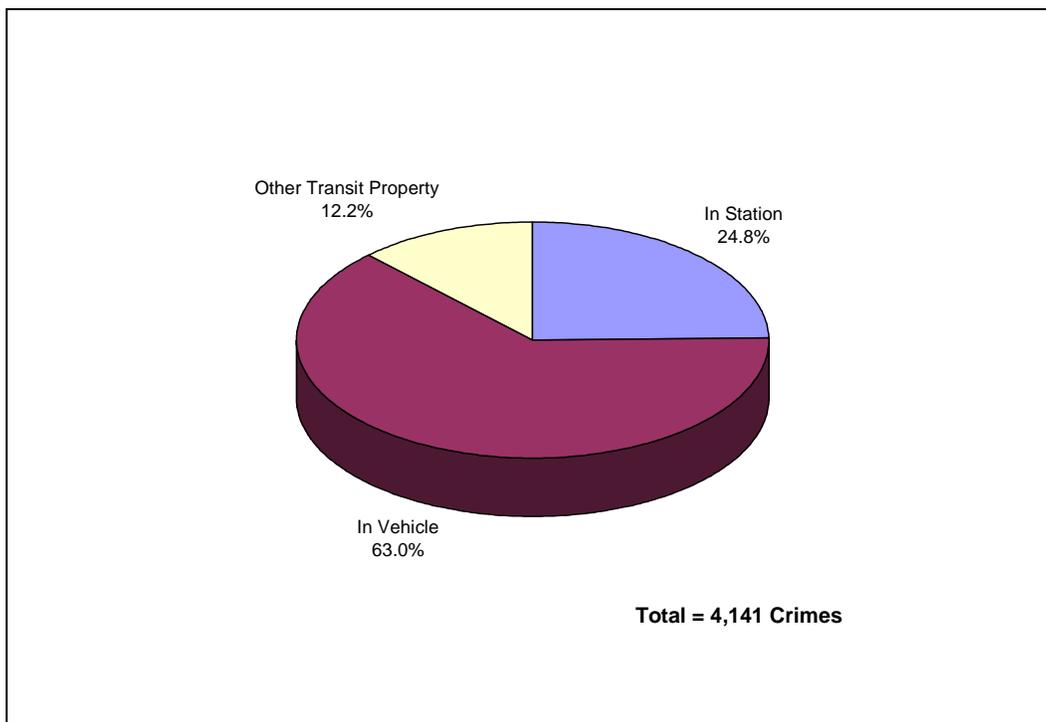


Figure 23: Motor Bus Violent Crimes by Location, 1996

5.1.3 Comparison of Motor Bus and RFGS Crime

NTD statistics indicate that overall crime levels reported on motor bus systems are, indeed, considerably lower than those on RFGS. Figure 24, Figure 25, and Figure 26 compare quality of life, property, and violent crime levels reported by RFGS and motor bus systems. Data is presented in number of crimes per ten million passenger trips. For nearly every crime, RFGS levels exceed those experienced by bus systems. A notable exception is vandalism, which is more prevalent on bus systems.

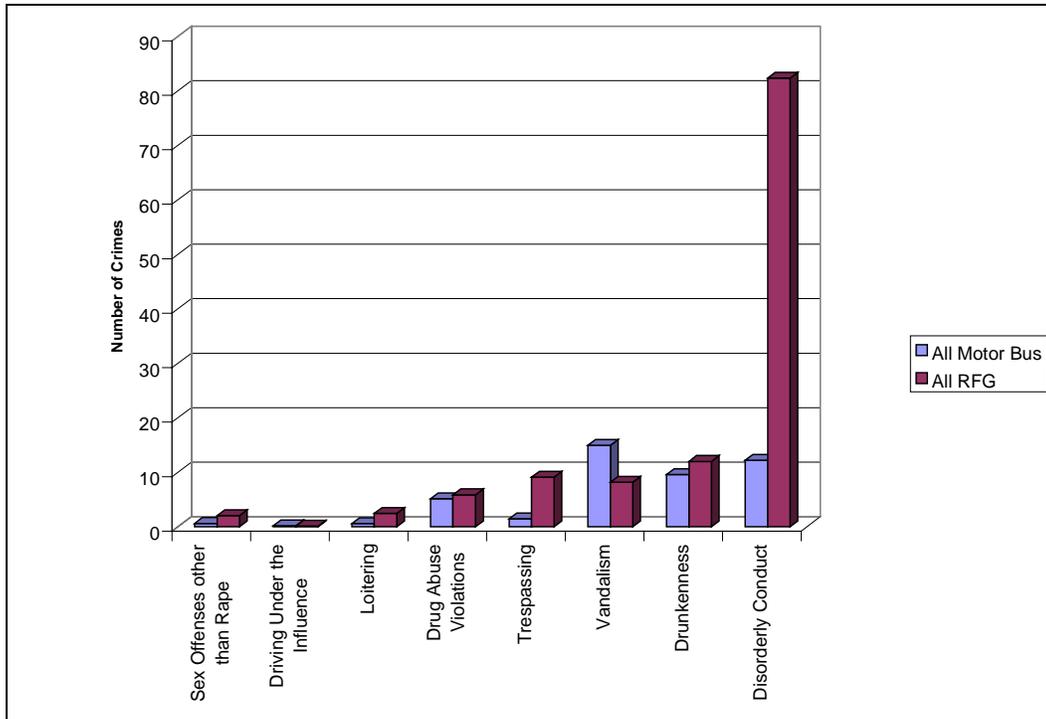


Figure 24: Rail and Motor Bus Quality of Life Crimes per Ten Million Passenger Trips, 1996

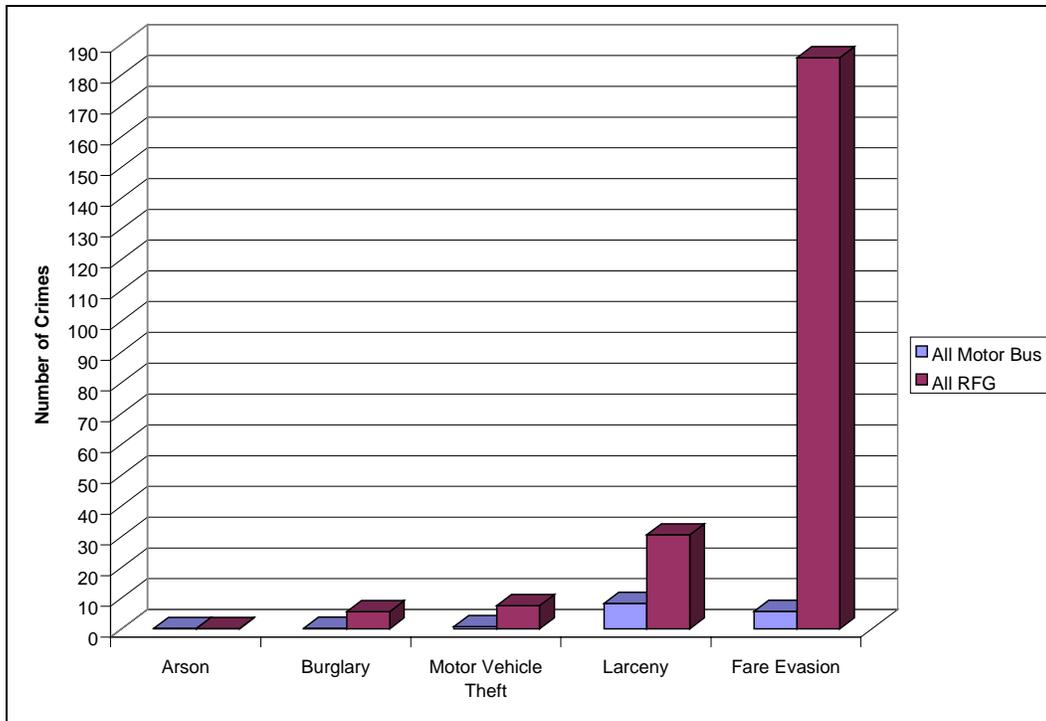


Figure 25: Rail and Motor Bus Property Crimes per Ten Million Passenger Trips, 1996

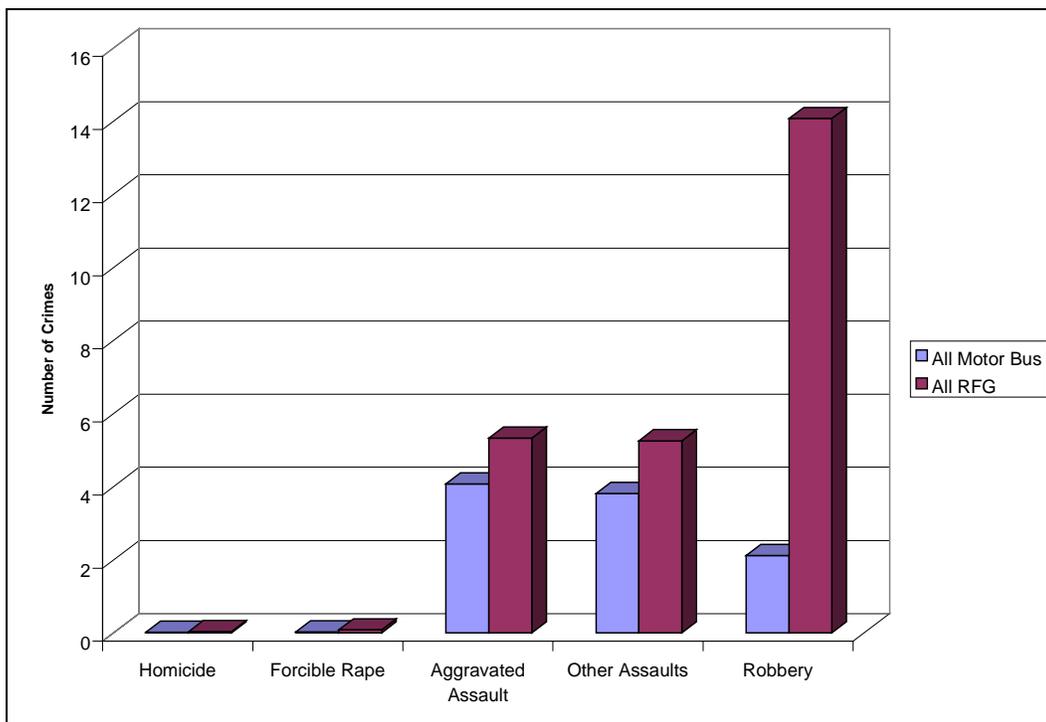


Figure 26: Rail and Motor Bus Violent Crimes per Ten Million Passenger Trips, 1996

When comparing and contrasting crime level data between RFGS and motor bus systems, it is important to recognize that in many instances, it is difficult to employ security methods that address crime in just one particular mode. Due to the intermodal nature of those terminals that share both motor bus and rail operations, it is encouraged that agencies implement the systems security approach to criminal activity prevention and mitigation with the entire transit system in mind, thus increasing security levels within both modes of transportation.

5.2 Patron Perceptions

System crime, whether on rail or motor bus, and the subsequent impact of such activity upon the public, presents a unique challenge for the transit agency. This situation is complicated by both the difficulty of measuring and documenting security effectiveness and by the highly emotional nature of the public's response to crime. The transit environment is unfamiliar, even uncomfortable, for many passengers, producing feelings of confinement, vulnerability, and intimidation. These feelings must be addressed by the system in order to reduce patron fear and to increase passenger confidence in the system.

Transit agencies struggle daily with the problem of patron fear or the discomfort that fear of crime creates in some riders. Transit systems provide a valuable service, which must be marketed to and supported by the public. Communities perceiving a link between crime and the presence of a bus depot or a rail station will not support the expansion of mass transit into their neighborhoods. Patrons who perceive the transit system as dangerous will limit their use of the system, especially during off-peak hours.

Transit-dependent populations, who must use the system to get to work or other locations, may become irritable or even abusive to system employees when travelling on routes they feel are unsafe. Bus operators and rail personnel who work in the transit environment must deal with the stressful consequences of disruptive behavior, fare evasion, intimidation, and public drinking on a daily basis. This environment can have a significant impact on transit personnel morale, absenteeism, management, and the quality of customer interaction.

Transit police and security personnel can utilize modern crime data collection and analysis techniques to assess their success or failure in reducing crime on transit property. Gauging the efficacy of fear reduction efforts, however, is far more challenging. Many different observations and experiences can trigger the public perception of disorder, and these triggers may vary from patron to patron. Both disorder and the patron response to it are very difficult to measure in quantitative terms traditionally used by police organizations to evaluate performance. In the transit industry, there are many assumptions about the effectiveness of various deployment and technology strategies to reduce disorder and patron fear.

6. Security by Design

Like many other “specialized environments,” RFGS are designed and preserved by professionals including engineers, architects, planners, managers, operators, and maintenance personnel. Twenty years of research demonstrates that the environment created by these professionals has a significant impact on the level and types of crime to occur.¹²

The *system security approach* encompasses the concept that crime can be “designed out” of RFGS facilities during the planning phase of the transit life cycle. Failure to recognize and incorporate crime prevention features during system planning may result in higher than anticipated crime rates, elevated passenger fear, and expensive system modifications in response to serious criminal incidents.

It is important to recognize, however, that in the transit environment, the utility of architectural design principles is not limited to the planning life cycle phase. Older RFGS, such as New York City Transit (NYCT) and Massachusetts Bay Transportation Authority (MBTA), have effectively incorporated crime prevention design to legitimize public space, improve passenger flow through stations and corridors, and reduce criminal opportunities. Environmental criminology, focusing on the relationship between physical space design and behavior, has provided RFGS operators with a valuable crime prevention tool.

This chapter provides a general discussion of the theoretical foundation behind the two key approaches used in designing and maintaining transit facilities and vehicles:

- Crime Prevention through Environmental Design (CPTED), and
- Situational Crime Prevention (SCP).

This chapter also describes effective design and policy solutions used in the transit environment to reduce the incidence of crime and passenger fear.

6.1 Foundation of Environmental Crime Prevention

In the United States, crime prevention efforts, particularly for RFGS, have not always recognized the importance of facility design and maintenance. Traditionally, crime prevention has been based on the assumption that efforts to understand and control crime must begin with the offender. Therefore, through the 1960s, crime prevention strategies consisted primarily of deterrence and the rehabilitation of the individual.

¹² Clarke, Ronald V. Preventing Mass Transit Crime, Vol. 6. Criminal Justice Press, New York, 1996, pg. 2.

During the 1970s, however, new approaches to crime prevention changed these traditional assumptions by focusing not on the individual who committed the crime, but on the *context* in which the crime was committed. This shift removed the burden of trying to predict crimes to providing an opportunity for deterring crimes within the transit environment itself.

Based on this new understanding, crime is now perceived as an activity in which criminals “go to work,” trying to get the most, with the least amount of effort, while subjecting themselves to the least amount of risk. In the transit environment, crime requires the convergence of three elements:

- A motivated offender,
- A suitable target, and
- The absence of a capable guardian.

This understanding avoids speculation regarding the motive of the offender, and directs RFGS efforts to four distinct classes of crime prevention activities:

- Increasing the difficulty of committing crimes,
- Increasing the perceived risks,
- Reducing the rewards associated with criminal acts, and
- Reducing the rationalizations that facilitate crime.

6.2 Principles of Crime

Before discussing specific characteristics of CPTED and SCP, an understanding of the principles of crime as they apply to the transit setting is helpful. Crime relies on the following three principles:

- Participant Principle,
- Behavior Settings Principle, and
- Flow Principle.

6.2.1 Participant Principle

Crime requires the following three elements:

- Motivated offenders,
- Suitable victims, and
- The absence of intervening forces to prevent criminal activities.

For example, a drug deal in a transit facility is dependent upon a buyer, a seller, and the absence of transit police or other personnel to prevent the sale.

6.2.2 Behavior Settings Principle

Social control concepts suggest that communities are divided into various behavior settings: slices of time and place where various activities occur, whether legal or illegal, and orderly or disorderly. A behavior setting contains three distinct features:

- Time,
- Place, and
- The activity that occurs there.

In the transit environment, several behavior settings might be present. For example, a RFGS station may consist largely of settings that generate a great deal of social control, such as passenger platforms, stores and vending carts, and information booths. Within this legitimate setting, however, there may be an area that fosters illicit behavior, such as a bathroom or a remote waiting area.

6.2.3 Flow Principle

The Flow Principle applies to crime and disorder within a given behavior setting. Transit stations attract large numbers of people, usually carrying cash and other belongings that can be readily stolen. As people flow from one behavior setting to another, a legal behavior setting can exist next to an illegal behavior setting in space and time.

The order, or flow, within a transit setting is divided into two categories:

- Channeling, and
- Chunking.

Channeling provides a distinct advantage in the transit environment by creating more public space and encouraging a smoother flow for people. Chunking divides space into smaller units creating “nooks and crannies” which provide potential offenders with a physical space to commit a crime.

6.3 Crime Prevention Through Environmental Design and Situation Crime Prevention

The three principles of crime described above are central to both CPTED and SCP. CPTED advocates that proper design and effective use of the physical environment contributes to a reduction in both the fear and incidence of crime, and to an improvement in quality of life. CPTED focuses solely on design and use of a particular space; the creation of an environment that does not tolerate crime. For example, CPTED solutions, such as improved access control, better lighting, and architectural structures that effectively move passengers through facilities, do not address other environments that may support crime (social, organizational, or legal).

SCP uses CPTED design solutions and integrates them with management policy and legal/prosecution measures. For example, to resolve pay phone fraud at major RFGS terminals, an SCP solution would involve both surveillance/environmental controls, and the provision of “call trace” facilities to private telephone subscribers. CPTED provides a general framework for the design and operation of RFGS facilities, while SCP provides the tools to address specific criminal occurrences.

Both CPTED and SCP create physical and social conditions through environmental design in selected environments aimed at reducing both crime and the fear of crime. SCP typically addresses physical measures, modifies existing operating procedures, and addresses the specific nature of crime.

While CPTED is invaluable in the initial design of the RFGS environment, SCP offers many advantages during the operational life cycle of the RFGS. As opposed to other methods of crime prevention strategies that may require many years to produce a reduction in crime (e.g., Operation Head Start that intervenes in lives of three- to four-year-olds), SCP efforts reduce crime relatively quickly after intervention. These preventive measures are focused on reducing opportunities for specific forms of crime. Solutions for a particular crime in a particular situation, however, will not necessarily work in other situations for other types of crime. Therefore, identifying and designing appropriate measures based on an accurate understanding of the success of offenders is essential.

SCP provides a scientific framework for practical use. This framework relies on a standard action research methodology consisting of five sequential stages:

- Collecting data relevant to the specific crime problem;
- Analyzing the specific situational conditions that facilitate such criminal activity;
- Analyzing the costs and benefits associated with methods of deterring such criminal activity;
- Implementing the most promising countermeasure; and
- Monitoring and evaluating the results of the particular implementation plan.

SCP addresses the specific issues of transit security through this methodology by focusing on the reduction of opportunities and the removal of “negative space.” Opportunity refers to the situational components of the context of the crime, rather than those structures of opportunities that underlie the motivation of the offender. Negative space refers to those spaces that might inherently promote illegal or illegitimate activity.

Advocates of CPTED and SCP techniques recognize the possibility of displacement, or the movement of criminal activity that would occur in one location to another location as a result of crime prevention measures. In the transit setting, this issue may be a political deterrent to RFGS expansion.

Theoretically, environmental criminology suggests that the offender “chooses” to commit a crime based upon the notion of receiving the greatest reward for the least amount of effort. Based on this theory, a petty shoplifter will not, in all likelihood, turn to mugging or rape. Ronald V. Clarke proposed a positive rebuttal to the displacement concern. He suggests that reducing crime in one place may actually lead to reductions in another.¹³

¹³ Clarke, Ronald V. Preventing Mass Transit Crime, Vol. 6. Criminal Justice Press, New York, 1996

6.4 Using Crime Prevention Through Environmental Design and Situation Crime Prevention to Reduce Crime

To classify SCP solutions in an easy-to-understand framework, Clarke and others have developed the following matrix to categorize the sixteen techniques for SCP:

Sixteen Opportunity-Reducing Techniques¹⁴			
Increasing Perceived Effort	Increasing Perceived Risks	Reducing Anticipated Rewards	Inducing Guilt or Shame
1. Target hardening	5. Entry/exit screening	9. Target removal	13. Rule setting
2. Access control	6. Formal surveillance	10. Identifying property	14. Stimulating conscience
3. Deflecting offenders	7. Employee surveillance	11. Reducing temptation	15. Controlling disinhibitors
4. Controlling facilitators	8. Natural surveillance	12. Denying benefits	16. Facilitating compliance

Table 9: Situational Crime Prevention

Each of these techniques is discussed below.

6.4.1 Increasing Perceived Effort

Techniques in this category focus on the rationale behind environmental criminology. If an offender must exert an increased amount of effort to commit the crime, the crime is unlikely to be committed. There are four categories for this method.

¹⁴ Ronald V. Clarke, Situational Crime Prevention: Successful Case Studies, (New York: Criminal Justice Press, 1996), p. 18.

6.4.1.1 Target Hardening

Target hardening involves using locks, safes, reinforced materials, or other physical barriers to obstruct the potential offender, thus reducing criminal opportunities. Examples include:

- Glass or plexiglass screens in token and information booths;
- Cages, covers, and shields to protect public RFGS property (clocks, safety devices, fare card equipment, etc.);
- Graffiti and vandal-resistant materials; and
- Landscaping and barriers to enhance visibility and direct passenger movement.

6.4.1.2 Access Control

Access control involves using mechanical or electrical systems to exclude potential offenders from designated areas and to prohibit offenders from performing specific crimes. Examples include:

- Fare gates or “fare only” areas;
- Access gates on parking lots and garages;
- Stand-alone lock systems (for employee areas); and
- Magnetic strip cards (for employee areas).

6.4.1.3 Deflecting Offenders

Deflecting offenders is a situational technique applied to “deflect” potential offenders away from crime targets. Examples include:

- Closing RFGS stations between 1:00 a.m. and 5:00 a.m.;
- Eliminating seating in stations/limiting seating on platforms;
- Limiting station entrances and exits; and
- Modifying pay-phones (reducing phone card fraud).

6.4.1.4 Controlling Facilitators

This technique involves placing controls on a range of crime targets, almost eliminating a possibility of the commission of the intended crime. Examples include:

- Caller identification (i.e., caller ID);
- Removal of pay-phones; and
- Monthly fare tickets.

6.4.2 Increasing Perceived Risks

In addition to increasing the effort to commit crime, which places a greater burden on the offender, increasing the perceived risks of the offender also helps to deter criminal activity. There are four categories for this method.

6.4.2.1 Entry/Exit Screening

Entry/exit screening methods are employed to increase the likelihood of detection of those who do not comply with RFGS regulations. Examples include:

- Introducing exact fare cards and automatic fare gate systems;
- Locating turnstiles directly in front of ticket/information booth agents; and
- Installing locks on train doors and passenger facilities to prevent multiple escape routes.

6.4.2.2 Formal Surveillance

The formal surveillance technique includes methods to furnish a deterrent threat to potential offenders. Examples include:

- CCTV cameras and recorders, linked to fully staffed monitoring facilities;
- Security guards;
- Police patrols;
- “Spot checking” for fare evasion;
- Intercoms and passenger call buttons, linked to monitoring facilities; and

- Passenger telephones, linked to monitoring facilities.

6.4.2.3 Surveillance by Employees

This technique suggests using employees, particularly those with positions involving public contact, to perform surveillance. Examples include:

- Security awareness training for transit personnel;
- Two-way radios for transit personnel;
- Station attendants; and
- Public address systems to enable employees to address observed activities.

6.4.2.4 Natural Surveillance

This technique uses “natural” surroundings to enhance vision and surveillance in RFGS facilities. Examples include:

- Increased lighting;
- Wide, open spaces and high, arched ceilings; and
- Clear doors between train cars.

6.4.3 Reducing Anticipated Rewards

Removing the reward, or the goal of the offender, also helps to reduce the opportunity for criminal behavior. The following categories present examples of this method.

6.4.3.1 Target Removal

This technique requires the recognition and removal of potential criminal targets. Examples include:

- Recessed light bulbs;
- Frequent trains;
- Off-hours waiting areas;

- No pay-phones;
- Clear signage; and
- Information booths, maps, and schedules.

6.4.3.2 Identifying Property

This technique encourages marking property or using signs to denote ownership. Examples include:

- Photo identification on monthly fare passes; and
- Photo identification on employee badges.

6.4.3.3 Reducing Temptation

This technique requires removing temptations that attract crime. Examples include:

- Eliminating corners, nooks, long passageways, and unused space;
- Improving visibility; and
- Improving lighting.

6.4.3.4 Denying Benefits

Similar to reducing temptation, this technique requires the denial of any associative benefits with committing a crime. Examples include:

- Rapid removal of graffiti and repair of vandalism; and
- Easy invalidation of stolen fare media.

6.4.4 Inducing Guilt or Shame

This SCP technique is designed to associate feelings of guilt and shame with the potential criminal activity and the offenders who commit crimes. For example, this category encourages posting signs and advertisements stressing the impact of crime on victims. Four techniques are presented below.

6.4.4.1 Rule Setting

This technique supports the introduction of new rules or procedures intended to remove any ambiguity concerning acceptable modes of conduct. Examples include:

- Drug-free zone markers;
- Regulation signs; and
- Posting penalties for fare evasion, smoking, etc.

6.4.4.2 Stimulating Conscience

This technique attempts to stir “second thoughts” in the minds of potential criminals. Examples include:

- “Shoplifting is stealing” signs; and
- Advertisements campaigns.

6.4.4.3 Controlling Disinhibitors

This technique requires the prohibition of agents, such as alcohol and drugs, used to undermine social inhibitions. Examples include:

- Anti-alcohol and drug rules; and
- No loitering rules.

6.4.4.4 Facilitating Compliance

This technique reduces opportunities for crime by supplying conditions for compliance with rules and regulations. Examples include:

- Clearly marked trash bins;
- Graffiti boards; and
- Community art programs.

6.5 Implementation Periods of Situational Crime Prevention

SCP techniques can be used during the following three RFGS life cycle phases:

- System design,
- Renovation, and
- In response to specific crimes.

SCP techniques are most readily and cost-effectively employed when included in the design of an RFGS facility or vehicle. The design, maintenance, and management of WMATA provides an excellent example of “designing out crime.” Documented studies indicate that WMATA’s low crime rates, in comparison to similar RFGS, can be attributed to the system’s design. WMATA’s entrances, exits, and pathways were designed with the following attributes:

- Clear pathways and stairs to alleviate the problem of criminal activity in dark corners (like those found in many older subway stations);
- Enhanced lighting to remove shadows (which are sometimes responsible for passenger fear);
- Installation of CCTV’s to provide greater visibility, thus deterring criminal activity;
- A farecard system which prevents fare evasion; and
- Training transit police and personnel to deter disorderly conduct.

WMATA scores high on visibility, and the CCTVs assist this open environment by optimizing employee and natural surveillance capabilities. The following table describes these features.

Security by Design WMATA	
Area Addressed	Preventative Efforts
Supporting Columns	<ul style="list-style-type: none"> • Decreased number to reduce cover for criminals
Entrances, Exits, and Pathways	<ul style="list-style-type: none"> • Designed long and straight pathways, stairways, and escalators • Eliminated corners to reduce shadows and decrease transient occupation
Lighting and Maintenance	<ul style="list-style-type: none"> • Used recessed lighting to reduce shadows and enhance the environment • Excluded public bathrooms in design to eliminate undesirable activity • Recessed walls and bars installed in front to discourage graffiti • Placed litter bins on platforms • Implemented policy directing the cleaning of graffiti and repairing of vandalism within 24 hours of incident
Security Devices	<ul style="list-style-type: none"> • Installed CCTVs on the end of each platform, deterring criminals • Installed kiosks at entrances to platforms • Installed passenger-to-operator intercoms • Installed blue light boxes with emergency phones every 600 feet
WMATA Transit Police and Personnel	<ul style="list-style-type: none"> • Added formal surveillance of facility • Required to enforce all facility rules • Trained to report all maintenance problems

Table 10: Security by Design

The second phase of SCP implementation occurs during RFGS renovation. Though not as cost effective as SCP methods applied during the time of original construction, major reductions in both crime and passenger fear may result.

Although New York City's Port Authority Bus Terminal (PATH) is not a RFGS, as defined by FTA's State Safety Oversight Rule, modifications of this system provide an excellent example of this SCP approach. During terminal renovation, in an effort to ease access throughout the station, movement control issues were addressed. Entrances and exits were re-designed to control passenger flows, as were stairways and escalators. Niches and corners were removed to eliminate transient populations inhabiting these areas. Walls were removed to open up closed spaces, recessed doors were moved forward, and some stairways were blocked off entirely.

Further, since the restrooms fostered illicit activities, the following restroom renovations were conducted:

- Attendants were deployed, providing informal security;
- Ceiling panels were secured;
- Lighting was improved;
- Nooks were removed; and
- Retail stores were set up in close proximity.

In addition to the above renovations, an emphasis was placed on the maintenance and sanitation of the facility. Broken Windows, the landmark article published by James Q. Wilson and George Kelling in 1982, details ways in which disorder and negligence in an environment lead to deterioration and contribute to increased criminal activity. PATH, in line with this hypothesis, realized the importance of the following:

- Clean floors,
- Clean elevators, and
- Enhanced lighting.

The following table presents SCP techniques implemented by PATH during the renovation.

New York City's Port Authority (PATH) Bus Terminal Renovations

Problem Area	Modification	Effect
Entrances, Escalators and Crowd Flow	<ul style="list-style-type: none"> • Modified doors for easier entrance and exit • Arranged better stairway and escalator flow pattern 	<ul style="list-style-type: none"> • Improved movement and reduced transient population at entrances
Nooks, Columns, and Spaces	<ul style="list-style-type: none"> • Closed in areas between stairwells and columns • Closed unneeded areas • Renovated the food court • Kept stairs away from street entries • Centralized ticketing • Put merchants in key areas • Filled empty spaces • Removed benches • Removed low brick walls • Implementation of technology to stop phone hustlers • Increase supervision with police officers 	<ul style="list-style-type: none"> • Reduced number of transients • Reduction in patron fear • Facilitated natural social control • Eliminated hiding spaces • Discouraged transients from loitering in facility
Restrooms	<ul style="list-style-type: none"> • Secured ceiling panels • Improved lighting • Straightened walls • Removed nooks • Added attendants • Added automatic controls for sinks, toilets and hand drying machines • Installed corner mirrors 	<ul style="list-style-type: none"> • Eliminated transient problem • Increased visibility • Increased security • Reduced patron fear • Improved sanitation
Maintenance and Sanitation	<ul style="list-style-type: none"> • Improved floor cleaning process • Improved lighting • Rehabilitation of elevators 	<ul style="list-style-type: none"> • Improved the appearance of the facility

Table 11: New York City's Port Authority Bus Terminal Renovations

As a result of SCP’s flexibility, techniques of implementation are also effective in response to specific crimes. Target hardening at NYCT stations in the 1980s provides an example of the many SCP techniques employed in response to specific crimes. Select NYCT stations were experiencing the following fare evasion problems:

- Walking through unmanned “slam” gates to enter the paid-fare area;
- “Backcocking,” or turning back the arms of the turnstile, and squeezing through;
- Vaulting over waist-high turnstiles or low fence railings; and
- Using slugs at stations with antiquated mechanical turnstiles.

The following table describes the changes implemented at the 110th Street and Lexington Avenue station in the Harlem District of upper Manhattan.

Changes at NYCT 110th Street and Lexington Avenue Station
<p>To reduce fare evasion, NYCT implemented the following changes:</p> <ul style="list-style-type: none">• Installed floor-to-ceiling railings,• Replaced older token devices with modern electronic models, and• Installed clerk-controlled “high wheel” turnstiles.

Table 12: Changes by NYCT to Reduce Fare Evasion

7. Security Technology in the Transit Environment

As discussed in the previous chapter, the potential exposure of passengers and employees to crime necessitates security considerations throughout the design, construction, and operation of an RFGS. Security technology plays a key role in the following:

- CPTED and SCP techniques, and
- RFGS operations -- assisting transit police and security personnel in deterring crime, responding to incidents, and reducing passenger fear.

Security technology can be installed either at the time the RFGS is being constructed, or after the facility has been in operation. In some cases, security technology has been introduced without appreciation for the unique environmental attributes of individual RFGS facilities. Ideally, security technology should be integrated into the security design process prior to RFGS construction. An integrated approach, comprised of CPTED/SCP techniques and appropriate security technology, offers the best opportunity for crime prevention.

Successful security technology utilization in the transit environment has three key requirements:

- An understanding of the types of crimes that occur and may occur on the system,
- A technology evaluation process that identifies needs based upon actual and likely crime patterns, and
- A focus on technology integration to achieve increased efficiency.

To support Oversight Agency personnel in reviewing and monitoring RFGS security programs, this chapter provides an overview of the types of security technologies used in the transit environment. Security technologies presented in this chapter are categorized into four distinct groups:

- 1. Access Control Systems (ACS).** Monitoring entrances and exits to various areas/facilities (e.g., electronic access control systems, locks, motion detectors, etc.)
- 2. Closed Circuit Television (CCTV) Surveillance.** Establishing surveillance/visibility to enhance monitoring of an area/facility (e.g., cameras and networks)
- 3. Emergency Communications Systems (ECS).** Providing effective communication (e.g., “blue-light” police phones, emergency signs, passenger intercoms, etc.)
- 4. Security Materials Technologies.** Using technological materials or physical features that are difficult to abuse or harm (e.g., protective seat coverings, operator shields, sacrificial coatings, etc.)

The four security technology groups are discussed below.

7.1 Access Control Systems

Access Control Systems (ACS) manage facility entrances and exits, including restricted areas. They improve security measures by restricting entrance to those persons authorized to enter the system. Selecting the appropriate ACS depends on the following criteria:

- Type of facility to be secured, its use, and the level of security required,
- Number of entrances/exits to be controlled,
- Amount of time permissible in the controlled area, and
- Type of user.

ACS provide RFGS with a variety of functions including:

- Control over facility entry/exit,
- Alarm monitoring and response,
- Improved emergency management capabilities,
- Elevator control,
- Parking lot access control,
- Police/security guard patrol tracing and auditing, and
- Audit functioning to trace patterns of access/egress from facilities.

The following ACS technologies are discussed in this section:

- Electronic access control devices,
- Intrusion detection systems, and
- Motion detectors.

7.1.1 Electronic Access Control Systems

Over the last decade, electronic ACS technology has improved significantly in efficiency and reliability. Electronic ACS require databases to store and manipulate information. Improved

database capabilities offer RFGS operators a variety of functions that can be administered from a personal computer. In particular, employee badge identification systems, vehicle management systems, and incident response systems have been tied to ACS technology with improvements in efficiency, reductions in crime and internal theft, and increases in emergency management capabilities.

When electronic ACS technology was first introduced, access card reader and Personal Identification Number (PIN) entry systems operated with limited memory and flexibility. Cards were coded for entry, but levels of access could not be distinguished. Operating software was not fault tolerant: if one sector of the database or hardware component failed, the entire system shut down. Power supplies to wall panels and card readers were difficult to wire and maintain, and voltages differed from other wiring specifications in use at the facility. Successful ACS implementation required extensive customization from the manufacturer to achieve the desired level of performance. The necessary use of proprietary software increased ACS lifecycle costs by as much as 100 percent.

Recent innovations in ACS technology include:

- Improvements in off-the-shelf distributional database software,
- The introduction of the micro controller (which enables fault tolerance and independent decision-making for access denial and alarm triggers), and
- The development of miniature micro controllers that can be housed in the card reader panel and do not require a separate wall panel and wiring.

In addition, CCTV and “smart” building management systems have revolutionized ACS capabilities. Software innovations allow electronic ACS technologies to be integrated with Building Management Systems (heating, ventilation, air conditions, and lighting), Fire Detection and Suppression Systems (alarms, emergency access doors, roster of personnel in the building in the event of fire), and CCTV Surveillance Systems.

Integration also provides the opportunity to implement an alarm paging system, through which the operating system notifies police and security personnel of unauthorized access, systems failures, and unusual occurrences with alarm messages designed to distinguish priority response. Finally, Computer-Aided Design (CAD) and Computer-Aided Dispatch (CAD) technologies allow RFGS to use computer-generated maps of trackway, rail yards, fans, and city streets to communicate effectively in an emergency. Some RFGS are working toward centralization of tunnel fire, communications, and ventilation systems on one computerized system.

The importance of ACS as the “backbone” of the electronic security system makes the choice of ACS technologies in the RFGS environment especially critical. Efficiencies in system integration depend on subsystem relationships. The electronic ACS provides the foundation for the integrated system and serves as the primary monitoring system for all subsystem relationships. In this capacity, the electronic ACS must provide for both current and future security needs of the RFGS.

RFGS utilize three basic electronic ACS devices to ensure authorized access to stations and equipment, passenger areas, parking lots, and non-revenue buildings and support facilities, including:

- **Magnetic Swipe Card Readers.** Used to provide access to parking lots and garages, to restricted areas in revenue collection facilities, and to support employee photo badging systems. This technology is also used for vehicle management, or the tracking of company vehicles as they are used by system employees.
- **Alphanumeric Code Entry Systems.** Uses a PIN punched into a touch-sensitive alphanumeric keypad. PIN entry systems are used primarily in support facilities, machine shops, and inventory control rooms. A simple four digit PIN entry system provides thousands of possible combinations to be utilized by employees with differing levels of access. Both magnetic card readers and PIN entry systems provide full audit capabilities to trace employee entrance/exit.
- **Personal Feature Identification (PFI)/Biometric Systems.** Biometric identification devices are relatively new to RFGS facilities. These devices are installed with a magnetic swipe card reader to ensure a further level of security to prevent unauthorized access. Generally, these devices are used only to secure key restricted areas.

Example

In the near future, a Biometric Identification Device will be in use at the Bay Area Rapid Transit (BART) District in San Francisco, California. BART's biometric identification device will be installed with a Magnetic Swipe Card Reader to ensure a further level of security. The construction of BART's airport station with air side access at the International Terminal of the San Francisco International Airport (SFIA) necessitated the use of this system.

The BART system will utilize advanced computer and electrical equipment supported by fault tolerant software. The system will be controlled through a distributed database, and will be installed at all restricted access points, defined according to Federal Aviation Administration (FAA) regulations.

This Biometric Identification Device will use the following steps:

1. The access card containing a magnetic strip is presented at the card reader.
2. The reader transmits the number associated with the card to the remote panel database.
3. If the number is found in the database, it is conveyed to the biometric identification device.
4. If the number is not found in the database, a request is sent to the micro controller to determine the acceptability of the card.
5. If the request is granted, the micro controller downloads the record information into the remote panel database.
6. If the request is not granted, access is denied.
7. The biometric identification device compares the hand data to the appropriate hand template.
8. If a match is confirmed, the reader sends verification to the remote panel database.
9. At this point, access is granted.
10. If a match is not found, access is denied and the security monitoring post is notified.

Table 13: Bay Area Rapid Transit Access Control System

The introduction of fiber optic cable for camera linkages along a Local Area Network (LAN) has significantly improved the ease with which CCTV systems can be connected to ACS electronic devices, increasing monitoring capabilities.

Example

Amtrak is piloting a program combining cameras, electronic ACS, and intrusion detection systems to alert security monitoring personnel to the presence of trespassers or obstacles on the right-of-way and to issue photo citations to automotive violators. In addition, this integration provides the opportunity to implement an alarm paging system, through which the operating system notifies police and security personnel of unauthorized access, system failures, and unusual occurrences with alarm messages designed to distinguish priority response breaches.

Table 14: Amtrak Access Control System

7.1.2 Intrusion Detection Systems

Intrusion Detection Systems are most often used on Automatic Train Control (ATC) systems, commuter rail, and freight railroads. The following types of sensors are used to identify obstacles on tracks and unauthorized access:

- Vibration,
- Weight-loading,
- Electronic, and
- Beam.

Vibration sensors are triggered when extreme shaking causes detectable movement. Weight-loading sensors detect the presence of weight in excess of a pre-specified amount programmed into the sensor. Electronic sensors are triggered when unauthorized access causes a lock or rail system component to disassemble without authorization. These sensors operate through the advanced transmission of radio or electronic signals over a computerized ACS. Once the alarm is activated, it is monitored by this system.

Intrusion detection sensors are improving in reliability. Previous problems included:

- Hyper-sensitivity to vibration and weight,
- Electromagnetic interference with the transmission of radio waves in tunnels,
- Operating failures, and
- Software errors.

Newer generation sensors and operating systems have been modified specifically for the transit environment.

Example

Pilot programs are being considered by several RFGS to use intrusion detection systems to safeguard patrons with visual impairments. Such a program entails the installation of edge detection systems that operate using radio or electronic transmissions to notify disabled patrons that they are near the edge of a RFGS platform.

In addition, manufacturers of intrusion detection systems are marketing a trespassing identification system to be used at rail grade crossings located near schools and busy intersections.

Table 15: Intrusion Detection Systems

7.1.3 Motion Detectors

Motion detectors may be installed in RFGS station facilities, administrative buildings, and maintenance shops to control the use of lighting and building control systems. When movement is detected, these devices are automatically activated. In revenue collection facilities, inventory storage facilities, and rail yards, motion detectors are connected to an alarm system. In this configuration, when motion is detected an alarm is transmitted electronically to a centralized monitoring device. Generally, motion detectors used in both these capacities are useful in the transit environment.

Though many RFGS personnel support the use of motion detectors, this technology is not problem-free. Motion detectors may be triggered too easily, causing alarm at the slightest disturbance. In addition, depending upon the level of integration of motion detection technology with other alarm systems, this technology may be easily disabled.

7.1.4 Other Systems to Control Access

7.1.4.1 Stand-alone Lock Systems

Manually operated locks are commonly used to secure RFGS stations, restrooms, and many support facilities. The cost-effectiveness of this particular approach ensures that it is the most popular method of access control. Manually-operated locks are often referred to as "stand-alone security devices" and can be placed into four basic categories:

- Pin and tumbler (the key lock, which because of its simplicity, cost, reliability, and acceptance is the most popular method for securing a door in the transit environment),
- Combination locks (moveable dials with a series of disk shaped tumblers, used to secure gates, cabinets, storage facilities, tool storage containers, power substations, wayside facilities, and doors),
- Keypad/Push-Button Locks (numbered push-buttons must be pushed in the right combination to open the lock -- used for access to certain restricted facilities, restrooms, and storage areas), and
- Cardkey readers (battery operated devices which read cards encoded with magnetic stripes; distinct from an electronic magnetic swipe card reader in that it is not connected to an operating system and must be managed manually at the unit -- used primarily in the transit environment for administrative access restrictions and inventory access control).

Older RFGS, in particular, rely on stand-alone security devices to limit access to a significant portion of transit facilities and equipment. Key and Code Control programs are administered to limit unauthorized access.

7.1.4.2 Turnstiles

Manually operated or motor-driven turnstiles are used in the RFGS environment to count people, restrict entry until another function is complete (such as verification of an authorized card key), and allow exit but not entrance. When combined with an electronic ACS (such as a keypad or swipe reader), turnstiles can rotate in such a manner that only one person can pass through the opening in each cycle of operation. Turnstiles are used in four basic configurations in the RFGS environment:

- Operation in a single direction only (common for exits on train platforms),
- Operation in both directions, to ensure that only pedestrians and no equipment move through the opening (used for entrances into RFGS administrative facilities),
- Free exit, with an electronic ACS (swipe card reader/ PIN system) on the entrance (commonly used in parking lots, where people can freely exit, but must have an access code to prevent unauthorized entry; also used for fare collection purposes with tokens or magnetic stripe cards), and
- Electronic ACS on both turnstile entry and exit (used when turnstiles separate two secure entrances, such as in a revenue collection area or a police holding facility).

Turnstiles are commonly waist high for admissions and crowd control purposes. High security turnstiles, used outdoors to control pedestrian access into RFGS stations, may be as tall as seven feet. Turnstile materials range from galvanized metals to match the look and durability of a fence line, to stainless steel and anodized aluminum.

7.1.4.3 Revolving Doors

A revolving door differs from a turnstile because it separates two distinct environments, such as an outside environment to an inside environment (e.g., a climate-controlled building). A revolving door, set at six (6) Revolution per Minute (RPM), permits access to as many as twenty-four people a minute in both directions. Use of a card reader generally reduces this number to twenty people per minute due to reader malfunctions and reader system rejections. Revolving doors can be used in the following settings:

- Rail station entrances/exits, and
- Entrances/exits to administrative facilities.

Revolving doors are often described as the only door that is both open and closed, providing both access and a barrier for heating and air conditioning. Revolving doors can be used for interior applications in the transit environment, but, as they are more expensive, generally they are selected for climate-control capabilities only. Turnstiles are more commonly used to control passenger access to RFGS service.

7.2 Closed Circuit Television Surveillance Systems

In recent years, CCTV and Closed Circuit Video Recording (CCVR) have become increasingly popular in the security industry. Using CCTV and CCVR significantly reduces manpower requirements; however, this type of surveillance is only as effective as the person monitoring it. Further, in purchasing CCTV equipment, an RFGS's specific needs must be considered. Successful acquisition of CCTV and/or CCVR equipment requires both a clear knowledge of the area to be monitored and expert advice in recommending a system.¹⁵

Initially used to monitor isolated spaces and off-hour waiting areas at transit stations, CCTV and other new-generation digital technology are proving an effective surveillance measure for both RFGS facilities and vehicles. Fixed focal length and zoom lenses, in both black-and-white and color, are used for indoor applications. While lighting levels have limited cameras to black-and-white in most outdoor applications, color is now available and growing in popularity. Micro-cameras can be installed in ticket vending machines, in passenger alert devices, and on-board transit vehicles.

Pole-mounted pan/tilt telephoto cameras with infrared spotlights can monitor park-and-ride lots, even in low-light situations. Fiber optic cable and digital technology allow images from multiple locations to be transmitted via phone lines to computer driven monitors for digital storage. With all of these options available, however, CCTV surveillance can be over-promoted as a solution to security problems. While it is becoming a more important component of transit security programs, it must be successfully integrated with transit and police operations if it is to yield maximum benefit.

7.2.1 CCTV Utilization

Though CCTV technology is used extensively in the transit environment, enthusiasm for the technology varies. For some RFGS, CCTV technology supplements transit operations in a number of important ways, including:

- Improving customer service,
- Improving detection and response to fare evasion,
- Preventing vandalism and graffiti,
- Improving assistance for passengers with disabilities,
- Improving emergency response and management activities, and
- Increasing patron confidence in RFGS security.

¹⁵Neil Cumming, Security (Boston, MA: Butterworth-Heinemann, 1992), pg. 177.

For other RFGS, CCTV is useful, but overrated because it:

- Requires a high level of manpower for maintenance and monitoring,
- Requires considerable and expensive integration with other security and communications technologies (e.g., passenger intercoms, public address systems, alarm control panels, etc.), and
- Creates the threat of legal action from patrons, or perpetrators, seeking to document crimes occurring in transit facilities.

Many RFGS use CCTV technology in rail stations, restricted areas, parking lots, and elevators. Other RFGS use CCTV on vehicles. MBTA, Maryland MTA, Houston Metro, and SEPTA are examples of systems that have recently participated in a pilot program to install cameras on transit vehicles.

Table 16 identifies the applications of CCTV technology in the transit environment.

Application	Description
Monitoring of Revenue Facilities	Use of CCTV to view stations/terminals. Camera feeds may be directed to a centralized (dispatch) location or to a localized monitoring area (e.g., Station Agent's Booth)
Monitoring of Vehicles	Use of CCTV to monitor activities on rail vehicles; to record accidents/incidents; to promote patron perception of security
Incident Management	Camera feeds to dispatch room, central control, or station manager's booth to enable personnel monitoring CCTV to call staff to respond to an incident; to enhance accurate description of incident; to provide a video record
Legal Evidence	Continuous, random, or emergency monitoring of facilities or vehicles for use as evidence in legal proceedings
Customer Service	Visibility of passengers (e.g., at customer assistance phones) to assist patrons more efficiently; to identify patrons with problems; to identify mechanical failures
Crowd Control	Use of cameras to alert dispatch of crowd control problems on platforms or in other areas of facilities
Security of Problem Areas	Use of CCTV in difficult-to-patrol areas such as elevators or parking lots to deter criminal activity; to support police operations; to enhance incident response
Visibility for Operators	CCTV and monitors are used as a safety feature, providing rail operators with additional visibility of platform areas prior to door closure or vehicle pull-in/pull-out
Special Police Operations	Portable or mounted cameras used to assist undercover police officers in observing facilities; identifying perpetrators; documenting activities
Risk Management	Verification of insurance claims against the RFGS, typically resulting from (alleged) accidents
Vehicle Routing	Use of CCTV cameras on bridges or highways to identify traffic patterns, accidents, and delay patterns
Non-revenue Areas	CCTV utilized for monitoring non-revenue areas such as cash counting areas, power sub-stations, storage rooms, and administrative facilities

Table 16: Closed Circuit Television Applications in the Transit Environment

7.2.2 Cameras and Networks

Generally, RFGS with the greatest appreciation for CCTV technology are the most committed to interfacing CCTV with other security systems. Several examples are presented below.

EXAMPLE

MARTA uses a cable network of black-and-white cameras to provide coverage for rail stations. Cameras monitor points of access, fare arrays, patron waiting areas, restrooms, platform ends, and escalators/elevators. These cameras feed into centralized dispatch rooms, which also receive feeds from ACS, fare card readers, mechanical indicators, fire alarms, passenger intercoms, and other security/safety technologies.

Dispatchers answer patron questions; identify fare evaders; communicate through passenger intercom systems; monitor the anti-passback feature on the fare card reader; address mechanical malfunctions in escalators/elevators and fare turnstiles; provide assistance for patrons with disabilities; dispatch police for quick response to incidents; and provide police with a visual record of incidents by providing a VCR record.

Table 17: MARTA Closed Circuit Television System

EXAMPLE

At WMATA, black-and-white CCTV cameras feed into Station Agents' booths at most stations to improve station management activities. This technology allows Station Agents to:

- Identify mechanical problems with elevators and escalators,
- Identify patrons in trouble,
- Dispatch police, and
- Monitor ACS.

Camera use is localized, and generally used for monitoring purposes only. An advanced CCTV system is used, however, to ensure security of the revenue collection facility. This system consists of approximately forty cameras, fixed and pan/tilt/zoom, located both indoors and outdoors and wired to a single distributions network system to identify unauthorized access to the facility and to monitor traffic patterns around the facility. Advanced multi-plexing and video recording features support this CCTV technology.

Table 18: WMATA Closed Circuit Television System

EXAMPLE

BART is installing a fiber optic CCTV system for stations along its new extension rapid transit lines (most CCTV networks in transit use coaxial cable). This technology will utilize a distributional system that connects all CCTV cameras through a Local Area Network (LAN) so that any location on the LAN can access real-time video from any camera on the network. Signals are transmitted to the LAN over fiber optic cables. This system will be connected directly to BART's Central Control, with feeds available at the individual stations as well. This CCTV surveillance system will allow a dispatcher at a remote console to assess a given situation and dispatch the appropriate personnel to any incident. In an emergency situation, multiple BART officers can be informed of the situation by CCTV assessment. Videotape can also be recorded off any camera on the LAN.

Table 19: BART Closed Circuit Television System

Standard technical criteria for camera placement have not been developed; however, many RFGS recommend identifying camera and monitoring locations prior to purchasing CCTV technology. The physical requirements of implementing the technology and varying environmental conditions can have a significant impact on the operational capabilities of the equipment and its effectiveness. These impacts should be assessed before implementation.

Most RFGS using CCTV technology to support station operations place cameras in the following locations:

- On one or both sides of restricted access doors,
- In emergency stairwells and on emergency exit doors,
- On turnstiles, ticket vending machines, and Add Fare machines,
- On passenger intercoms and passenger courtesy phones,
- At opposite ends of station platforms for full line-of-site view,
- In/on elevators,
- At the top and bottom of escalators/stairs,
- On restroom doors, and
- On train doors and platforms, to assist train operators with door closings.

In parking lots and garages, CCTV technology may be used in the following locations:

- On entry/exit lanes,
- On attendant booths,
- By elevators in parking garages,
- On courtesy phones/passenger intercoms,
- Mounted on high poles or roosts to provide a full view of parking lots, and
- In parking garage stairwells.

The following list identifies some of the locations for CCTV in restricted areas:

- On entry and exit doors from administrative facilities,
- On one or both sides of restricted doors,
- Throughout cash-counting facilities,
- Posted on mounts in rail yards, and
- Throughout maintenance facilities, especially in inventory control areas (in combination with motion detectors).

7.2.3 Housings and Accessories

In the RFGS environment, housings are required to protect camera and lens assemblies. Camera system housings are composed of aluminum, steel, or thermoplastic. Housings installed for indoor cameras in stations, terminals, and restricted areas generally provide two basic functions:

- Protection from dust, dirt, and excessive temperatures, and
- Protection from vandalism.

Many RFGS place aluminum or stainless steel rectangular housings over indoor cameras. These housings have glass or plastic faceplates for the camera lens, and must be mounted with the camera. The faceplate can be popped out for easy replacement in the event of vandalism/graffiti. This configuration affords only limited opportunity for vandalism or graffiti, and offers solid protection from the metallic dust generated by trains entering and leaving stations.

While this configuration has proved durable, it provides users of the station, terminal, or restricted area with a clear view of the camera direction. To improve the security of the camera/lens assembly, some RFGS, such as MARTA, have installed dome-shaped housings constructed of a combination of aluminum and shaded plastic. The dome encloses the entire camera/lens assembly as well as the camera mount, allowing cameras to move within the dome without detection. Many of MARTA's stations have both indoor and outdoor components, and the dome-shaped housings function well in this environment.

In addition, many RFGS use stainless steel or aluminum ducting to protect the cables and wiring used to support indoor cameras. The aluminum or stainless steel ducting makes severing the cables almost impossible, and also protects the cables and wiring from the environment within the station, reducing maintenance requirements.

Since cameras are not weatherproof or watertight, all outdoor camera applications require some type of housing for protection. Many RFGS use either the rectangular housing case or the dome-shaped housing case. Housing accessories, such as sun shields and heaters, are usually not required for an indoor application but must support all camera/lens assemblies used outdoors.

Heaters or heater assemblies are still a basic requirement for all outdoor applications, even in areas with warm climates. Heater or heater assemblies support outdoor camera surveillance by:

- Ensuring that the camera and lens are kept within the normal operating temperature range, and
- Protecting the faceplate of the housing from frosting or fogging, which usually occurs when sudden temperature changes occur between the interior of the housing and its surroundings.

7.3 Emergency Communications Systems

Most RFGS have a number of ECS in place to address issues of passenger and operator security and safety. ECS are used to deter serious crimes (often for assistance in cases of crimes against persons involving passengers or employees).

With the exception of Automatic Vehicle Locator (AVL) Systems, ECS technologies are not complex, and are simply variations of the telephone. When interfaced with CCTV surveillance, fixed post monitoring areas, and dispatch rooms, however, ECS significantly improves the RFGS's ability to respond to incidents in progress and increase passenger trust in the system's commitment to providing a secure environment.

Table 20 presents a list and a description of ECS technologies typically used at RFGS.

Emergency Communication System Technologies	
Automatic Vehicle Locator/Computer-Aided Dispatch (AVL/CAD) Systems	AVL assists emergency response units in locating vehicles quickly; CAD system prioritizes RFGS and police response for vehicles and ensures that radio silence is maintained
"Blue Light" Police Phones	These phones feed directly into municipal police departments; utilized primarily in parking lots
Emergency Call Boxes	These phones allow patrons to speak with RFGS personnel to request assistance
Emergency Signs on Vehicles	Sign displaying "Emergency -- Call Police" indicates a serious situation on-board vehicle and assists in notifying police when operator cannot communicate via radio
"Holdup" Alarm Buttons	Push-button alarms utilized to send priority response message to police/RFGS personnel
Passenger Assistance Buttons	Signals RFGS personnel that a crime is in progress; provides priority response to patron in distress; most useful if interfaced with CCTV Surveillance System
Passenger Intercoms	Two-way intercoms utilized to enhance passenger and RFGS communications, to resolve fare disputes, and to receive emergency assistance
Public Pay Phones	Emergency call box installations are often not feasible. Adequate number of pay phones located near stations and in parking lots often serve the same purpose. Pay phones should be wired for out-going calls only
Silent Alarms	Use in conjunction with appropriate dispatch procedures which do not endanger operators or passengers and/or to call emergency units in event of a serious assault on-board vehicle

Table 20: Emergency Communication System Technologies

ECS are used both to improve RFGS response to security incidents, and to improve customer relations. Passenger intercoms, public pay phones, and passenger alarm buttons provide the following functions:

- Provide extra assistance for passengers with disabilities,
- Resolve fare disputes, and
- Assist patrons with car problems in parking facilities.

7.4 Security Materials Technology

Security materials technology can be used to support CPTED/SCP techniques and to protect other security technologies. RFGS generally use security materials technology to:

- Control environmental variables that determine the relationship between the station, vehicle, or building, and its users,
- Decrease graffiti and vandalism by using technological materials resistant to tampering and destruction, and
- Reduce isolation in pathways, stations/terminal, and parking lots through enhanced lighting systems and effective landscape design.

Security materials technology used by RFGS includes the following:

- Lighting,
- Landscaping control,
- Sacrificial coatings,
- Seating materials,
- Shelter panel materials,
- Fencing,
- Temporary barriers,
- Signage,
- Covers,

- Operator shields, and
- Security fasteners.

Security materials technology is effective for a number of reasons. Primarily, they take advantage of subconscious cues in space to direct user behavior. For this reason, technologies such as lighting systems and graffiti/vandalism sacrificial coatings may actually have a more significant impact on passenger perception than the much more expensive CCTV surveillance systems.

Further, these technologies, precisely because they are inexpensive, can be tailored to address specific and localized problems. For example, several RFGS have installed plexiglass covers over public information displays to prevent graffiti and to protect display materials. These displays allow passengers to find their way around the system more easily, and the clean, well-maintained appearance of the displays improves passenger confidence in system security.

Table 21 describes common materials selection and physical features used in RFGS facility designs.

Materials Selections and Physical Features in the Transit Environment		
Material Selection or Physical Feature	Function	Description
Lighting Systems	Increased visibility increases chances of apprehension; reduces isolation; and improves patron perceptions of security	<ul style="list-style-type: none"> • Halogen lighting (outdoors) • Florescent lighting (indoors) • Minimum lumination: 2-foot candles in outdoor parking lots/garages; 5-foot candles in outdoor stations/platforms
Landscaping Control	Clear lines-of-sight reduce isolation; ivy vines covering columns reduce opportunity for graffiti/vandalism; short bushes and flowers clarify pathways; and prickly bushes near walls and system entrances reduce likelihood of occupation by homeless population	<ul style="list-style-type: none"> • No landscaping in excess of three feet in height • Careful selection of vines to reduce water damage to columns/buildings • No poisonous flowers Prickly bushes with thorns located under leaves, not directly exposed
Sacrificial Coatings	Peel-off or wash-off coatings used to absorb graffiti and etching	<ul style="list-style-type: none"> • Plastic liners on windows to reduce etching • Coatings on walls and columns to improve graffiti removal • Careful selection of non-hazardous wash chemicals

Table 21: Materials Selections and Physical Features in the Transit Environment

Materials Selections and Physical Features in the Transit Environment (continued)		
Material Selection or Physical Feature	Function	Description
Seating Materials	Reduces the expense of seating replacement costs due to graffiti and vandalism	<ul style="list-style-type: none"> • Plastic seats with sacrificial coatings • Vinyl seat covers for easy washing/replacement • Removal of benches in shelters and stations • Concrete benches when seating is required
Shelter Panel Materials	Reduces the expense of vandalism/graffiti	<ul style="list-style-type: none"> • Pressed/honey-combed metal panels instead of glass • Plexiglass panels • Lighting installed at shelters • Removal/relocation of shelters
Fencing	Secures the perimeter of RFGS property; prevents trespassing; improves access control	<ul style="list-style-type: none"> • Minimum: chain-linked or wire mesh fencing, 6 feet in height • Topped with 2-foot rungs of barbed wire (if necessary) • Personnel entry gates on ACS system; rolling gates for vehicle entry secured with padlock and chain or ACS

Table 21 (continued): Materials Selections and Physical Features in the Transit Environment

Materials Selections and Physical Features in the Transit Environment (continued)		
Materials Selection or Physical Feature	Function	Description
Temporary Barriers	Direct passenger flow; deter access to isolated or hidden locations	<ul style="list-style-type: none"> • Concrete or plastic barriers placed in pathways, terminals, parking lots, and garages direct passenger flow/interrupt established crime patterns • Selection barrier material for fire resistance
Signage	Instruct patrons of RFGS rules and regulations; inform passengers of emergency procedures; notify potential criminals of likely apprehension for crimes committed on RFGS property	<ul style="list-style-type: none"> • Place signage to attract attention • Sacrificial coatings resist graffiti/vandalism • ADA compliance • Fire-resistance
Covers	Target-harden RFGS facilities; prevent theft; reduce vandalism/graffiti damages	<ul style="list-style-type: none"> • Wire mesh, plexiglass, or stainless steel covers protect station/terminal assets (e.g., clocks, displays, heaters, vents)
Operator Shields	Placed behind the operator to protect him/her from behind-the-back assaults	<ul style="list-style-type: none"> • Plexiglass or wire mesh composition ensures visibility while providing protection
Security Fasteners	Require non-traditional tools for disassembly	<ul style="list-style-type: none"> • Require fasteners in vehicles/equipment from vendors

Table 21 (continued): Materials Selections and Physical Features in the Transit Environment

8. Rail Fixed Guideway System Security Personnel Deployment

While environmental design techniques (discussed in Chapter 6) and security technology (discussed in Chapter 7) contribute substantially to RFGS security programs, deployment of police and security personnel is the primary method used by the majority of RFGS to protect passengers and employees. As discussed in previous chapters, the affected RFGS uses a variety of organizational and contractual structures to provide security, including sworn transit police forces, contracted local law enforcement, contracted non-sworn police, and local police.

RFGS police and security departments deploy *uniformed* and *undercover* personnel to:

- Maintain order on the system,
- Reduce or eliminate conditions that may support criminal activity,
- Respond to calls for service,
- Arrest offenders,
- Collect and organize legal evidence to support the conviction of offenders,
- Enforce RFGS rules and regulations,
- Protect RFGS property and facilities, and
- Manage the security program.

To some extent, the ability of RFGS police and security personnel to perform these functions depends on the authorities vested in them by local and state governments. For example, sworn RFGS police perform the full range of police functions, while non-sworn police perform fewer functions. Legislation in a number of states, however, has empowered non-sworn RFGS personnel to issue citations for code-of-conduct, quality-of-life, or fare-evasion violations. Using this authority, these personnel actively enforce RFGS rules and regulations.

Research indicates that a well-patrolled system, which effectively solves passenger problems, prevents crime (rather than responds only after incidents have occurred), and maintains order, enhances passenger perceptions of security and may increase ridership. Based on this research, which is an outgrowth of the experiences of the fourteen new RFGS constructed since 1970, most RFGS now commit the majority of their personnel resources to uniformed deployment programs, emphasizing visibility over apprehension.

While uniformed deployments do not rule out apprehensions, the primary goal of this tactic is to ensure a safe and secure environment by providing a sense of omnipresence to deter crime and reduce patron fear. Undercover deployment tactics, however, are still used to arrest offenders for specific types of violations. For example, many RFGS incorporate undercover tactics into specialized programs to address crimes such as automobile theft, drug dealing, graffiti, vandalism, and pickpocketing.

Uniformed Deployment	Undercover Deployment
<ul style="list-style-type: none"> • Maintains order • Affects passenger/employee perceptions • Deters crime 	<ul style="list-style-type: none"> • Apprehends, cites, and/or arrests offenders • Deters crime

8.1 Deployment to Reduce Passenger Fear

As indicated in Chapter 5, RFGS crime rates are considerably lower than crime rates in the municipalities served by these systems. Research indicates, however, that passenger fear deters RFGS ridership. “Unlike crimes committed in neighborhoods, homes, public housing projects, or other community settings where victims and offenders are often known to each other, crime victimization [on RFGS] almost always involves strangers, making it somehow far more frightening than crimes in other locales.”¹⁶

Therefore, RFGS management and police/security personnel must address both crimes occurring on their systems, and passenger fear. For example, communities perceiving a link between crime and the presence of an RFGS station will not support the expansion of the RFGS into their neighborhoods. Patrons who perceive the RFGS as dangerous will limit use of the system, especially during off-peak hours.

Transit-dependent populations, who must use the RFGS to travel to work and other locations, may become irritable, or even abusive, to system employees when travelling on routes perceived as unsafe. RFGS personnel who work in the transit environment must deal with the stressful consequences of disruptive behavior, fare evasion, intimidation, and public drinking on a daily basis. This environment significantly impacts RFGS personnel morale, absenteeism, management, and the quality of customer interaction.

Alleviating the fear of crime is difficult. During the 1960s and 1970s, citizen fear became an important factor governing the use of all public spaces, including public transportation. Since that time, significant research has been conducted to answer questions concerning the apparent lack of correlation between high rates of crime and citizen fear levels. In the early 1980s, researchers discovered that citizen fear is more closely correlated with perceptions of *disorder*

¹⁶ Vincent Del Castillo, *Fear of Crime in the New York City Subway*, (Ann Arbor, MI: University Microfilms International, 1990), p. 40.

than with crime. This finding is of particular importance to RFGS that routinely experience littering, vandalism, homelessness, and public intoxication -- all conditions that indicate disorder.

The problem of passenger fear is further complicated by the difficulty of evaluating the impact of various techniques and strategies on passenger perceptions. For example, RFGS police and security personnel can use modern crime data collection and analysis techniques to assess their success or failure in reducing the levels of actual criminal occurrences on RFGS property. Gauging the efficacy of fear reduction efforts, however, is far more challenging.

Many observations and experiences trigger public perceptions of disorder, and these triggers vary from passenger to passenger. Both disorder, and passenger response to disorder, are difficult to measure in quantitative terms traditionally used by police and security organizations to evaluate performance. In the RFGS industry, there are many assumptions about the effectiveness of various deployment strategies to reduce disorder and patron fear; however, RFGS police and security professionals have only limited measurable evidence with which to evaluate actual effectiveness in reducing fear.

This lack of quantitative information is further complicated by recent research findings which suggest that passenger fear is not only related to the level of disorder evident in RFGS facilities and vehicles, but also that the very nature of the RFGS service may promote passenger fear. RFGS stations serve a crowded mix of passengers. This interaction may produce feelings of vulnerability for some passengers. These feelings may cause passengers to avoid using public transportation or to behave in ways more difficult for RFGS operations and police personnel to manage.

Given the absence of a direct correlation between crime rates and passenger fear, considerable debate exists in the RFGS industry over how much emphasis to place on patron fear reduction. While RFGS must address passenger fear to maintain and increase ridership and to improve relationships with the localities they serve, they also must concentrate their limited resources to address patterns of actual crime occurring on the system.

8.2 Proactive Deployment

To reduce patron fear, many RFGS police and security departments have committed to deploying uniformed personnel. RFGS promote an enhanced uniformed police presence in facilities and vehicles to demonstrate a strong commitment to a secure environment. This relatively new focus on uniformed deployment constitutes a new brand of proactive policing. No longer focusing exclusively on response, many RFGS police and security departments are attempting to increase ridership and protect system property through interactive security programs focusing on the following:

- Customer interface,
- Community-outreach,
- Youth programs, and

- Directed teams designed to handle special problems (e.g., vandalism and parking lot crime).

Uniformed police and security personnel are deployed either at fixed posts or on patrols. When stationed at fixed posts, police/security personnel monitor activity in a given area, handle access control, supervise inventories and revenue collection, and provide public information. When on patrol, police/security personnel provide security throughout a given geographical area by responding to calls for service, providing a uniformed presence to deter crime, and conducting special operations targeting specific types of criminal incidents.

The following list identifies key uniformed patrol tactics used at affected RFGS:

- 1. Fixed Post.** Stationing police/security personnel at one area or station, with limited mobility and specific instructions to guide activities.

Fixed posts may be placed throughout an RFGS, including:

- Points of public access/egress,
- Near turnstiles,
- Near restrooms,
- At passenger boarding areas,
- Parking lots, and
- Administrative facilities.

Fixed posts are generally used in the transit environment to provide the following:

- Police/security personnel visibility,
- Access control,
- Distribution of information,
- Assistance for passengers,
- Monitoring fare payment, and
- Facility observation.

- 2. Random Foot Patrol within Post Area.** Patrolling of a post area by police or security personnel in a random and unscheduled manner. This type of patrol relies on individual discretion and initiative. Police/security personnel performing this type of patrol provide a sense of security for passengers. These personnel enhance the quality of the transit environment by actively enforcing laws, preserving peace, and maintaining zero-tolerance policies for criminal activity, including vandalism and graffiti. Random foot patrol is used by many RFGS employing off-duty police officers. This type of patrol offers considerable management flexibility.

- 3. Directed Patrol within Post Area.** Officers are assigned to specific posts based upon results of crime data analysis indicating that a given area is susceptible to specific criminal activities. Police/security personnel are briefed on the types of incidents occurring in the

area, and if possible, the names and physical characteristics of perpetrators. Directed patrol allows maximum resources to be focused on problem routes and areas. This type of patrol is the primary type used by RFGS police departments.

4. **Visibility Posts.** Stationing of uniformed police/security personnel at various points within the RFGS setting, where they will be most visible to the travelling public. This tactic is designed to provide RFGS patrons with a sense of security and protection. Police/security personnel are typically assigned to these posts during RFGS peak hours and reassigned to random or directed patrol during off-peak hours.
5. **System or Zone-wide Patrol.** Police/security personnel are assigned to patrol the entire RFGS, or sections of the system called “zones,” in an irregular and unscheduled manner. Similar to random foot patrol, this technique requires discretion and initiative. It is necessary for police/security personnel not responding to a service call to engage in activities that will improve patron perception of safety, while deterring the criminal. It is also the duty of the assigned officer to perform the following:
 - Enforce zero-tolerance policies,
 - Protect RFGS property,
 - Monitor the behavior of patrons,
 - Work closely with operations personnel, and
 - Ride the system.
6. **System or Zone-wide Directed Patrol.** Based on crime data analysis, police/security personnel are assigned to patrol the system, or zones within the system, utilizing pre-planned, crime- and location-specific activities to deter crime and respond to incidents. The objectives of this patrol technique are similar to the directed patrol technique. Uniformed officers are assigned to those areas, or zones, of the system where criminal incidents have been determined as likely to occur. More often than not, the zone-wide directed patrol is conducted using a vehicle. Like the directed foot patrol method, this type of patrol allows maximum resources to be directed at problem areas and routes.
7. **Vehicle Patrol.** Vehicle patrol may be of the random type, or it may be directed based on crime analysis data. The use of motorized vehicles allows police/security personnel to tour RFGS property, primarily in an effort to deter crime and to respond to calls for service. Generally, RFGS deploy police/security personnel in zones or sectors throughout the system, in an effort to reduce response time. The marked vehicles provide a visible police presence, and patrols are used to safeguard system property. Virtually every U.S. police department employs vehicle patrols as a means of deterring crimes and responding to calls; RFGS follow the same method in this deployment technique.
8. **Canine Patrol.** Uses professionally trained canines, teamed with police/security personnel counterparts to perform patrol activities. Very few RFGS enlist the aid of canine patrols. Because of the costs associated with this type of patrol, canines are only deployed in specialized situations. The following list identifies possible canine use in the transit environment:

- Facilitate high-risk arrests that present a potential for violence,
- Provide directed patrol in high crime areas,
- Detect narcotics or explosives, and
- Locate lost persons.

9. Fare Inspection. Random checks by uniformed police/security personnel to ensure that patrons have paid the correct fare. This form of deployment is used within “barrier-free” or “lack proof-of-payment” facilities. The use of fare inspection is a functional method of deterring fare evasion in RFGS facilities that do not use traditional methods of fare collection.

Uniformed Officer Deployment On NYCT Buses

Motivated by a series of unusual bus crimes in 1993, the New York City Police Department, in coordination with the Surface Unit of the New York City Transit Police Department, assigned 28 officers to patrol New York City buses for the years 1994 to 1996. The Practical Field Test was implemented in an effort to reduce patron fear and deter criminal activity. The test involved two distinct types of “bus boarding.”

Bus Rides

- A “bus ride” was defined as a police officer riding the bus from one official bus stop to the next
- Officers were not required to fill out any trip sheets

Bus Checks

- A “bus check” was defined as an officer getting on a bus at a stop, and getting off before the bus departed from that stop.
- Officers were mandated to complete a “Public Bus Inspection Report,” which requires them to record for each check:
 - The route and bus number
 - Time of check
 - The operator’s name and ID number
 - The location they checked the bus
 - Any remarks

On the test bus line, the number of incidents reported declined considerably. Total incidents fell from:

- 63 in 1994, to 42 in 1995, down to 19 during 1996
- A total decline of 70 percent

A comprehensive discussion of deployment tactics and strategies in the RFGS environment is presented in Guidelines for the Effective Use of Uniformed Transit Police and Security Personnel, available from the Transportation Research Board.

8.3 Determining Tactics

To determine the appropriate use of deployment tactics, RFGS police/security departments must determine the goals of personnel deployment; and to what extent deployment tactics can be employed after applying the RFGS limited resources to those goals. The following key assessments must be addressed in developing security deployment objectives in the transit environment:

- Determining where the most crime-prone areas are by using crime data analysis,
- Determining which types of crime are prevalent in which areas,
- Deciding which deployment tactics are most appropriate for specific areas and crimes, and
- Effectively deploying security personnel and evaluating results, making deployment adjustments as necessary.

Once RFGS security needs are determined, the police/security department should utilize deployment tactics that counter the specific crimes or situations most likely to occur within the RFGS. Since transit crime, like all other crime, is dynamic, program evaluation to assess the effectiveness of techniques is essential. On-going evaluation assists in identifying externalities and allows fine-tuning of strategies to ensure a maximum positive effect. On-going evaluation also offers realistic indicators of success and provides a means of guaranteeing flexible strategy deployment.

9. Rail Fixed Guideway System Terrorism Preparedness

While all sectors of U.S. society are vulnerable to the changing nature of modern terrorism, RFGS are particularly susceptible. Analysts John P. Sullivan and Henry I. DeGeneste note that, “Transit systems are attractive targets for a number of reasons. They carry large numbers of people within concentrated predictable areas and time frames. They are accessible (since they provide easy user access). Finally, their target-rich infrastructure, which often covers extensive geographic areas, frequently renders effective countermeasures impractical.”¹⁷

The purpose of this chapter is to describe RFGS activities used to manage the increasing threat of terrorism. The majority of these activities are focused on improving emergency response capabilities. To address the rising terrorist threat, a RFGS must be able to:

- Improve the awareness of the likelihood of terrorist threats and scenarios, including incidents involving Chemical, Biological, and Nuclear (CBN) agents,
- Determine jurisdictional responsibility for preventing and responding to terrorist acts,
- Develop coordination with local, state and federal law enforcement and emergency agencies,
- Identify, test, and select technologies to support counter-terrorism initiatives, and
- Obtain accurate and timely intelligence information concerning terrorist organizations, motivations, and threats.

9.1 Definition of Terrorism and Background Information

Since the word “terrorism” was first used in the French Revolution, it has been the explanation for a wide range of acts and motivations around the world. Specific definitions of terrorism vary, but a common element among them is the assessment that terrorism is a form of intimidation designed to influence an audience beyond the immediate victims. The goal of terrorism is not just the impact of a given act of violence on the intended target, but also the psychological impact created by that act on citizens and politicians.

In the United States, no federal or state crime is specifically termed “terrorism.” Perpetrators of terrorism can be convicted of associated crimes, such as murder, weapons and explosives violations, or destruction of property. To ensure that an act of terrorism is appropriately identified and investigated, however, the FBI has been given jurisdiction over terrorism in the United States.

¹ DeGeneste Henry I, Sullivan, John P., 1994. *Policing Transportation Facilities*, p. 73.

The FBI defines terrorism as:

“The unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives.”

Generally, to investigate an act of terrorism, the FBI requires three components:

- *Motivation*: a clear political or social agenda,
- *Perpetrators*: a conspiratorial dimension involving a group(s) of two or more individuals, and
- *Means*: the use or threat of force or violence.

The vulnerability of RFGS to acts of terrorism and intentional violence has stimulated the necessity to incorporate terrorism response planning into overall RFGS security programs.

According to the United States Department of Transportation (USDOT) Office of Intelligence and Security (OIS), since 1991, public transportation has been the target of 34 percent of worldwide terrorist attacks. In 1996, OIS reported 700 violent attacks against all modes of transportation worldwide. This was the highest number of attacks since OIS began collecting and analyzing data in 1991, and the 700 attacks recorded represent a 30 percent increase over 1995.

According to OIS findings, bus agencies and RFGS are the targets of choice for terrorists, accounting for 34 percent of all violent acts against transportation. OIS also reports that the greatest number of casualties occurred against bus and rail systems, 1,577 and 1,089 respectively. In addition to OIS findings, attacks against transportation and transportation infrastructures accounted for nearly one-third (92) of the 296 international terrorist attacks reported by the U.S. State Department.¹⁸

Managing response to an RFGS terrorist incident, particularly one causing significant casualties, damage and disruption, requires significant organizational effort. The generally recognized phases of emergency management are the following:

- Mitigation and Preparation,
- Response, and
- Recovery.

¹⁸ U.S. Department of Transportation, Bureau of Transportation Statistics, *Transportation Statistics Annual Report*, 1995 (Washington , D.C.), p.2.

9.2 Mitigation and Preparation for Rail Fixed Guideway System Terrorism

RFGS terrorism planning requires identification of resources and methods used to reduce the impact of terrorism. This process includes assessing actual capabilities, and then, through coordinated planning, determining the best strategic application of these resources and methods to the problem. Planning for terrorism has two goals:

1. Terrorism Mitigation, which includes:

- SCP techniques, focusing on system design and physical security measures to enhance observation and deter criminal activity;
- Deployment techniques, such as police patrol and surveillance, and coordination with operations and maintenance personnel to identify and resolve security threats; and
- Communication and coordination with local, state, and federal law enforcement agencies to obtain terrorism intelligence, training, and technical support.

2. Terrorism Response, which includes:

- Developing plans and procedures to minimize the potential danger to passengers and emergency responders during incidents, and
- Maximizing the effectiveness of the RFGS and other personnel while managing the critical incident.

9.2.1 Key Planning Prerequisites

Three key planning prerequisites are essential for a RFGS to assess mitigation and response capabilities to acts of terrorism. *First and foremost, RFGS police and security departments require active support from top management.* A precise and widely distributed “terrorism policy” established by the RFGS general manager provides the necessary support to develop terrorism prevention and response by:

- Emphasizing the importance of addressing the threat of terrorism,
- Designating authority for the police/security department or some other operational unit to develop and implement necessary plans and procedures and purchase necessary technology, and
- Demonstrating management commitment of resources and personnel.

The second RFGS prerequisite is the development of the Security Plan, as required by FTA's State Safety Oversight Rule. The Security Plan, focusing primarily on activities performed system-wide to provide a secure environment for RFGS customers and employees, should also document counter-terrorism programs and initiatives. As mentioned in previous chapters, the Security Plan provides important benefits, including:

- Identifying all RFGS responsibilities for security and educating all employees of these responsibilities,
- Examining and strengthening key interfaces between the RFGS police/security department and the RFGS operating and maintenance departments, and
- Strengthening coordination and cooperation with local, state, and federal law enforcement and emergency service organizations.

The Security Plan provides an opportunity to focus on security within the RFGS. Preparing this plan also encourages adoption of the systems approach to reduce criminal incidents, including the threat of terrorism.

Finally, in assessing the RFGS ability to mitigate and respond to a terrorist incident, a terrorism preparedness-planning group can be established. These designated groups may reside within the RFGS police/security departments, and are capable of developing the plans and procedures required to address both the threat of terrorism and on-going security issues.

Agencies Targeting Terrorism

In 1995, municipal officials in the Washington, D.C. area took the first steps toward confronting the threat of a chemical or biological attack by terrorists by establishing the nation's first "metropolitan strike team." The task force, which consists of thirty members (physicians and emergency personnel), was designed to respond to terrorist incidents similar to the nerve-gas attack on the Tokyo subway. The federal government offered to pay a one-time amount of \$220,000 for the purchase of supplies, equipment, and training.¹⁹

¹⁹ John Jay College of Criminal Justice. *Law Enforcement News*, Dec. 15, 1995.

9.2.2 Beginning the Planning Process

To initiate the planning process, RFGS personnel may perform the following four activities:

- Intragency coordination,
- Coordination with local, state, and federal agencies,
- Risk assessment, and
- Threat identification.

9.2.2.1 Intragency Coordination

The first activity of a terrorism preparedness planning group is to develop policies to improve internal coordination for the *mitigation* of terrorist incidents, and to provide the necessary organizational interfaces for improving *response* to such incidents. Appropriate internal coordination provides the following:

- Clear communication pathways which ensure the free flow of information among departments and within departments to those responsible for notification and response, and
- Definitive understanding of roles and responsibilities for mitigation of and response to terrorist incidents.

Strengthening Intragency Communication

By Memoranda of Understanding, the Metro Transit Police department established a long-standing program to familiarize other law enforcement agencies with the transit environment. Training programs must include the use of the entire transportation system infrastructure — ventilation systems, electrical configurations, communications capabilities, etc.²⁰

²⁰ Hunter, Geoffrey C. *Transit Policing* Volume 6, Number 1. Spring 199s, p.18

9.2.2.2 Coordination with Local, State, and Federal Agencies

Effective communication with local, state, and federal agencies provides RFGS with an understanding of jurisdictional relationships. These relationships are a key component for effective coordination. Response to a terrorist incident is likely to be emotionally charged; therefore, inter-agency coordination in advance of an incident is essential.

9.2.2.3 Risk Assessment

A risk assessment is a comprehensive study of a RFGS to identify components most vulnerable to criminal activity, including acts of terrorism, and to assess the impact of such activity on passengers, employees, and the RFGS. The results of a risk assessment assist RFGS officials in allocating available resources. Some risk assessment methods include:

- Terrorism-specific risk assessments,
- Risk assessments performed as a part of the overall system design process, and
- Security inspections, performed in the normal course of police or private security operations.

9.2.2.4 Threat Identification

Once a risk assessment has been completed, the RFGS can document potential terrorist threats to the high-risk areas of the system. This documentation enables RFGS vulnerabilities to be clearly identified and prioritized. Several methods may be used to identify these threats, including:

- Analysis of historical data and application of this information to the development of various attack scenarios against the RFGS,
- Review of threat checklists developed by the RFGS or obtained through other sources (e.g., consultants),
- Judgment of RFGS senior personnel (based on experience and knowledge of system vulnerabilities), and
- Use of formal analyses, including Preliminary Threat Analysis (PTA) and Fault Tree Analysis (FTA).

RFGS police/security professionals, safety departments, and RFGS personnel in operations, maintenance, procurement, and administration all play a role in developing the plans, policies, and procedures that direct counter-terrorism programs at the RFGS. In addition, many RFGS rely on a significant level of support from local and state law enforcement and emergency management agencies, as well as federal agencies, such as the FBI and the Bureau of Alcohol, Tobacco and Firearms (BATF).

9.2.3 Resolving Identified Risks and Threats

Terrorist profiles are a valuable tool for RFGS in designing deterrence programs. For example, knowledge of the habits, capabilities, and target selection process of terrorists targeting city officials using mail bombs enabled one agency to develop an effective procedure for receiving and screening mail and packages. Transit security information circulars available from the USDOT OIS (distributed by FTA) and local law enforcement agencies also provide vital information to assist RFGS in identifying chronic vulnerabilities.

Limited resources force RFGS police/security personnel to choose which assets to protect and which to leave unprotected. To assist in making these decisions, a resolution process can be implemented for identifying risks and threats. This process involves the following procedures:

- Assessing RFGS resources available to support anti- and counter-terrorism programs,
- Assessing outside resources available at the local, state, and federal level to support anti- and counter-terrorism programs,
- Determining specific activities to be performed by the RFGS to deter acts of terrorism and extreme violence,
- Determining specific activities to be performed by the RFGS to manage a terrorist incident and to coordinate response with appropriate local, state, and federal agencies, and
- Allocating RFGS and outside resources to support identified activities for terrorism prevention and response.

Typical countermeasures for terrorism include law enforcement presence, physical security measures, improved response capabilities, warning or detection technologies, and response and emergency management training. To determine which of these countermeasures best resolves identified risks and threats, RFGS police/security personnel can evaluate the following issues:

- Physical areas in high-risk facilities that are susceptible to terrorist activity,
- RFGS policies in high-risk facilities that may encourage terrorist activities,
- Methods to improve system design in high-risk facilities, and
- Methods to improve RFGS management in high-risk facilities.

9.2.4 Integrating Terrorism Response

Effective emergency management requires sound decision-making in a chaotic and emotionally-charged environment. Management of this caliber can only be achieved through dedicated emergency planning and training. This is particularly true for response to acts of terrorism and extreme violence.

RFGS emergency preparedness for terrorism directly influences the magnitude of danger in an emergency situation. Terrorism emergency preparedness in the transit environment is strengthened by the following methods:

- Developing an Emergency Action Plan,
- Integrating emergency policies and procedures into existing operating and emergency response procedures,
- Identifying and training with emergency equipment,
- Designing emergency features in system and vehicle design,
- Training RFGS employees and emergency response organizations, and
- Providing advance information to emergency response organizations on transit components.

Most RFGS have developed Emergency Action Plans for direct response to any incident threatening life safety at the RFGS, including accidents, natural disasters, and hazardous materials (hazmat) spills. A few RFGS have supplemented general Emergency Action Plans with specific Terrorist Incident Response Plans. These plans address contingencies arising specifically from large-scale mass violence, including the need for enhanced notification, if possible, and coordination with federal, state, and local law enforcement and emergency management agencies.

The purpose of an Emergency Action Plan, also referred to as a general Emergency Plan, is to establish procedures to be implemented by the RFGS and other responding agencies when a life-threatening situation occurs at or near the system. In the transit environment, the goals of such a plan are to:

- Facilitate the flow of information within and between all levels of the RFGS,
- Facilitate interaction and coordination among all responding agencies.

In general, Emergency Action Plans used in the transit environment provide guidance for:

- Reporting the incident,
- Evaluating the incident,
- Designating an Incident Commander,
- Notifying emergency response personnel/agencies,
- Protecting personnel and equipment at the incident site,
- Dispatching emergency response personnel and equipment to the incident site,
- Evacuating passengers and non-essential personnel,
- Providing incident briefings and situation updates,
- Providing medical treatment and transportation to medical facilities,
- Managing the emergency,
- Restoring the system and agency to normal, and
- Incident debriefings and After Action Reports.

A key goal of the Emergency Plan is to establish Unified Command with local responders. Unified Command allows all agencies with geographical, legal, or functional responsibility to establish a common set of incident objectives and strategies, and a single plan for action. Using the Unified Command, the RFGS coordinates with local police, fire, and Emergency Medical Services (EMS) personnel to ensure that:

- One set of objectives is developed for the entire incident,
- A collective approach is used to develop strategies to achieve incident goals,
- Information flow and coordination is improved between all jurisdictions and agencies involved in the incident,
- All agencies with responsibility for the incident have an understanding of joint priorities and restrictions,
- Each agency is fully aware of the plans, actions, and constraints of all others,
- The combined efforts of all agencies are optimized, and

- Duplicate efforts are reduced or eliminated, thus reducing cost and chances for frustration and conflict.

RFGS Emergency Plans are significantly influenced by the Incident Command System (ICS), first implemented in the late 1970s to cope with large-scale multi-agency responses to wild-land fires. Perhaps the most important feature of ICS is its ability to be integrated into the command structure of local police and fire departments. In the event of a terrorist incident at a RFGS, either local police or fire services ultimately assume the duties of the Incident Commander, or join in a "unified command." RFGS police and operations personnel, however, continue to play a vital role during emergency response. By using ICS, RFGS police and operations remain "plugged into" the command structure, ready to assist and supply information and resources to the effort.

9.2.5 Incident Command System Management Concepts

ICS has been successfully used for a wide range of emergency and disaster management applications. These applications range from humanitarian assistance in famines and natural disasters to civil disturbance management. ICS is the standard emergency management framework for interagency wildfire management and is also known as the National Interagency Incident Management System (NIIMS). ICS is required by federal law for response to hazardous materials situations and is the mandated incident management framework in California.²¹

The seven ICS operating requirements are the following:

1. The system must provide for a wide variety of operations including: single jurisdiction responsibility with single agency involvement, single jurisdiction responsibility with multi-agency involvement, and multi-jurisdiction responsibility with multi-agency involvement;
2. The organizational structure must be adaptable to include any emergency encountered by public safety agencies;
3. The system must be applicable and acceptable to all user agencies;
4. The system must be capable of rapidly expanding from an initial response effort into a major incident response, while retaining the ability to reduce its size as incident demands decrease;
5. It must have common terminology;
6. Implementation should cause minimal disruption to existing systems; and

²¹ California's Standardized Emergency Management System (SEMS), codified at Section 8607(a) of the California Government Code, mandates ICS for all state agencies. All local agencies must use SEMS/ICS in emergency and disaster management to be eligible for any state reimbursement for disaster-related personnel costs.

7. It must meet these requirements while remaining simple enough to ensure understanding.

9.3 Responding to Transit Terrorism

The resolution of complex emergencies resulting from acts of transit terrorism and extreme violence is a pivotal function shared by the RFGS and the law enforcement and emergency services communities. This section presents organizational structures, tactics, and programs used to manage response for acts of RFGS terrorism.

The following table outlines key incident objectives for managing response to transit terrorism:

Objectives for Response to Terrorist Incidents (General)
<ul style="list-style-type: none">• Secure Perimeters (establish inner and outer perimeters and control zones; contain the situation; avoid creating new victims, contaminating evidence, and spreading contaminants).• Control and Identify the Threat (including CBN agent release).• Rescue, Decontaminate, Triage, Treat and Transport Impacted Persons.• Move Crowds to Safe Zones (minimize additional casualties).• Stabilize Incident (prevent escalation, establish control of the situation to allow rescue and recovery to proceed with minimal delay).• Protect Rescuers (injured responders cannot effectively rescue and place an additional strain on scarce resources, potentially jeopardizing operational success). All response personnel should receive an incident specific safety briefing when extraordinary hazards exist. All personnel should be provided and required to wear and use Personal Protective Equipment (PPE) appropriate to incident conditions.• Avoid Secondary Contamination.• Secure Evidence and Crime Scene (evidence management and crime scene issues are important to the identification of offenders and future prosecution; inner and outer perimeters and proper procedures must be followed).• Protect Against Secondary Attack (global experience with terrorist attacks and bombings has shown that secondary attack, [i.e., secondary explosive devices intended to injure emergency responders], is a real threat).
Objectives for Response to Terrorist Incidents (Rail Fixed Guideway System-Specific)
<ul style="list-style-type: none">• Provide Alternative Modes of Transport.• Assess and Mitigate Secondary Impact on System (crowd conditions throughout the system, particularly at key transfer points, are likely depending on the site of the incident; additionally, RFGS should maintain a high index of suspicion for additional attacks or “copycat” incidents in the immediate aftermath of an attack).• Restore Service Quickly (restore transit service through re-routed vehicles and alternative modes, [i.e., “bus bridges”]. Clearing the incident scene and repairing damaged areas must be a priority).• Restore Passenger Confidence (on-going security measures must be reinforced. Transit customers should be advised of enhanced awareness and measures).• Restore Employee Confidence (integrate employees into system security team).

9.3.1 Responsibilities for Incident Management

In the event of a major act of transit terrorism requiring full-scale response from local, state and federal law enforcement and emergency management organizations, the local police or fire department generally assumes ultimate control over the scene. While specific responsibilities or jurisdictional issues may vary among RFGS, some activities are common to all. For example, all RFGS have the initial responsibility of assessing the incident and requesting response from local police and fire departments.

Not all RFGS have their own police force, however, and not all RFGS police have investigative responsibilities for complex crimes. In many cases, the role of RFGS police agencies is to act as first responders and then provide technical assistance and support (e.g., crowd control, securing crime scenes, escorting specialized investigative teams) to the investigative and emergency response agencies. In addition to this support role, RFGS police assume the lead role in assessing and managing secondary impacts throughout the RFGS.

9.3.2 First Responder Considerations

When a terrorist incident occurs, numerous personnel and agencies are contacted to address the many individual actions required for incident resolution. At a RFGS, such responders may include the RFGS police/security department; RFGS operations personnel; and local police, fire, and EMS. During this immediate response phase, efforts are focused on the:

- Assessment of the situation (also known as “size-up”) to develop a situation estimate,
- Containment of the incident to prevent additional casualties and preserve evidence, and
- Search for additional terrorist devices, and notifications.

In the event of a confirmed CBN incident, first responders must recognize that:

- CBN incidents are essentially intentional hazardous materials incidents,
- They are crime scenes,
- A multi-jurisdictional response is required, and
- Existing transit-specific hazards (e.g., traction power) must be managed appropriately.

9.3.3 Developing an Incident Action Plan

After first response, the work of incident management begins. During this “operational period,” development of an Incident Action Plan (IAP) is advised. The IAP establishes incident management objectives and describes the strategy, tactics, resources, and other support required.

Chicago PD Basic Organizational Emergency Procedures—Bomb Incident Plan

1. Designate a chain of command.
2. Establish a command center.
3. Decide what primary and alternate communications will be used.
4. Establish clearly how and by whom a bomb threat will be evaluated.
5. Decide what procedures will be followed when a bomb threat is received or device discovered.
6. Determine to what extent the available bomb squad will assist and at what point the squad will be requested.
7. Provide an evacuation plan with enough flexibility to avoid a suspected danger area.
8. Designate search teams.
9. Designate areas to be searched.
10. Establish techniques to be utilized during the search.
11. Establish a procedure to report and track progress of the search and a method to lead qualified bomb technicians to a suspicious package.
12. Have a contingency plan available if a bomb should go off.
13. Establish a simple-to-follow procedure for the person receiving the bomb threat.
14. Review your physical security plan in conjunction with the development of your bomb incident plan.

9.3.4 Reconciling Crisis and Consequence Management

Response to a major incident consists of the following two elements:

- Crisis management, and
- Consequence management.

This distinction is derived from the federal distribution of responsibilities articulated in Presidential Decision Directive 39 (PDD-39) which describes the federal response to terrorism. While the distinction does not directly impact the role of local responders, understanding of the federal response directive will greatly reduce confusion and potential role conflict at an actual incident.

Crisis management is defined as measures to resolve the hostile situation, investigate, and prepare a criminal case for prosecution under federal law. *Consequence management* defines those measures that alleviate the damage, loss, hardship, or suffering caused by emergencies. These include measures to restore essential government services, protect public health and safety, and provide emergency relief to affected entities.

Crisis management response falls under the jurisdiction of the federal government with the FBI acting as the lead agency. Crisis management response involves measures to:

- Confirm the threat,
- Investigate and locate the terrorists and their weapons, and
- Capture the terrorists.

Consequence management response is within the jurisdiction of the affected state and local governments. Federal agencies support local efforts under the coordination of the Federal Emergency Management Agency (FEMA).

Crisis management focuses on criminal intelligence and investigations with the goal of:

- Preventing or interdicting the act, or
- Containing or minimizing the consequences of an incident.

When an incident is determined to be a terrorist act, on-scene command is assumed by the FBI field office with national command and control at FBI Headquarters in Washington, D.C. In the early stages of an incident, particularly one without prior warning, local police play a major crisis management role pending arrival of FBI personnel. (Arrival of FBI personnel on the scene may take some time.) Collaboration between local police and the FBI continues throughout management of the incident. FEMA has the lead in consequence management at terrorist-caused disasters and coordinates federal support to local agencies using the Federal Response Plan (FRP), for Public Law 93-288, as amended April 1992.

Effective resolution of a terrorist incident requires close integration of crisis and consequence management efforts. Ideally, crisis and consequence management function as individual threads which weave together to resolve the incident. Successful incident resolution depends upon effective coordination among all responding entities. Response must fully integrate the resources, knowledge and skills of police, RFGS personnel, and emergency responders.

9.3.5 Federal Emergency Management Agency Emergency Support Functions

Effective incident resolution requires RFGS personnel in both operations and security roles to recognize limitations as well as potentially vital contributions to response. Similarly, RFGS personnel, including the police/security force, must be aware of the tensions present in response to a RFGS terrorist incident (e.g., tensions between rescuers and investigators, and investigators and RFGS personnel anxious to restore RFGS service). Unified command is a useful way to reconcile the tensions that develop between crisis and consequence management objectives.

Effective integration of a multi-agency response also requires an understanding of the roles and functions of responding agencies. Federal support for managing the consequences of a major terrorist incident are organized through pre-designated Emergency Support Functions (ESF). These functions utilize a wide range of federal resources, and are coordinated by FEMA to support local incident response and recovery efforts.

9.4 Recovery

The final element of effective incident response involves integrating response and recovery operations as early as possible. Once the incident shifts from the initial first response phase into actual rescue and response operations guided by an incident command organization, assessment and planning for recovery begins. Recovery planners collect information on situation status, resource status, and damage assessment to formulate a plan for recovery and restoration of service. Recovery issues should be addressed through a recovery branch or group.

Emergency Preparedness for Transit Terrorism, available from the Transportation Research Board, provides much greater detail on the issues discussed in this chapter.

10. Data Collection

A vital and shared security function for a RFGS is the collection of security information. The collected data can be used to:

- Prioritize problems,
- Design strategies to solve these problems,
- Assess the effectiveness of these strategies, and
- Communicate this information with local public safety agencies.

A strong data collection process enables a RFGS to use resources more effectively by targeting high crime areas, identifying trends in crime, and designing and testing countermeasures. Data content, collection, storage, and format dictate the utility of the data collection effort. The arrangement of data within files largely determines the types of analysis that can be performed and, hence, the utility of the collected data for deployment decision-making, case clearance, and the design of effective countermeasures. The content and form of information released to the public assists in determining the framework within which a department is held accountable, and impacts public expectations.

The following figure describes the security information flow through a typical transit agency with its own in-house dedicated police force.

As is demonstrated in this figure, security information enters the transit system in three ways:

1. Reports from transit police patrol activity
2. Reports from transit employees
3. Reports from transit passengers/victims

During patrol, transit police observe criminal activity and cite or arrest offenders; assist passengers; and maintain order on the system. During these activities, transit police may issue citations or warnings, complete field identification cards or perform other activities to track suspicious actions or persons, and complete patrol logs. When issuing citations or warnings, or engaging in other patrol activities, transit police may call transit police dispatch to ensure that each case or citation is assigned a case number. Further, some police may notify dispatch in the event of suspicious activities or to assist passengers with particular problems.

Transit employees may also report suspicious activities or other occurrences to either transit dispatch, which will notify transit police dispatch, or directly to transit police dispatch. In either case, upon such a report, a transit police officer should be assigned to investigate the call.

Further, the transit employee may be asked to complete an incident form, sometimes referred to as an “unusual occurrence report.”

Transit passengers, or the victims of crime – either transit passengers or employees – may also report criminal activity to transit dispatch or the transit police dispatch. In the event of such an occurrence, a transit police officer will be dispatched to investigate the report, process the crime, and reassure the victim.

As indicated in the figure, the transit police dispatch and the transit agency dispatch both play crucial roles in the security information collection process. The vast majority of security information reported at a transit system with a dedicated police force goes through the transit police dispatch. To capture information on actual incidents, transit police dispatchers initiate “run cards” for each call for service. These cards, which may be pre-numbered, assign a case number to each call for service to ensure that the call can be tracked from initial report through to case disposition. Further, transit police dispatchers may track call-ins from patrol officers, as well as activities performed to assist transit passengers and employees. Transit dispatchers also may perform warrant searches, notifications, and specific requests for information from local police. In each case, a record of this activity may be preserved in the form of the recorded phone call, dispatch log, and in the 24-Hour Reports prepared for both management and data collection and analysis purposes.

Transit police dispatchers also maintain records on the number of bomb threats received at the transit agency, and may also file completed bomb threat management checklists or other documentation on the incident.

In response to a call for service, transit police officers will investigate the incident and prepare an Incident Report Form and, if necessary, a Supplemental Report Form. These forms describe the incident, including such key information as the type of incident, time of incident, list of witnesses, actions of perpetrator and victim, and any contributing factors to the incident. While under investigation, incident evidence will be collected and a chain of custody will be established for managing and storing this evidence. Once the incident has been resolved, a Disposition or Arrest Report will be filed. This information, when combined with citation records, provides the primary source of crime data used guide crime analysis activities at most transit police departments.

To perform crime data analysis, transit police and civilian analysts review dispatch records, Incident and Supplemental Report Forms, Disposition/Arrest Forms, and information provided by transit operations personnel. Further, depending upon the level of cooperation with local police, transit crime analysts may be able to information concerning criminal occurrences near and on transit property that may have not been reported to the agency.

At a minimum, transit crime analysts prepare monthly reports summarizing criminal activity on the system, annual reports, and submissions for the UCR program and FTA’s National Transit Database. Analysts may also prepare reports evaluating the results of special programs or deployment strategies used to address special problems (parking lot crime, homeless population, etc.).

While varying among RFGS, the goals of crime data collection can be categorized as follows:

- The collection and organization of data on legal evidence that supports the arrest and conviction of perpetrators,
- The provision of a decision-making aid for the deployment of RFGS police and security manpower,
- The organization of information to improve and test the effectiveness of crime countermeasures,
- The presentation of crime information to strengthen the position of the RFGS police or security department within the RFGS system, and
- The communication of information to influence passenger perceptions of system security.

RFGS police and security personnel, and RFGS management, must identify three critical components of criminal incident information:

1. The number and types of criminal incidents occurring on the system,
2. The location and time of these incidents, and
3. Information on the underlying conditions surrounding the occurrence of these incidents.

Supplemental information that improves the crime analysis process, but that is not essential to a basic information system includes:

- The impact of the incident on transit service,
- Information concerning other "quality of life" violations that may have been committed by the perpetrator of a serious incident prior to the incident, and
- The attention/treatment of the patrons involved in the incident (victims and witnesses).

Given the varying police powers of the organizations that provide security at RFGS, not every security organization can collect this information. Limited access to crime data is a special problem for RFGS relying exclusively on municipal police for security and for non-sworn security agencies that must provide security in partnership with municipal police.

RFGS can collect crime data from the following readily available sources:

1. *Dispatch logs,*
2. *Operator reports,* and
3. *Incident report forms.*

While none of these sources present a complete picture by itself, in combination they enable the RFGS to obtain an accurate assessment of the crime occurring on the system, as well as valuable information to improve both the deployment of police/security personnel and the design of crime countermeasures.

10.1 Dispatch Logs

The amount of information recorded in a RFGS dispatch log varies from system to system. In most cases, however, effective monitoring of the dispatch log enables RFGS personnel relying on municipal police to establish an accurate assessment of serious incidents. The dispatch log is particularly useful for RFGS police and security departments, as they must organize operations and record-keeping efforts in accordance with the RFGS dispatch system.

While the majority of RFGS dispatchers possess no police training, the following information is routinely recorded:

- The day, date, and time of an operator call for assistance,
- Reason for the call,
- Whether police notification was required, and
- Total delay time resulting from an incident.

For RFGS passing through several police jurisdictions, the dispatch log also provides a record of RFGS interaction with these municipal police agencies. This information can be summarized in weekly or monthly reports that supplement RFGS understanding of the security problem.

The dispatch log is not a comprehensive source for transit crime information. While it identifies incidents, it offers no description of the incident, nor of the underlying circumstances that contributed to it. Furthermore, the dispatch log does not identify “quality of life” issues that may discourage ridership. Finally, the dispatch log does not provide data in sufficient detail to design countermeasures or to test their effectiveness. For many RFGS, however, the dispatch log provides a valuable, if preliminary, assessment of RFGS crime.

10.2 Rail Fixed Guideway System Operator Reports

Since RFGS operators, conductors, or station personnel are often the only representatives of the RFGS present when a security incident occurs, they provide considerable information concerning the level of crime experienced by the system. Security information is collected from RFGS operators in a variety of ways, including:

- Using informal means to discuss crime, such as weekly or monthly meetings, newsletters, union coordinators and support services, or joint-committees within the RFGS, and
- Implementing formal means to document incidents witnessed or experienced by operators, including the requirement that operators file formal reports and the establishment of incentive programs encouraging operators to testify in court against offenders.

Wherever possible, RFGS should encourage the use of operator reports. These reports, generally filed with the Operations Department, are especially valuable for RFGS relying on municipal police to provide security. Many systems use a brief, one-page form that records operator information (e.g., name, badge number, etc.) and a description of the incident (e.g., date, time, location, incident type, and operator actions, including notification of the dispatcher). Although this information does not comprehensively assess incidents, it does target problem routes and riders, and provides RFGS operators with an opportunity to actively take part in combating crime.

When cross-referenced with dispatcher records, operator reports offer municipal police added insights into RFGS crime. This additional information may improve the relationship between the RFGS and the municipal police. Familiarity with operators may encourage local police to place a higher priority on RFGS incidents.

For RFGS with transit police or security departments, operator reports offer an opportunity for responsive and productive working relationships between operators and police/security departments. Operator reports also provide a valuable source of information to supplement police reports, resource allocation decision-making, and investigations.

10.3 Incident Report Forms

In addition to the effective use of dispatch records and operator reports, information can be collected from police/security incident report forms. Incident report forms provide crime data analysts with sufficient information to:

- Group similar incidents together for monitoring and analysis,
- Improve the efficiency of deployment, and

- Design effective countermeasures.

Further, involving crime data analysts in incident report form design improves the likelihood that the form will be used to provide maximum benefit.

Incident report forms generally contain the following two sections:

- The first section allows for quick classification of the incident through general information coded for easy entry into an information management system, and
- The second section contains a detailed write-up of the incident.

While the incident write-up may provide more specific information relative to a given crime, the RFGS crime analyst may find the information included in the first section, because of its format, more valuable in constructing a complete profile of crime on the system. Thus, an effective form includes as much detailed information as is feasible in the first section.

Incident report form changes are best conducted by RFGS police and security departments in charge of completing and monitoring incident reports. Most RFGS police and security departments require detailed information on the following:

- Time and place of an incident, including the day, date, and time of the incident,
- Exact location of the incident,
- Rail line and run on which the incident occurred,
- Name of the rail operator driving the vehicle at the time of the incident, and
- The vehicle number.

These departments also use a variety of classification schemes to define the incident and to provide more effective grouping and analysis of incidents for monthly reports.

In addition, the following information assists the crime data analyst in targeting the conditions that contributed to the occurrence of the incident:

- Information on victim actions prior to the incident,
- Suspicious actions committed by the perpetrator before the reported incident (e.g., fare evasion, public drunkenness, stake-out of facility, loitering),
- Environmental conditions that may have contributed to the incident (e.g., burned-out light bulb, broken lock), and
- The apparent target of the perpetrator (if applicable).

RFGS police and security departments also include a series of measurements reflecting the impact of the incident on the system, such as:

- Service delay,
- Vehicle pulled from service, and
- Employee injury.

These measurements assist RFGS police and security departments in quantifying the value of the service they provide and the extent of the operational problems caused by crime on the system. Finally, incident report forms can be redesigned to request information concerning the involvement and treatment of patron victims and witnesses. This type of information assists RFGS management in handling affected patrons such that negative impressions of the system are minimized. These changes can be incorporated into the standard incident report form with the cooperation of the RFGS crime data analyst, so that the information is presented in an easily coded format.

For RFGS relying on municipal police, meetings with municipal crime analysts and officials can result in alterations to the municipal incident report form. Some RFGS have coordinated with local police to modify report forms to include exact locations, times, and, in some circumstances, information concerning the environmental conditions where the incident occurred. RFGS can also coordinate with municipal police to demonstrate the importance of an accurate record of transit crime, including the establishment of monthly or quarterly meetings to discuss data collection and analysis issues.