13. SYSTEMS & SECURITY

13.1 Design Objectives

This section presents the security systems designed to provide a reasonable level of safety and security for Omnitrans patrons, employees, the general public and local emergency service personnel. The design criteria are intended both as a reference and as a guide to the designers of facilities and systems.

Facility design and operating procedures shall promote a sense of well-being by patrons, and personnel, discouraging acts of crime, violence, and abuse. Security provisions shall also discourage acts of vandalism, theft and fraud.

The purpose of system safety and security design criteria is to provide sufficient definition and description of all facets of a system security concept so that design engineers and architects have guidance for the proper selection of equipment. Through these criteria, security considerations will be integrated into all aspects of the design, equipment selection, architectural concepts, procedures and operations.

Security systems are safety critical, and shall therefore be designed to remain in service during security emergencies under all conditions as well as within the environmental operating limits of the security equipment involved.

Security shall be incorporated into facility design as follows:

- Provide sufficient space for electronic security system monitoring stations and equipment;
- Provide adequate, redundant electrical power for security systems;
- Provide access control as needed; and
- Protect utilities by locating transformers, control valves, switches and similar equipment within security-controlled areas.

The objective is to create an environment where customers, employees and visitors are not only free from crime and other threats to personal safety, but in which they perceive and believe themselves to be so.

In order to achieve this objective, the following concepts must be applied to the design:

- Provide lighting to reduce fear of crime;
- Apply Crime Prevention Through Environmental Design (CPTED) principles as appropriate;
- Use fencing/barriers as needed to deter intrusion;
- Provide closed circuit television coverage as needed;
- Provide intrusion alarms as needed;
- Provide access control as needed; and
- Maximize lines of sight by minimizing obstructions to vision by occupants.

13.1.1 Physical Security Planning

The system shall contain deterrence from, protection against, and surveillance of potential acts of violence. This approach to design shall apply to both fixed facilities and mobile elements (vehicles) of the Omnitrans system. In general, the sbX system shall include features that enhance patron and personnel security. This can be accomplished through:

- Facility design;
  - Architectural Design;
  - Structural Design;
  - Lighting;
  - Landscaping;
  - Barriers / bollards;

  - Perimeter fencing;
  - Tamper resistant equipment;

- Security systems;
  - Access control;
  - Intrusion detection;
  - CCTV;
  - Communications; and
  - Information systems security.

13.1.2 Station Related Systems

Design standards and specifications for each station related system will be developed as the design progresses. As with all phases of the design process, these standards and specs will be reviewed with affected agencies and utilities as applicable for conformance with existing standards, or the need for approval of variances. Station related systems include, but are not limited to the following systems:

- Variable Message Signs (VMSs);
- Advanced Travel Information System;
- Public Telephones (PTELs);
- Emergency Telephones (ETELs);
- Public Announcement (PA) System;
- Communication Transmission System (CTS);
- Fare Collection System, Ticket Vending Machines (TVM) and Equipment;
- Wide Area Network (WAN); and
- Closed-Circuit Television (CCTV) System.

Station related systems are addressed further in Section 11 of this report.

13.1.3 Public Areas

Public areas must maximize their self-policing capabilities by providing broad and easy surveillance ability, minimizing areas of visual obstruction, avoidance of unobservable corners and niches, and providing inherently intuitive functional layouts. The objectives for employing police presence facilities and physical and electronic security systems include both enhancing protection and creating an environment where customers, employees, and visitors perceive a higher level of personal security. These measures also serve as a deterrent against criminal and terrorist activities.

Provide visible signs of security features, including:

- Closed-circuit television system (CCTV);
- Signage;
- Lighting; and
- Security presence (Police, fare inspectors, security guards, etc.).

13.1.4 Facility Design

Risk to Omnitrans facilities from physical attack must be mitigated through a combination of architectural and structural design.

Where glass is used in construction where adjacent spaces are occupied, use materials specifically designed to resist shattering into sharp fragments in an explosion. Window frames and their supports must be capable of resisting the ultimate capacity of the glazing.

Wayside signal and communication enclosures at grade must also be protected by barriers or bollards from direct vehicle impacts. The vehicle impact force to be mitigated must be for a 4,000 pound vehicle at 30 miles per hour.

13.1.5 Barriers/Bollards

Vehicle barriers can be used to provide: safety; theft deterrence; asset protection; pedestrian vs. vehicle traffic separation;

pedestrian control; and traffic control. Barriers protect facilities, critical infrastructure, and people from both errant and terrorist vehicle attacks. Properly designed and installed barriers are effective in controlling both pedestrian and vehicular movement inside a facility, within a facility's perimeter, or gaining access to the exterior of a facility.

Structural barriers can be grouped into two general categories:

- Natural barriers (water, vegetation, terrain); and
- Fabricated barriers (bollards, guardrails, fences, walls).

Table 13-1 below shows typical vehicle barrier usage and potential locations.

13.1.6 Perimeter Fencing

Fences provide a visible demarcation of non-public space and define the limits of a facility and/or yard. Fencing can range from high-security grill type fencing to cost effective chain-link fencing. If the security threat is lower or if aesthetics are a high priority, ornamental fencing can be used providing it is designed to prevent scaling. Low security fencing shall be used to define functional areas, and high security fencing shall be used for control of access to Omnitrans property by unauthorized persons.

Perimeter fences should be located and constructed to prevent the introduction of persons, dangerous substances or devices, and should be of sufficient height and durability to deter unauthorized passage.

Areas adjacent to fences should be cleared of vegetation, objects and debris that could be used to breach them or hide intruders.

Gates should provide an equivalent level of protection as the fence, be self-closing and have access control.

Table 13-1: Potential Barrier Uses and Locations

		Potential barrier location				
		Entrances, Exits, Perimeters of Admin/Control facilities	Entrances to parking lots	Entrances to stations	Entrances to Maintenance / Storage facilities and yards	Construction sites
Barrier Usage	Create stand- off distance	♦	♦	♦	♦	
	Protect assets / pedestrians	♦	♦	♦	♦	
	Slow vehicles		♦		♦	
	Stop vehicles		♦	♦	♦	
	Restrict vehicle entry		♦	♦	♦	♦
	Direct traffic	♦	♦	♦	♦	♦
	Revenue collection		♦			
	Theft deterrent		♦		♦	

13.1.7 Security Systems

Security systems must be designed to remain in service during emergencies. There must be sufficient space inside communication rooms for the electronic security system.

Integrating both physical and electronic security systems provides the highest level of protection for operations, employees, commuters, and visitors. To achieve this, the following design philosophy must be used:

- Auto-sensing day/night and/or infrared cameras must be used where it is not feasible to provide light levels sufficient to meet video surveillance requirements;
- Electronic security system equipment (command, control, and communication racks and panels) must be protected;
- Provide access control and intrusion detection to areas where this equipment is mounted or maintained. Security equipment racks or components must be segregated from non-security system equipment. These racks or components must have tamper indication using additional access control. Normal and stand-by power must be provided from dedicated security breakers;
- Provide tamper alarms on all security equipment racks and panels;
- Cabling must be protected in rigid conduit. If conduit is marked, the label must not include descriptive terms such as "Security," "Alarm," "CCTV," etc.;
- Communication (both data and video transmission) must use fiber optic cable for network connections and to devices wherever feasible;
- An independent rack-mounted security workstation must be provided in each communication room with dedicated electronic security system equipment racks. This workstation must provide all administrative and maintenance access to the respective security system, must be mounted inside a secured security rack, and must be protected against intrusion;
- Access control card reader systems must support both contact-less card and magnetic swipe cards;
- Electronic locks, when used, must be configurable for failing secure or un-secure in the event power is interrupted; and
- Modular camera components must be used to the greatest extent possible to minimize maintenance time. Use vandal-resistant, low-profile, dome housings for cameras wherever feasible.

13.1.8 Environmental Requirements

The security systems equipment must be capable of safe, correct and reliable operations at full load capacity and within the full range of environmental conditions.

For outdoor installations, the security equipment must be installed in enclosures and able to operate safely and correctly within the temperature ranges of minus 13 degrees F (-25 degrees C) to plus 158 degrees F (+70 degrees C) at 95% humidity with rainfall at up to 4" per hour. The design must protect against condensation, heat and water build-up in and around system elements.

13.1.9 Closed Circuit Television Cameras

CCTV cameras are an important part of the overall security of a facility. Not only can the cameras provide real-time surveillance

of unmanned or remote locations, they can provide valuable information should a breach or incident occur. In addition, the presence of cameras can serve as a deterrent to potential intruders who may believe they are being observed.

13.1.10 Requirements

The CCTV system must provide reliable video surveillance, video data storage, and video display. The system must:

- Provide immediate display of CCTV cameras triggered by the corresponding intrusion detection system and at access point alarms;
- Provide fixed camera video coverage of all designated public entrances and exits, including platforms entrances and exits, TVM's and key intersections;
- Use digital video technology as the method for transmitting video images, point-to-multi pint video transmission system;
- Use closed-circuit television cameras to provide immediate view of all intrusion detection alarm zones and doors protected by electronic access control;
- Provide electronic digital storage of all video surveillance (all cameras). The minimum required is 30-days of storage for all cameras (minimum of 8-frames per second); and
- Cameras triggered by alarms must have an automatic capability to provide 10 seconds of pre-alarm video recording at not less than 30 frames per second. (Note: storage capability inside the camera does not satisfy this requirement – it must be stored a minimum of 100' from the camera being recorded). The system must automatically continue to store video at not less than 30 frames per second until the alarm is cancelled.

This Page Intentionally Left Blank