SYSTEMWIDE BASELINE
CHANGE NOTICE (SBCN)

METRO RAIL DESIGN CRITERIA SECTION 12 SAFETY, SECURITY AND SYSTEM ASSURANCE
REV. 3

CHANGE IMPACT ASSESSMENT SUMMARY:  (Attach written explanation of impacts identified)

<table>
<thead>
<tr>
<th>SCHEDULE ISSUES?:</th>
<th>N</th>
<th>OTHER DOCUMENT REVISIONS REQUIRED?:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROM (RANGE):</td>
<td>NO COST</td>
<td>DESIGN ISSUES?: N</td>
</tr>
<tr>
<td>TIME IMPACT:</td>
<td>N/A</td>
<td>SAFETY ISSUES?: N</td>
</tr>
<tr>
<td>CAL DAYS</td>
<td>N/A</td>
<td>THIRD PARTY?: N</td>
</tr>
<tr>
<td>OTHER CONTRACTS/PROJECTS?:</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Related Request(s) For Change: NONE

JUSTIFICATION (including benefit or impact if not pursued):

This Design Criteria Section 12 Rev. 3 is being issued for inclusion in Contract C0980 Regional Connector RFP. Formal review and approval process will follow. Any additional changes identified will be processed in a subsequent revision, and issued through the SBCN and Addenda process.

Updated the communications section based on revisions to DC section 9. These updates are based on lessons learned from the field and current projects. The updates are needed for correct operation and to avoid change orders on new projects.

PROJECTS/CONTRACTS AFFECTED: For new projects only

<table>
<thead>
<tr>
<th>PROJ CONTRACT CN #</th>
<th>ACTION STATUS</th>
</tr>
</thead>
</table>

TOTAL ESTIMATED CHANGE COST: (DIRECT)
TOTAL ESTIMATED CHANGE COST: (INDIRECT: POTENTIAL COST RECOVERY)
TOTAL ESTIMATED CHANGE COST: (INDIRECT + DIRECT)

RECOMMENDATION AND APPROVAL SIGNATURES: (R = RECOMMEND, A = APPROVE)

<table>
<thead>
<tr>
<th>RTG</th>
<th>APPROVAL</th>
<th>NAME/TITLE</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>DIRECTOR CONFIGURATION MANAGEMENT</td>
<td>D. CURZON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>DIRECTOR PROJ. ENG. FACILITIES</td>
<td>A. DAVIDIAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>DIRECTOR PROJ. ENG. SYSTEMS</td>
<td>M. RATNASINGHAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>INTERIM EXECUTIVE DIRECTOR, RAIL OPERATIONS</td>
<td>B. SHELBURNE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>DIRECTOR QUALITY MANAGEMENT</td>
<td>W. MOORE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>EO, PROJECT ENGINEERING</td>
<td>S. MAYMAN</td>
<td></td>
<td>05/15/13</td>
</tr>
<tr>
<td>A</td>
<td>EXECUTIVE DIRECTOR TRANSIT PROJECT DELIVERY</td>
<td>K.N. MURTHY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>IMPACTED PROJECT MANAGER - N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
METRO RAIL DESIGN CRITERIA

SECTION 12

SAFETY, SECURITY, AND SYSTEMS ASSURANCE
# TABLE OF CONTENTS

12.1 INTRODUCTION ............................................................................................................... 1  
  12.1.1 Abbreviations and Acronyms ........................................................................... 1  
  12.1.2 References ...................................................................................................... 2  
  12.1.3 Codes, Standards and Regulations ................................................................. 3  
12.2 SYSTEM SAFETY ............................................................................................................. 4  
  12.2.1 Specific Provisions for Safety .......................................................................... 4  
  12.2.2 General ............................................................................................................ 4  
  12.2.3 System Safety Design Approach ..................................................................... 5  
  12.2.4 Station and Guideway Design ......................................................................... 6  
  12.2.5 LRT Photo Enforcement .................................................................................. 7  
  12.2.5.1 Description ...................................................................................... 7  
  12.2.5.2 System Functional Requirements ................................................... 7  
  12.2.5.3 Servicing and Equipment Maintenance ........................................ 10  
  12.2.5.4 Intersection Design ....................................................................... 10  
  12.2.5.5 Data Communications ................................................................... 11  
12.3 SECURITY ...................................................................................................................... 11  
  12.3.1 Introduction .................................................................................................... 11  
  12.3.2 General Requirements .............................................................................. 11  
  12.3.3 Basis for Security Strategy ............................................................................ 12  
  12.3.4 Security Plan ................................................................................................. 12  
  12.3.4.1 Rationale for Creating a Security Plan .......................................... 12  
  12.3.4.2 Definition of a Security Plan ...................................................... 1243  
  12.3.4.3 Relation to Other Documents ................................................ 13  
  12.3.4.4 Scope .................................................................................... 13  
  12.3.4.5 Goals and Objectives ................................................................ 1344  
  12.3.4.6 Goals ................................................................. 1344  
  12.3.4.7 Objectives ............................................................................. 14  
  12.3.4.8 Contents of a Security Plan ..................................................... 14  
  12.3.5 Families of Technologies ........................................................................... 16  
  12.3.6 Vehicles ........................................................................................................... 1647  
  12.3.7 Communications ............................................................................................. 17  
  12.3.8 Station and Guideway Design ....................................................................... 19  
  12.3.9 Security Systems Integration ......................................................................... 19  
  12.3.10 Characteristics of an Integrated System..................................................... 20  
12.4 SYSTEM ASSURANCE .................................................................................................. 20
<table>
<thead>
<tr>
<th>12.4.1</th>
<th>Introduction</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4.2</td>
<td>Scope</td>
<td>20</td>
</tr>
<tr>
<td>12.4.2.1</td>
<td>Design Criteria</td>
<td>20</td>
</tr>
<tr>
<td>12.4.2.2</td>
<td>Definitions</td>
<td>21</td>
</tr>
<tr>
<td>12.4.3</td>
<td>Maintainability</td>
<td>22</td>
</tr>
<tr>
<td>12.4.3.1</td>
<td>Vehicle</td>
<td>22</td>
</tr>
<tr>
<td>12.4.3.2</td>
<td>Systems</td>
<td>23</td>
</tr>
<tr>
<td>12.4.3.3</td>
<td>Activities</td>
<td>23</td>
</tr>
<tr>
<td>12.4.4</td>
<td>Reliability</td>
<td>24</td>
</tr>
<tr>
<td>12.4.4.1</td>
<td>Vehicle</td>
<td>24</td>
</tr>
<tr>
<td>12.4.4.2</td>
<td>Systems</td>
<td>24</td>
</tr>
<tr>
<td>12.4.4.3</td>
<td>Activities</td>
<td>25</td>
</tr>
<tr>
<td>12.4.5</td>
<td>Availability</td>
<td>28</td>
</tr>
<tr>
<td>12.4.5.1</td>
<td>Scope</td>
<td>28</td>
</tr>
<tr>
<td>12.4.5.2</td>
<td>Calculation</td>
<td>28</td>
</tr>
</tbody>
</table>
SAFETY, SECURITY AND SYSTEMS ASSURANCE

12.1 INTRODUCTION

This section provides Design Criteria relative to safety, systems assurance and security issues. Matters dealing explicitly with Fire/Life Safety issues are covered separately in the Metro Fire/Life Safety Design Criteria. The definitions in the APTA Lexicon apply unless modified herein.

12.1.1 Abbreviations and Acronyms

The following abbreviations and acronyms are used in Section 12 of these Criteria.

<table>
<thead>
<tr>
<th>Abbreviation / Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>APTA</td>
<td>American Public Transportation Association</td>
</tr>
<tr>
<td>ATMS</td>
<td>Advanced Transportation Management System</td>
</tr>
<tr>
<td>HRV</td>
<td>Heavy Rail Vehicle</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CM</td>
<td>Corrective Maintenance</td>
</tr>
<tr>
<td>CPTED</td>
<td>Crime Prevention Through Environmental Design</td>
</tr>
<tr>
<td>CNG</td>
<td>Compressed Natural Gas</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>FHWA</td>
<td>Federal Highway Administration</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure Modes and Effects Analysis</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom Of Information Act</td>
</tr>
<tr>
<td>FRACA</td>
<td>Failure Reporting and Corrective Action</td>
</tr>
<tr>
<td>FTA</td>
<td>Federal Transit Administration</td>
</tr>
<tr>
<td>IES</td>
<td>Illuminating Engineering Society</td>
</tr>
<tr>
<td>LRV</td>
<td>Light Rail Vehicle</td>
</tr>
<tr>
<td>Metro</td>
<td>Los Angeles County Metropolitan Transportation Authority</td>
</tr>
<tr>
<td>MDBF</td>
<td>Mean Distance Between Failure</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failure</td>
</tr>
<tr>
<td>MTBSF</td>
<td>Mean Time Between Service Failure</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
</tr>
<tr>
<td>MTTFF</td>
<td>Mean Time To First Failure</td>
</tr>
</tbody>
</table>
12.1.2 References

In light of the tragic events of September 11, 2001, enhancing the security of the rail system is expected to be one of the highest priorities of Metro. FTA, APTA, FEMA, TRB, The National Academies and other related organizations have generated extensive information on this issue in recent years. Their website brings together much of this information. They also included links to other related websites that contain discussions of issues, actions which can be taken, guidance and training opportunities. For example, the TRB (http://www.TRB.org/SecurityPubs) website, which is sponsored by the TRB Committee on Critical Transportation Infrastructure Protection (ABE40), continues to be updated as more information becomes available. TRB provides monthly updates, summarizing pre- and post-September 11 transportation security activities. In addition to the TRB website, other transportation resource and their websites are listed below:

- Recommended Practice for the Selection of Cameras, Digital Recording Systems, Digital High Speed Train-lines and Networks for Use in Transit Related...
12.1.3 Codes, Standards and Regulations

The items included in this section shall meet or exceed safety-related codes, standards and regulations, as amended by applicable local, state and federal authorities.

Where the requirements stipulated in any such document, or in this document are in conflict, the stricter requirement shall govern.

Unless specifically noted otherwise herein, the latest editions of the code, standards and regulations that are applicable at the time the design is initiated shall be used. If a new edition or amendment to a code, regulation or standard is issued before the design is completed, the...
design shall conform to the new requirement(s) to the extent practical or required by the government agency forcing the change.

The applicable codes, standards and regulations include the following:

1. Americans with Disabilities Act (ADA).
6. Crime Prevention Through Environmental Design (CPTED)
8. California Code of Regulations (CCR): Title 24, Title 8, Title 19.

12.2 SYSTEM SAFETY

12.2.1 Specific Provisions for Safety

Specific provisions for safety are addressed in the specific design criteria for each rail system element. Certain provisions accounted for elsewhere in the Rail Design Criteria are cited in this section to highlight how safety shall be collectively incorporated in specific design elements.

This section of the design criteria provides design guidance in System Safety for systemwide aspects and phases of the Metro Rail Transit System.

12.2.2 General

Safety is a primary consideration through the evolution of each Light-Rail Transit and Heavy Rail Transit System, from preliminary engineering through revenue operations. To achieve safety goals, all applicable codes and regulations, augmented by modern safety engineering technology and industry standards, are to be used to ensure that each Metro Rail Line achieves a level of safety that equals or exceeds that of the rail transit industry.

Safety can be achieved by eliminating, minimizing, or controlling hazards through analysis, review, and design selection. The objectives of the safety program are the elimination or control of condition that may endanger human life or property. It includes acceptable and unacceptable
hazardous conditions. Unacceptable Hazardous Condition means a hazardous condition determined to be an unacceptable hazardous condition under the Accident /Hazard Matrix set out at APTA’s Manual for the Development of Rail Transit System Safety Program Plans. Acceptable Hazardous Condition means a hazardous condition inherent to the operation of the transit system which, based on review and concurrence of the transit agency management and the Department, is impractical to eliminate, but may require special procedures to reduce risk of accident.

To achieve these objectives and provide a level of safety that equals or exceeds that of other rail transit systems requires a comprehensive and complete safety program.

The safety program shall establish safety requirements and verify safety of design through various analyses.

Transit station construction should consider accepted Crime Prevention Through Environmental Design (CPTED) standards within underground station and on at-grade platforms or plazas. The basic function of public transit is to efficiently and safely move the public from one location to another. CPTED promotes open space and the use of structure and seating design to inhibit loitering.

Safety program(s) shall ensure the Visibility Triangle of both the cab of a moving train along the entire right-of-way and at stations, from adjacent moving automobiles, bicycles, and pedestrians. The Visibility Triangle shall be improved by removing visibility obstructions where practical, but never degraded by designing other obstructions such as equipment cabinets, TPSS buildings, trees, etc.

### 12.2.3 System Safety Design Approach

Prior to preparation of specifications and design development, a Preliminary Hazard Analysis (PHA) shall be prepared which analyzes the loss or malfunction of each operational function and categorizes its affect on the equipment, personnel, patrons and general public to determine the associated hazard level as defined in the referenced documents.

According to the results of the PHA, individual contractors may be required to develop more detailed safety analyses for their specific contracts. In addition, particular contract specifications may require contractors to prepare System Safety Program Plans. Contractor submittals of required plans and analyses shall be scheduled as early in the contract design phase as possible, with the Conceptual Design Review phase as a target for submittal of Systems Safety Program Plans. Submittals early in the design phase facilitate determination that the contractor's design satisfies the safety requirements of the contract.

Identified hazards shall be eliminated or controlled as applicable, using the following hierarchy of hazard resolution:

1. **Design for Minimum Hazard**
   
   To the extent permitted by cost and practicality, identified hazards shall be eliminated or controlled by the design of equipment and facilities.

2. **Safety Devices**
Hazards that cannot reasonably be eliminated or controlled through design shall be controlled to the extent practicable to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices. Provision shall be made for periodic functional checks of safety devices.

3. Warning Devices

When neither design nor safety devices can reasonably, effectively eliminate or control an identified hazard, devices shall be used to the extent practicable to detect the hazard and to generate an adequate warning signal to provide for operating personnel/public reaction. Warning signals and their application shall be designed to minimize the probability of incorrect operating personnel/public reaction to the signals.

4. Procedures and Training

Where it is impossible to reasonably eliminate or adequately control a hazard through design or use of safety and warning devices, procedures and training shall be used to control the hazard. Precautionary notation shall be standardized, and certain safety-critical tests shall require certification of personnel.

12.2.4 Station and Guideway Design

Safety at stations and along the guideway shall be reflected in the following characteristics:

Visibility - For Visibility Triangle, Safe Stopping Point and Crossing Sight Distances refer to FHWA (Federal Highway Administration) Grade Crossing Handbook, Chapter III.C Assessment of Crossing Safety and Operation, Engineering Study.

Designs shall include sight lines respective of moving trains and pedestrians, providing maximum visibility, with no hidden spaces behind objects and corners. This includes trees, shrubbery, fencing, alcoves and the like. Additionally, locks shall be provided on doors to all adjacent wayside support structures. Landscaping and lighting levels shall support the intended means of surveillance.

Platform Layout - Platforms shall be designated with paid and non-paid areas where proof-of-payment fare enforcement is applied. The entrance to “fare enforcement zones” on each platform shall be clearly identifiable to separate the paid passengers from non-paid passengers.

Illumination - Illumination shall be in conformance with Metro, IES, and ANSI criteria and recommendations within the station and along station perimeters with no dark or shadowy areas, including Park and Ride areas at designated stations.

Materials and Construction - In addition, any surfaces or equipment accessible to the public, such as emergency or passenger assistance telephones, station floors and walls shall comply with the architectural requirements and vandal-resistant design.

Service Vehicle Parking – Each station shall have provision for service vehicle parking.
**De304.12**  Revision 2  05/09/12
Metro Baseline  03/15/10

**Signage** - Adequate signage shall be created and posted in plain view similar to those used in the Metro rail system.

**Landscaping** - Landscaping around the platforms and parking, and along the Right-of-Way shall be selected to allow for minimal upkeep and to prevent persons and objects from being hidden or concealed. All areas of the stations shall be in clear view from adjoining streets and not hampered by landscaping. When police or security patrol units drive by the stations they shall be able to observe all areas of the stations without certain points being concealed by the landscaping.

### 12.2.5 LRT Photo Enforcement

**12.2.5.1 Description**

The purpose of the following design criteria is to describe the Photo Enforcement System and compatible equipment to be used with Light Rail Transit (LRT) facilities (non-exclusive and semi-exclusive) within street/intersection right of way where crossing gates will not be used.

**12.2.5.2 System Functional Requirements**

The following general requirements shall apply to public transportation corridors, where motorists' traffic makes left or right turns or straight movement that crosses the corridor.

**A.** The Photo Enforcement system shall:

- Comply with intersection designs and be able to receive a direct feed from the automated train warning system or signal light controller to initiate enforcement mode capturing all applicable phases in compliance with California Vehicle Code (CVC) statutory requirements
- Utilize detectors (invasive or non-invasive) that accurately capture vehicle presence and profile to measure vehicle speed
- Employ camera equipment including auxiliary strobe equipment that meets or exceeds issuance criteria established by Metro
- Meet all requirements described in the CVC relating to photo enforcement systems
- Capture motor vehicle movements that violate straight movement, the dedicated left or right turn traffic signals. These movements are typically left or right turn movements that parallel then cross the LRT right-of-way
- Interface with a dedicated automated train warning system or signal light controller
- Capture infractions of motor vehicles with no minimum speed threshold as required per Metro Systems Safety
- Provide a minimal curbside footprint (visibly appealing installation and hardware) customizable to Metro design guidelines

**B.** Selection of the enforced approach shall be based on (but not limited to):

- Traffic analysis;
- Policy to be utilized for LRT
C. All applicable intersections shall have a minimum of two cameras, provided for each left turn (one digital still camera and one digital video camera) and two cameras provided for each right turn (one digital still camera and one digital video camera), with additional numbers based on intersection configuration and traffic analyses. Rear cameras may also be required based on the intersection configuration.

D. The functional requirements of the main components shall include, but not be limited to, the following:

- One digital still camera (21 Mega Pixel)
- One digital video camera
- One secure, weatherproof housing for both cameras
- One digital recording device and camera controller (with capacity for up to 30 days of stored video and still images)
- One camera pole (per unit)
- One auxiliary flash unit with pole
- One stop bar flash unit with pole
- One detection unit per approach (invasive or non-invasive)

E. Capabilities of the main components shall include, but not be limited to, the following:

1. General Characteristics:
   - Designed to withstand vandalism and other malicious intent.
   - Designed to withstand the elements (24/7 operating capability).
   - Designed to include “break away” capability in case of collision
   - Height: Dependent on individual installation
   - Designed for easy access by law enforcement personnel and field service technicians
   - Compliant with jurisdictional engineering standards
   - Designed for aesthetics (minimal footprint)
   - Engineered to provide a simple, easy installation process
   - Designed for maximum adaptability and flexibility
   - Interchangeable and easily replaceable components
   - Remote access ready

2. Security
   - Strengthened cabinet
   - Shatter-proof glass/plexiglass
   - Multi point security locking mechanism

3. Interface
   - Designed for ease of use
   - High Speed internet or Ethernet communication connection
• 120 V AC power
• Signal isolation detection of signal phases (limiting the interface connection to the intersection controller).
• Compatible with other photo enforcement approaches currently in use within the Metro Photo Enforcement program

F. Detection system

1. In ground (inductance)
   • Loop detection control and interface with camera system.
   • Loop configuration designed to maximize capture of vehicle profile and speed data.
   • Pull boxes, power supply line, direct line connection to camera system, and in ground wiring.

2. Radar
   • Virtual loop detection control and interface with camera system.
   • Designed to maximize capture of vehicle profile and speed data.
   • Power supply line, antenna for wireless connection to camera system, power supply line, and pole (or mounting hardware for using existing intersection poles).

3. Laser
   • Virtual loop detection control and interface with camera system.
   • Designed to maximize capture of vehicle profile and speed data.
   • Pull boxes, power supply line, direct line connection to camera system, and in ground wiring.

G. Flashes

1. 1200 or 1600 watt flash unit (dependant on the intersection configuration needs)
2. Recharge in under 1 second (to capture two photos in succession)
3. Total control software for flash intensity settings
4. 120 V AC power
5. Direct line feed from camera system to fire flash

H. Signage

1. Designed to meet CVC and California state requirements
2. One sign posted at each approach to the enforced intersection (whether or not a camera system is enforcing the approach)
3. Posted a minimum of 500 feet back from intersection

I. Camera System

1. 21 mega pixel digital still camera system
2. Professional grade, high speed glass lenses
3. Designed to maximize image quality with remote functionality
4. Software allows remote access to camera system to adjust settings
5. Data collection system capable of remotely uploading data to secure server at regular intervals
6. Incorporates multiple vehicle detection options
7. Monitors up to 8 lanes of traffic
8. Is capable of capturing multiple simultaneous violations
9. Designed with easily interchangeable components and hardware
10. Able to remotely send error messages and warning alerts in case of system failure

12.2.5.3 Servicing and Equipment Maintenance

Photo Enforcement equipment will require regular servicing (collection of data and replacement of consumable supplies) and normal maintenance.

12.2.5.4 Intersection Design

Provisions for power and communication will be included in the intersection design to accommodate Photo Enforcement power and data communication/upload.

Location of Equipment (such as pole base(s) and loop(s)) will be determined and designed based on individual intersection designs and requirements.

A. Conduits and pull Boxes

For Communications, 3 inch minimum branch conduit to be run from each device location to nearest photo enforcement communication pullbox or junction box located within area of pole base.

For Power, minimum 3” size branch conduit shall be run from each Pole base location to the designated power connection for installation of power wiring.

Conduits shall have all sharp edges removed.

Conduits shall be sealed and watertight

The conduit/pull box system shall be exclusively designed and built for photo enforcement use. No other system could share photo enforcement conduits and pull boxes.

B Connections to Photo Enforcement Equipment

Connections from the power and the communications at locations of Poles shall utilize conduit stub-ups

Conduit stub-ups shall be used (locations with provisions to install additional poles in future as required).

C Electrical
Power conduit shall be installed to run power circuits from the power source to each pole. Conduit shall utilize intermediate power pull boxes appropriate for the length of main conduit run(s). Conduit arrangement should use main run to each general location of equipment with branch runs continuing between junction box and each pole location.

Dedicated 120V, 60 Hz, and 20 amp circuits shall be provided.

Power wiring shall be kept separate of data communications cabling and shall be run continuously, without splices, from source to each pole location including identified future locations.

D. Data Communications Equipment

Data communications cabling shall be kept separate of power wiring; and shall be run continuously, without splices, from source to System Components location.

12.2.5.5 Data Communications

High Speed Communication Link Requirements for each site will require:

- All infrastructure conduits and communication link requirements for leased or Metro provided data lines.
- The ability to upload collected data at regularly scheduled intervals for processing.

12.3 SECURITY

12.3.1 Introduction

Design for Rail facilities shall ensure a high level of security for patrons and operating personnel. Facility design and operating procedures shall promote a sense of well-being for 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 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 and the design of facilities. Through these criteria, security considerations shall be integrated into all aspects of the design, equipment selection, architectural concepts, procedures, and operations. Additionally, it shall enable trade-off studies to be performed to achieve a balanced, comprehensive level of system wide security.

12.3.2 General Requirements

The system shall provide 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 Rail system. In general, the design of the rail facilities shall include features that enhance patron and personnel security.
Standards of safety shall also apply to vehicles. For example, vehicles shall be designed with unbroken lines of sight, absence of blind areas, and adequate vehicle lighting shall support the intended means of surveillance.

12.3.3 Basis for Security Strategy
Rail system design shall consider preparing and implementing security strategies that are consistent with Metro’s comprehensive system security plan that are based on a threat and vulnerability assessment (TVA). The results of the TVA can be used to help determine implementation priorities.


Metro will prioritize risks through threat TVA’s and select sets of countermeasures for each rail project that provide the best overall risk reduction for the system as a whole.

12.3.4 Security Plan
The purpose of a Security Plan is to enhance and maintain the security of Metro’s operation by establishing a framework in which a comprehensive (i.e., encompassing the entire security “spectrum”), effective and sustainable security program can be developed, implemented and maintained. A Security Plan also enables Metro to:

- Describe how various elements of its security program integrate;
- Establish security program roles and responsibilities, thereby ensuring tasks are assigned, understood, documented, tracked and organized in a consistent manner;
- Identify its partners and stakeholders in regards to enhancing and maintaining the security of its operations;
- Adjust its security preparations and operations in response to changing circumstances;
- Implement various security program elements, e.g. security measures, policies and procedures, etc. that can be measured, audited, and evaluated, to determine the effectiveness of Metro’s security program.

12.3.4.1 Rationale for Creating a Security Plan
Creating a Security Plan permits Metro to enhance its capabilities to prevent, mitigate, respond to and recover from a terrorist attack or security incident in a systematic and consistent way. A Security Plan outlines the measures Metro will use to secure its passengers, employees, freight, tenants, assets, operations, facilities and communications and the public against potential and actual terrorist attacks or security incidents. Hence, a Security Plan helps Metro to establish and maintain a formal and comprehensive security program and serves as a blueprint for all of Metro’s security activities.

The Security Plans shall be developed in consultation with appropriate partners, including transit police, sheriffs and police and other first responders, to help assure it is comprehensive and achievable by all stakeholders.

12.3.4.2 Definition of a Security Plan
A Security Plan is a strategic and agency sensitive document that:

- Sets security goals and objectives based on the results of a comprehensive TVA;
- Establishes a framework, reflecting the full security “spectrum” (prevention, mitigation, response and recovery) for addressing security threats and risks;
- Reflects a coordinated approach to Metro system security that integrates all available resources to enhance protection from potential terrorist activities and/or security incidents;
- Identifies key assets that require protection (as a result of the TVA);
- Identifies, and establishes measures to be implemented to address risks identified in the TVA (i.e., prevention and mitigation measures), including measures applicable at each alert level (e.g., low, medium, high);
- Clearly identifies coordinated and related plans (e.g., Emergency Management Plan, Business Recovery Plan) procedures, protocols and responsibilities for implementing Metro’s security program;
- Identifies a timetable or action plan to introduce new measures that are required to address priority risks, such as interim and long-term measures as appropriate;
- Gives full consideration to actions or resources required to support the implementation of various security program elements (e.g., security and emergency response training and awareness, information technology security, document control, etc.).

12.3.4.3 Relation to Other Documents

A Security Plan is part of a holistic approach to security. The Security Plan establishes a framework for Metro’s security program. The Security Plan may operate as part of a suite of other related plans, which in turn references more specific procedures. Plans that could be referenced by a Security Plan shall include, but are not limited to: the Threat and Vulnerability Assessment, Business Continuity Plan, Fire Evacuation Plan, Security Escalation Plan (Alert Levels), Information Management Plan, etc.

12.3.4.4 Scope

Metro’s Security Plan represents its commitment to continuously improving the security of its operations and services and to integrating security into all of its activities. Hence, the Security Plan shall address security risk, where appropriate for all of Metro’s activities as well as all of its organizational units, employees, and contractors.

12.3.4.5 Goals and Objectives

The Security Plan shall establish goals and objectives for the purposes of identifying goals as broad and general statements, while objectives shall be more focused and specific statements.

12.3.4.6 Goals

The overall goal of a Security Plan shall be to enhance the level of security and protection afforded to its employees, customers and assets from various security threats including
terrorism, crime and disorder. The Plan may also identify other goals applicable to Metro’s operation.

12.3.4.7 Objectives

The Security Plan shall include the following objectives:

- Enhance Metro’s ability to prevent, mitigate, respond to and recover from a terrorist attack and or security incident;
- Describe current security program elements and define associated security measures;
- Define roles and responsibilities for all personnel with regards to security;
- Demonstrate how security concerns are factored into relevant aspects of Metro’s activities;
- Establish processes for maintaining, evaluating, and modifying the Plan;
- Establish processes for identifying, receiving input (e.g., from employees, contractors and the public), reporting on and addressing security concerns, security incidents, suspicious activities, etc.;
- Establish processes for interfacing with partners, stakeholders and the public;
- Establish processes for reviewing and assessing Metro’s implementation of and adherence to the Plan and other related documents;
- Identify security program training requirements;
- Establish processes for investigating security incidents or suspicious activities;
- Ensure potential security implications are taken into account when making decisions regarding Metro’s rail operations.

12.3.4.8 Contents of a Security Plan

12.3.4.8.1 Minimum Contents

At a minimum, a Security Plan shall contain:

- A summary of and reference to the TVA;
- A description of security-related roles and responsibilities;
- A description of Metro’s current security program elements and reference to associated security measures; and security capacities (e.g., personnel, technology, resources, tools, instruments, etc);
- A description of the measures in place to address the risks identified by the TVA (including under various alert levels) and a reference to the relevant procedures for implementing those measures;
- A description of Metro’s security training and awareness programs;
- A description of Metro’s security exercise program(s);
12.3.4.8.2 Content Limits

The Security Plan shall not include detailed descriptions of the procedures, resources, tools etc required to implement the plan. Rather it shall identify the measure, tool, resource, etc., and reference the other relevant documents (e.g., procedures, inventories, resource allocation, etc.) where the more detailed and required security plan implementation information can be found. For example, by providing the file number or identifying its custodian. The three main reasons for this are:

- First, such detail would make the plan too long and more difficult to use;
- Second, details about Metro would make it more difficult to serve its intended audience and purpose: i.e., as a strategic document and framework; and
- Third, Metro’s entire security program shall not be in one single document, in case the document should fall into the wrong hands.

The Security Plan shall also indicate where the referenced documents can be found (e.g., by providing the file number or identifying its custodian).

12.3.4.9 Protection of Sensitive Security Information (SSI)

By law, transit agencies are required to categorize and protect sensitive security information (SSI). Protecting SSI means restricting its distribution and controlling access to it. By law, SSI is not subject to disclosure under the FOIA or to state “Sunshine Laws.” It is also not available under discovery in civil litigation, and it is not required to be part of the record in a federal rulemaking.

SSI is based on the regulations in 49 CFR Parts 15 and 1520. Its purpose is to help transit agencies prevent the unauthorized disclosure or dissemination of SSI while preserving the public’s “right to know” about transit systems and operations.

For work-in-progress documents and upon approval, a security plan and other appropriately designated transportation information shall be designated, marked, and controlled as a Sensitive Security Information (SSI) document. Metro is responsible for accounting for and controlling the distribution of its security plan, as well as assigning and inventorying numbered copies, requiring that older versions be returned when updated versions are distributed, and for ensuring that the security plan (i.e., the original and approved copies) is properly safeguarded. Metro may consider distributing an abbreviated, sanitized version of the security plan with SSI.
removed for issue to persons who have not been granted access to Metro SSI and have the need to know the information.

12.3.5 Families of Technologies

Each rail project shall select specific countermeasures to implement, which are available as many options. They may have variations designed for different purposes or locations. Analyzing these technology differences within a single family to determine which variation best meets a particular need is important. For example, the Figure below illustrates families of technologies for exterior sensors which could be used for shops and yards. The advantages and disadvantages for many of these types of sensors are described in the Intrusion Detection for Public Transportation Facilities Handbook.

12.3.6 Vehicles

Vandal resistant materials shall be used on seats, seat backs, windows, trim panels, and floor coverings. The use of vandal resistant materials shall also be used for the exterior finish of the vehicle including windows capable of withstanding thrown objects and other projectiles.

Each project shall plan and design for consideration of the visibility triangle from the cab of a moving train at planned speeds.

Systems designs shall include provisions for devices capable of being activated by remote control that could shut off the vehicle power supply.
12.3.7 Communications

At Metro, communications are essential to managing routine and emergency functions, coordinating system activities, and functioning as both an asset and security tool. For example, these systems include:

Radio – Two-way voice communications over radio between train operators and central control dispatch personnel and emergency and maintenance personnel.

TPIS – Transit Passenger Information System for announcements to the stations and ancillary areas from the ROC or local communication location; phone access and access from the Emergency Management panel.

Telephone – All Metro required phone service including but not limited to Emergency Telephone (ETEL), Maintenance Telephones (MTEL), Passenger Telephones (PTELs), and Gate Telephone (GTEL) and Elevator Telephone (LTEL) at stations monitored by the Rail Operation Control Center (ROC).

Intercom – An intercom system provides two-way voice communications between passengers and train operator.

Silent Alarm – Silent alarm capability activated by the operator to trigger an annunciation at ROC indicating an emergency situation.

Closed Circuit Television – Provisions for a comprehensive CCTV System that will allow the system control to monitor activities at the stations and major intersections, including:

- Pan/Tilt/Zoom cameras on entrance/exit to stations and platforms
- Pan/Tilt/Zoom cameras on TVM’s and on the entire platforms
- Fixed CCTV camera or the home position of a PTZ camera on any room, cabinet, or enclosure housing network appliances, manual override or local control capabilities.
- Pan/Tilt/Zoom cameras shall be installed to monitor all intersections where the trains are in street run, and intersections where an interlocking is located, the cross passages, tunnel portals, bridges, yards, and other areas required by Section 9.9, Closed-Circuit Television (CCTV).
- Pan/Tilt/Zoom cameras on key street/rail intersections (i.e., high volume pedestrian crossings, event stations, etc.)
- Pan/Tilt/Zoom cameras that monitor required phone locations
- Pan/Tilt/Zoom cameras that monitor rail tunnel portals, looking both inward and outward
- Pan/Tilt/Zoom cameras that monitor underground railway tunnels
- Pan/Tilt/Zoom cameras that monitor Parking Lot entrance and exit and for the general observation of the parking lot.
- Pan/Tilt/Zoom cameras that monitor station plaza areas.
- Pan/Tilt/Zoom cameras (dedicated) that monitor each escalator at each landing.
• Pan/Tilt/Zoom cameras that monitor elevator entrance areas from the outside of the elevator, on plaza, courtyard or platform (etc.) areas.

• **Dedicated fixed cameras which shall be grip free vandal proof corner mounted** Pan/Tilt/Zoom cameras (dedicated) that monitor each elevator entrance inside the elevator and that provides full coverage of the cab interior. In some cases separate camera could be required to monitor the elevator interior. Note: two door elevators should have minimum two cameras.

• **IP Pan/Tilt/Zoom (PTZ) cameras installed to achieve 100% coverage in the public areas of the station with cameras at their “home” position (in other words, 100% coverage should be achieved without requiring PTZ).**

• Pan/Tilt/Zoom camera installed to provide full coverage in parking lots, including exits and entrances.

• Pan/Tilt/Zoom cameras shall be installed in parking structures in elevators, elevator lobbies (on each level), enclosed stairways, entrances and exits, and shall provide 100% coverage of parking areas.

• Monitoring at the ROC and/or other strategic locations

  A remote plug-in access CCTV jack box which provides access to the CCTV system for fire and law enforcement personnel shall be placed at an above ground location nearby an underground station entrance. CCTV jack box also needs to have an intrusion bug, and signage inside listing ROC’s phone number. The exact location shall involve input from the Fire, Life Safety Committee.

Intrusion detection – provide monitoring of designated doors, windows, gates and fences to detect authorized and / or unauthorized entry.

**Operations Control Center Emergency Communication** – Provide communication between police and security personnel and rail operations staff.

**Network Failure/Cyber Attack** – Rail system relies on computerized networks to facilitate operations and enhance efficient service delivery, which makes it vulnerable to network failure and cyber attacks. Refer to Metro Rail Design Criteria Section 9.19, Cyber Security for Rail Communication Networks/Control systems While this document does not offer specific considerations on how to protect computer networks, it is crucial to understand their importance to operating and communicating among Metro staff as well as with partner organizations and the public-at-large. Network failure may be caused by faulty or damaged internal components, direct cyber attack to Metro’s network, direct attack to a peripheral system or network, or even a blanket computer virus. The result may be loss of communications or operations capabilities as well as misinformation by hacking into a web site or server.
12.3.8 Station and Guideway Design

Visibility - For Visibility Triangle, Safe Stopping Point and Crossing Sight Distances refer to FHWA (Federal Highway Administration) Grade Crossing Handbook, Chapter III.C Assessment of Crossing Safety and Operation, Engineering Study.

Designs shall include sight lines respective of moving trains at planned speeds, providing maximum visibility, with no hidden spaces behind objects and corners. This includes trees, shrubbery, fencing, alcoves and the like. Additionally, locks shall be provided on doors to all adjacent wayside support structures. Landscaping and lighting levels shall support the intended means of surveillance.

Platform Layout - Platforms shall be designated as paid and non-paid areas where fare proof-of-payment and enforcement is applied. The entrance to “fare enforcement zones” on each platform shall be clearly identifiable to separate the paid passengers from non-paid passengers.

Illumination - Illumination shall be in conformance with appropriate Metro and industry standards within stations and along station perimeters without causing dark or shadow areas, including Park and Ride areas at designated stations.

Materials and Construction - In addition, any surfaces or equipment accessible to the public such as emergency or passenger assistance telephones, and station floors and walls shall comply with the architectural requirements and vandal-resistant design.

Service Vehicle Parking - Each station shall have designated area for service and revenue collection vehicle parking.

Signage - Adequate signage shall be created and posted in plain view similar to those used in Metro rail system.

Landscaping - Landscaping around the platforms and parking and along the Right-of-Way shall be selected to allow for minimal upkeep and to prevent persons and objects from being hidden or concealed. All areas of the stations shall be in clear view from adjoining streets and not hampered by landscaping. When police or security patrol units drive by the stations or right of way they shall be able to observe all areas of the stations without certain points being concealed by the landscaping.

12.3.9 Security Systems Integration

Enhanced security in the transit environment depends on three elements:

1. Appropriate design, of physical objects that together form the transit security system;

2. Relevant information and data, such as video images, being captured and delivered to the appropriate Metro representative and/or decision makers; and

3. Training focused on human factors to maximize deterrence, detection, minimization, and response/recovery.

Security systems integration is essential for these factors to work together. Security systems integration implies that each type of security system and its subsystems are linked together to enhance overall transit system security.
12.3.10 Characteristics of an Integrated System

In the same way that a system has multiple facets, systems integration occurs over spatial, temporal, institutional, functional, and data dimensions. An integrated system has the following characteristics:

- **Information generation**: synthesizing data into information that can be used for decision making; for example, automatically identifying suspicious activity by flagging anomalies in a stream of visual or auditory data.

- **Communication**: delivering the information to relevant decision makers, including external agencies and the public, where applicable.

- **Multiple internal and external organizations**: linking multiple agencies, enabling coordinated action.

- **Multiple devices**: linking multiple devices, including single types of devices from multiple vendors and multiple types of devices to engage a response; for example, for an unauthorized access attempt a video camera would be engaged to record movement and the event.

- **Multi-directionality**: enabling multi-way communications among devices and control centers where needed.

- **Redundancy**: maintaining the functionality of a security system during an attack is critical, especially if one part of the system has been disabled; and

- **Persistence**: preserving the ability to investigate past system activation or status.

12.4 SYSTEM ASSURANCE

12.4.1 Introduction

The primary objective of the Rail project system assurance design criteria is to provide guidelines to provide the highest levels of equipment and service reliability and availability together with optimized maintenance burden.

A program of sufficient depth and scope shall be developed and implemented to assure attainment of and to demonstrate compliance with all systems assurance goals/requirements. During all phases of the Rail project, design, evaluation, and test, the achievement of high levels of product systems assurance shall be a paramount consideration.

In achieving compliance, the inherent interrelationship of safety, reliability, maintainability and availability principles and methods in analysis, design, test, demonstration, and failure correction shall be recognized. The system assurance and safety goals/requirements shall be considered as dependent on each other.

In addressing a problem of noncompliance with a given requirement, an integrated approach to safety, reliability, maintainability and availability shall be employed. This shall recognize that while there may be separate reliability maintainability and availability actions that could each solve the problem, either action might impact safety.

12.4.2 Scope

12.4.2.1 Design Criteria
The Consultant and/or the Contractor on ALL stages of the design (conceptual, preliminary and final) and Construction (as-built) shall develop a System Assurance Program Plan for Metro's review and approval. These System Assurance Design Criteria provide guidance for the following sub-systems within a rail system:

- Vehicles
- Fare Collection Systems
- Traffic Signal and Train Control Systems
- Traction power
- Communications Systems
- Central/Satellite Control Facilities
- Maintenance Facilities

The system assurance quantitative goals/requirements provided shall be developed and used as a baseline during conceptual and preliminary engineering. The goals/requirements shall be refined and enhanced through improved design depending on the technology utilized and ultimate operational requirements. Accordingly, it is possible that during the various testing phases or warranty period a design deficiency is discovered. Such deficiencies shall be identified and mitigated or eliminated through design enhancements.

There are tradeoffs between cost, safety, security, risk, availability, reliability and maintainability. It is the intent to find the best balance between these items. Design Criteria shall define the minimum goals and prohibit any single point failures for each of these requirements

These System Assurance design criteria for Rail System are based on performance criteria that affect passenger service and the operational reliability of the system.

12.4.2.2 Definitions

Service Affecting Failures: Some failures may have a direct impact on the ability of the operator to complete an end-to-end trip within 3 (three) minutes of the schedule, while maintaining a safe and comfortable environment for the passengers. This can include onboard and some wayside systems. Infrastructure items with the potential to result in service affecting failures are those where there is a direct impact on passengers (e.g. Fare Collection), or where a safety or security function is unavailable (e.g., emergency communication, Train control systems).

Non-Service Affecting Failures: Failures of systems or functions which do not affect service, however, require corrective maintenance. Cumulative non-service affecting failures can eventually result in service affecting failures.

Availability: The fraction of time within which a system is actually capable of performing its mission.

Mean Time Between Failures (MTBF): The total operating time (t) accumulated by the total population of items divided by the total number of failures occurring within the population of items during time (t). A failure is defined as the event, or inoperable state, in which any item or part of an item does not, or would not perform as previously specified, regardless of the operational state of the system or subsystem. Includes service and non-service affecting failures.
Mean Distance Between Failures (MDBF): The total operating distance (d) accumulated by the total population of items divided by the total number of failures occurring within the population of items during distance (d). A conversion factor is often used between MTBF and MDBF.

Mean Time To Repair (MTTR): The ratio of the total active corrective maintenance time, Tcm, expended during a given time interval, t, for the total population of identical items to the total number of relevant failures, F, requiring corrective maintenance which occur within the population of items during the same time interval (t), expressed as $F_t$. It is expressed quantitatively as:

$$MTTR = \frac{\text{Tcm}(t)}{F_t}$$

Active Maintenance Time: The total time expended to troubleshoot and fault-isolate a functional failure, remove and replace/repair faulty items, and verify that the fault has been corrected to operational specifications.

Corrective Maintenance (CM): All maintenance tasks required to restore a system, subsystem, or item of equipment to operational status when the need for correction is due to an unscheduled event such as failure, accident, damage, vandalism, or severe environmental condition.

Preventative Maintenance (PM): All routine maintenance tasks performed on system, subsystems, or equipment. This activity may consist of servicing and inspection (S&I), component overhaul, or functional checks of operating systems.

Safety: Freedom from unacceptable risk of harm (EN.50126).

Risk: The probable rate of occurrence of a hazard causing harm and the degree of severity of the harm (EN.50126). The concept of risk is the combination of two elements: - the probability of occurrence of an event or combination of events leading to a hazard; - the frequency of such occurrences; - the consequence of the hazard.

Assurance: Combines safety, security, maintainability, reliability and availability.

12.4.3 Maintainability

Each system element and its constituent equipment shall be designed to permit ready access for maintenance. Maintenance personnel shall have access to perform all maintenance functions, including failure location and isolation, disassembly and reassembly, removal/replacement, and repair, as well as routine inspection/testing. Quantitative maintainability goals/requirements shall be specified for system elements where applicable. Manufacturer recommended preventive maintenance requirements shall have no detrimental effect on the operation of the Rail service.

12.4.3.1 Vehicle

The immediate operational requirement is to remove a failed vehicle from service and replace it with an operational vehicle with the minimum impact on the operation/schedule of other vehicles. The goal/requirement to remove and replace a vehicle from Rail service is 1 (one) hour. This relates solely to first line replacement, and includes logistic time to ready an alternate vehicle for service and recover the failed vehicle.
12.4.3.2 Systems
The design of all systems within the Rail operation shall allow ease of maintenance based on a modular design. Systems and equipment essential to the operational availability of the Rail system shall include redundancy.

It is assumed that there will be no repair functions performed by Metro. Economic repair of electronic / microprocessor based systems is unlikely to be achievable by an operator, therefore a policy of return to the supplier is anticipated.

An alternative policy may be suggested by the supplier however, this shall include the full implications including training of personnel, capital costs associated with a repair facility, test equipment etc.

12.4.3.3 Activities
In addition to the quantitative goals/requirements, requirements may be defined for maintainability engineering activities, such as a maintainability program plan, analyses, maintainability predictions, and demonstration tests.

Maintainability Program Plan (MPP): An MPP of the following system equipment, at a minimum, shall be established and submitted:
- Vehicles
- Fare Collection Systems
- Traffic Signal and Bus Control Systems
- Traction Power
- Communications Control Systems
- Central/Satellite Control Facilities
- Maintenance Facilities

The MPP shall include:
- Maintainability philosophy and approach
- A detailed listing and description of each maintainability task
- A schedule for each maintainability task and related milestones
- The organizational element responsible for each maintainability task
- Procedures for maintainability problem resolution.

Maintainability Analyses: Maintainability analyses shall include details such as FRACA, MTTR, and the consequences if the designer or the Contractor cannot meet the goals. The analyses shall be prepared which shall, as a minimum, include for each maintenance task:
- Frequency of task
- Time to perform
- Specified test equipment, tools, and facilities required
- Crew size and skill level
Manuels and instructions needed.

12.4.4 Reliability

12.4.4.1 Vehicle

The vehicles are the dominant factor for the rail system assurance characteristics (reliability, availability and maintainability). The vehicles will also produce the highest cost factor in terms of regular off line maintenance and overhaul. The dedicated rail track environment shall lead to measurable improvements in reliability when compared with normal street run operations. Detailed reliability goals/requirements shall be developed for the rail vehicle and support systems. The vehicle MTBF and MDBF goals/requirements shall ensure the ability of the rail system to meet the top level availability for the system. All items within the vehicle shall be developed from equipment with significant historical experience.

In addition, minimum quantitative reliability goals/requirements shall be developed for the following vehicle subsystems:

- Propulsion
- Friction or Dynamic Brakes
- Auxiliary Electrical Equipment
- Door Operation
- Vehicle Train Control and communication Equipment

There are significant differences in reliability of rail fleets from different manufacturers. Value engineering shall be completed during the selection of the vehicle supplier to determine its impact on the ability of Rail system to achieve its operational objectives.

12.4.4.2 Systems

Reliability goals/requirements shall be developed for the following systems included in fixed facilities:

- Fare Collection Systems
  - Ticket Vending Machines (expressed in terms of reliability for station platform)
  - Fare Validators
- Traffic Signal and Train Control Systems
  - Intersection crossing controls
  - Wayside signals
- Traction Power
- Communications Control Systems
  - Power (UPS)
  - Communication Links
  - Radio communication
  - Data communication
Central/Satellite Control Systems and Facilities
- Power (UPS)
- Work stations
- Control processors
- Data logging

Data Sources
Reliability quantification shall make use of the following data sources in the order of preference listed:

In service (field) performance data (for identical or similar units) or from past projects of similar nature

Reliability predictions via parts count based on MIL-HBK-217 (from component reliability database). Note: Where operating environments for components, subsystems and systems are required, the prediction shall use the average of the Ground Fixed and Ground Mobile environments. Unnecessary lengthy list of assemblies to artificially increase reliability goals/requirements is not allowed.

Supplier's assurance as to equipment performance with supporting documentation or other similar evidence.

Sub-suppliers' and component manufacturers’ data

Similar equipment from alternative suppliers or in different environments adjusted for the product maturity, quality, environment etc

Quantities of equipment based on PHA, FMEA or Fault Tree Analysis.

12.4.4.3 Activities
In addition to the quantitative goals/requirements, requirements may be defined for reliability engineering activities, such as a reliability program plan, analyses, reliability predictions, and demonstration tests.

Reliability Program Plan (RPP): An RPP of the following system equipment, at a minimum, shall be established and submitted:

Vehicles
Fare Collection Systems
Traffic Signal and Train Control Systems
Traction Power
Communications Control Systems
Central/Satellite Control Facilities
Maintenance Facilities

The RPP shall include, at a minimum:

A detailed listing and description of each reliability task
A schedule for each reliability task and related milestones
The organizational element responsible for each reliability task

Procedures for reliability problem resolution.

Consequences and steps to resolve if reliability does not meet

**Reliability Analyses:** Reliability analyses shall be prepared and submitted for acceptance which shall include, as a minimum:

- System definitions and related assumptions
- Functional flow and reliability block diagrams
- Description of any data sources and adjustment factors
- System and subsystem failure assumptions and predicted failure rates
- Comparison of reliability predictions with contractually specified values
- Impact of operation conditions or design changes on predicted values
- Definitions of all interfaces, such that every part is identified as being part of a particular subsystem
- FRACA, failure to perform, corrective actions and schedule impact
- Reliability schedule extension upon non-compliance

**Failure Trends**

New failures during Reliability analyses

**Reliability Demonstration Testing:** Reliability demonstration includes the Reliability Test Plan, detailed Test Procedures, and the final Reliability Demonstration Test Report.

The Reliability Test Plan shall include, as a minimum:

- Acceptance criteria for evaluating the equipment being tested
- Failure reporting procedures and corrective action to be used
- Mathematical verification that the test shall demonstrate the reliability levels specified

**Service Affecting:** Failures of following vehicle systems shall be considered as loss of ability to provide service.

- Traction motors - reduction in power
- Gear boxes
- Door control – loss of control, failure to open or close
- Brakes – failure of the brake system (i.e. air system)
- HVAC – loss of ability to control climate within reasonable limits

**Fixed Facility System Availability and Reliability:** System architectures shall be capable of providing the required system availability. All designs shall be expected to achieve the highest levels of system reliability and availability and shall be measured by their ability to provide passenger service levels expected of a high end mass transit system.

During final design, system designs and architectures shall be refined and contribution of failures to subsystems within the fixed facilities will be apportioned.
Fixed Facilities: Fixed facility equipment shall include self diagnostic capabilities sufficient to identify and report to central control the Line Replaceable Unit subject to fault.

Local fault indication shall provide maintenance personnel with indication of module within equipment cases subject to failure.

Self diagnostic capabilities shall include continuous monitoring and start-up checks.

Equipment shall include automated off line proof test capability, if appropriate. The proof test shall have the capability to confirm the proper operation of all functions within the equipment. The proof test may be initiated manually during routine maintenance operations (e.g. refilling ticket vending machines)

All functions essential to the successful operation of the rail system at full service capability shall where possible include redundant paths to allow normal operation following a single failure.

Fare Collection System: Failure of the fare collection system shall not prevent operation of the vehicles or overall system. Consideration shall be given to providing two ticket vending machines at each rail station

Traffic Signal and Train Control Systems: During operation it may be beneficial to obtain automated information regarding the position of vehicles, however, the presence of communication systems and fall back to manual control shall still allow operation of the rail vehicle at full capacity.

The control of crossings shall allow for local control (as per pedestrian crossings) to provide redundancy for the automated signal pre-emption systems (if procured).

Communications System: A single point failure shall not cause a failure of the Communication System.

Loss of data communications between the vehicle and Central Control shall not prevent operation of the rail system.

Details such as loss of communications, fallback process if the primary means of communications fail, backup, failures and impact of failures on operations shall be developed

Central/Satellite Control Facilities: The design of the central control facilities shall allow for graceful degradation of control functions enabling continued operation. Provisions shall be provided to continue operation of the rail system at full capacity in the event of loss of automated vehicle position information.

Maintenance Facilities: The inability to perform maintenance at the facility does not directly lead to the loss of rail service. However, the ability to perform regular maintenance on the system is essential to the success of the overall operation.

The maintenance facility shall include redundant capability to perform overnight and weekly vehicle system checks, repairs, and replenishment.

12.4.5 Availability
12.4.5.1 Scope

The Scope of availability is largely based on the types of downtimes used in the computation and on the relationship with time (i.e. the span of time to which the availability refers).

This classification is what is sometimes referred to as the availability as seen by maintenance personnel. This classification excludes preventive maintenance downtime, logistic delays, supply delays and administrative delays. Since these other causes of delay can be minimized or eliminated, an availability value that considers only the corrective downtime is the inherent or intrinsic property of the system.

12.4.5.2 Calculation

The corrective downtime reflects the efficiency and speed of the maintenance personnel, as well as their expertise and training level. It also reflects characteristics that should be of importance to the engineers who design the system, such as the complexity of necessary repairs, ergonomics factors and whether ease of repair (maintainability) was adequately considered in the design.

For a single component, the availability can be computed by:

\[ A_I = \frac{MTTF}{MTTF + MTTR} \]

MTTF = Total time / Number of Units Tested

For a system the mean time between failures (MTBF) shall be considered and compute this as follows:

\[ A_I = \frac{MTBF}{MTBF + MTTR} \]

MTBF = Uptime / Number of System Failures

MTTR = Corrective Maintenance Downtime / Number of System Failures

Note that until steady state is reached, the MTBF calculation may be a function of time (e.g. a degrading system). In such cases, before reaching steady state, the calculated MTBF changes as the system ages and more data are collected. Thus, the above formulation should be used cautiously. Furthermore, it is important to note that the MTBF
defined here is different from the MTTF (or, more precisely for a repairable system, MTTFF: mean time to first failure).

System availability can be enhanced during design by including redundancies and by the planned use of effective failure management procedure.

END OF SECTION