DOT-FTA-MA- 26-5005-00-01
DOT-VNTSC-FTA-00-01

U.S. Department
of Transportation
Federal Transit Administration

HAZARD ANALYSIS GUIDELINES FOR TRANSIT PROJECTS

U.S. Department of Transportation
Research and Special Programs Administration
John A. Volpe National Transportation Systems Center
Cambridge, MA 02142-1093

Final Report
January 2000

Federal Transit Administration

FTA OFFICE OF SAFETY AND SECURITY

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 2000	Final Report March 1998 - January 2000

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Hazard Analysis Guidelines for Transit Projects	U9170/TM899
6. AUTHOR(S) R. J. Adduci, W. T. Hathaway, L. J. Meadow	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U. S. Department of Transportation Research and Special Programs Administration Volpe National Transportation Systems Center 55 Broadway, Kendall Sq. Cambridge, MA 02142-1093	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-FTA-00-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Transportation Federal Transit Administration Office of Program Management, Office of Safety and Security Washington, DC 20590	10. SPONSORING/MONITORING AGENCY REPORT NUMBER FTA-MA-26-5005-00-01

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
A printed copy of this document is available to the public through the National Technical Information Service, Springfield, VA 22161. An electronic version of this document is also available at *http://transit-safety.volpe.dot.gov*.	

13. ABSTRACT (Maximum 200 words)

These hazard analysis guidelines discuss safety critical systems and subsystems, types of hazard analyses, when hazard analyses should be performed, and the hazard analysis philosophy. These guidelines are published by FTA to assist the transit industry as well as state and local organizations in providing the highest practical level of safety and security for the passengers and employees of the Nation's mass transportation systems. These guidelines apply to all transit projects that are directly related to the transport of passengers.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Hazard analysis, transit system safety, safety critical systems, transit, project life cycle	44
	16. PRICE CODE

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

PREFACE

These guidelines represent the cooperative efforts of many people. The authors give special thanks to Ms. Judy Z. Meade, Mr. Jerry Fisher, and Mr. Roy Field of the Federal Transit Administration's (FTA) Office of Safety and Security. They would also like to thank Korve Engineering for their overall contribution to this project. Thanks are also due to Ms. Annabelle Boyd and Mr. James Caton of Boyd/Maier, Inc., and Mr. Brian Moriarty of TRW for their support and technical review of the report. Also, thanks are also extended to Mr. James Harrison for his contribution in the overall review and preparation of this report. Their combined efforts greatly improved the content of this document.

TABLE OF CONTENTS

Section **Page**

1. INTRODUCTION 1

1.1 Purpose 1
1.2 Scope 1
1.3 Applicability 1

2. SAFETY ANALYSES 3

2.1 Safety Critical Systems 3
2.2 Hazard Identification and Resolution Process 3
2.3 Schedule for Hazard Analyses 6

3. DEFINITIONS FOR HAZARD ANALYSES 9

3.1 Safety Principles 12
3.2 Required Hazard Analyses 12
3.2.1 Overview 12

4. REFERENCES 25

APPENDIX A. EXAMPLES OF A GENERIC HAZARD CHECKLIST 27
APPENDIX B. DEFINITIONS 33
APPENDIX C. LIST OF ACRONYMS AND ABBREVIATIONS 35

LIST OF FIGURES

Figure **Page**

1. Hazard Resolution Process 4
2. Transit Project Life Cycle/Required Hazard Analysis 7

1. INTRODUCTION

1.1 PURPOSE

A primary goal of the Federal Transit Administration (FTA) is to assist the transit industry as well as state and local organizations in providing the highest practical level of safety and security for the passengers and employees of the Nation's mass transportation systems. The FTA is publishing these hazard analysis guidelines to further this goal.

In addition, the hazard analysis guidelines presented in this document are in response to the National Transportation Safety Board (NTSB) recommendation R-97-22 that requires the FTA to:

> "Revise the grant application process to require a comprehensive failure modes and effects analysis, including a human factors analysis, be provided for all federally funded projects that are directly related to the transport of passengers."

1.2 SCOPE

This document presents guidelines for the preparation of hazard analyses to assist local authorities in developing a safe and secure transit system. The guidelines discuss safety critical systems and subsystems, types of hazard analyses, when hazard analyses should be performed, and the hazard analysis philosophy.

1.3 APPLICABILITY

These guidelines apply to all transit projects that are directly related to the transport of passengers.

2. SAFETY ANALYSES

A key objective of any transit project is to provide a safe and reliable system. Transit agency personnel, consultants, and contractors are expected to implement high standards of safety and system assurance throughout the planning, design, construction, fabrication, installation, testing, pre-operational, and operational system phases of all transit projects during the life cycle of the system. The transit system's System Safety Program Plan (SSPP) is designed to eliminate and/or control identified hazards. Hazards that cannot be eliminated in the design are to be controlled by providing safety devices, warning devices, adequate training, and written instructions to transit system personnel to prevent accidents.

Safety analyses are part of a formalized process to identify, eliminate, and/or control hazards (see Figure 1). Safety analyses provide for:

- Identification of hazards
- Assessment of the severity and probability of occurrence of the hazard
- Timely awareness of hazards for those who must resolve them
- Traceability and control of hazards through all phases of a system's life cycle.

Safety analyses are essential to the preventive and proactive aspect of the system safety program. The primary purpose of safety analyses is to identify and describe hazards that might arise from flaws and fault conditions in the design and operation of a system or subsystem.

Major inputs to the hazard analyses come from the design data, drawings, operational plans and concepts, and from the experience of the analyst.

2.1 SAFETY CRITICAL SYSTEMS

Certain systems and subsystems in the design and development of transit systems are safety critical. Hazard analyses must be performed on these systems to identify potential safety problems. These systems and subsystems typically include train control, fire and emergency systems including ventilation, passenger vehicle (bus and rail), traction power, communications, and material selection.

Appendix A provides a list of generic hazards that can occur within a transit system.

2.2 HAZARD IDENTIFICATION AND RESOLUTION PROCESS

A hazard analysis should be performed on all facility modification and new construction projects. The Hazard Identification and Resolution Process is shown in Figure 1.

DEFINE THE SYSTEM

- DEFINE THE PHYSICAL AND FUNCTIONAL CHARACTERISTICS, AND UNDERSTAND AND EVALUATE THE PEOPLE, PROCEDURES, FACILITIES, EQUIPMENT, AND THE ENVIRONMENT.

▼

IDENTIFY HAZARDS

- IDENTIFY HAZARDS AND UNDESIRED EVENTS
- DETERMINE THE CAUSES OF HAZARDS

▼

ASSESS HAZARDS

- DETERMINE SEVERITY
- DETERMINE PROBABILITY
- DECIDE TO ACCEPT RISK OR ELIMINATE/CONTROL

▼

RESOLVE HAZARDS

- ASSUME RISK OR
- IMPLEMENT CORRECTIVE ACTION
  - ELIMINATE
  - CONTROL

▼

FOLLOW-UP

- MONITOR FOR EFFECTIVENESS
- MONITOR FOR UNEXPECTED HAZARDS

Figure 1. Hazard Resolution Process

System Definition

The first step in the hazard resolution process is to define the physical and functional characteristics of the system to be analyzed. These characteristics are presented in terms of the major elements, which make up the system: equipment, procedures, people and environment. A knowledge and understanding of how the individual system elements interface with each other is essential to the hazard identification effort.

Hazard Identification

The second step in the hazard resolution process involves the identification of hazards and the determination of their causes. There are five basic methods of hazard identification that may be employed to identify hazards:

- Data from previous accidents (case studies) or operating experience
- Scenario development and judgment of knowledgeable individuals
- Generic hazard checklists
- Formal hazard analysis techniques
- Design data and drawings.

When identifying the safety hazards present in a system, every effort should be made to identify and catalog the whole universe of potential hazards.

There are several hazard analysis techniques that should be considered to assist in the evaluation of potential hazards and to document their resolution including a Preliminary Hazard Analysis (PHA), Failure Modes and Effects Analysis (FMEA), and Operating Hazard Analysis (OHA). These analyses should be conducted in accordance with the latest version MIL-STD-882 (D). This standard provides uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps. The system safety program addresses hazards from many sources, including system design, hazardous materials, advancing technologies, and new techniques.

Hazard Assessment

The third step in the hazard resolution process is to assess the identified hazards in terms of the severity or consequence of the hazard and the probability of occurrence of each type of hazard. This should be accomplished in general conformity with the latest MIL-STD-882 (D).

Hazard Resolution

After the hazard assessment is completed, hazards can be resolved by deciding to either assume the risk associated with the hazard or to eliminate or control the hazard. The hazard reduction precedence is as follows:

- Design to eliminate or reduce the hazard

- Provide safety devices
- Provide warning devices
- Institute special procedures or training
- Accept the hazard
- Eliminate the use of the system/subsystem/equipment that creates an unacceptable hazard.

Various strategies or countermeasures can be employed in reducing the risk to a level acceptable to management.

Risk assessment should be used as the basis for the decision-making process to determine whether individual facility, system or subsystem hazards should be eliminated, mitigated or accepted. Hazards should be resolved through a design process that emphasizes elimination of the hazard.

Follow-up

The last step in the hazard resolution process is follow-up. It is necessary to monitor the effectiveness of recommended countermeasures and ensure that new hazards are not introduced as a result. In addition, whenever changes are made to any of the system elements (equipment, procedures, people and/or environment), a hazard analysis should be conducted to identify and resolve any new hazards.

2.3 Schedule for Hazard Analyses

Hazard analyses are performed in various stages of the transit project life cycle, as shown in Figure 2. They become part of the safety certification process for the system. Safety certification is necessary prior to opening of new facilities and systems, in addition to modifications of existing systems. The objective of the Safety Certification program is to produce a formal document that ensures at the time of operation and through its life cycle, a particular system is safe for passengers, employees, emergency responders, and the general public. ***(Safety certification is the process of verifying that certifiable elements comply with a formal list of safety requirements. The requirements are defined by design criteria, contract specifications, applicable codes, and industry standards)***

- The *concept-planning phase* begins with the decision to build and ends at the onset of preliminary design. A Preliminary Hazard Analysis (PHA) is performed during this stage.

Hazard Analysis	Transit Project Life Cycle				Operations/ Integration/ Test/Check-Out/Safety Certification
	Concept Planning	Preliminary Design	Final Design	Construction/ Procurement/ Installation	
Preliminary Hazard Analysis (PHA)					
Failure Modes and Effects Analysis (FMEA)					
Fault Tree Safety Hazard Analysis					
Operating Hazard Analysis (OHA)					
Software Safety Analysis (SSA)					

Figure 2. Transit Project Life Cycle/Required Hazard Analysis

- The *design phase* consists of two stages. It begins at the onset of preliminary design and ends when the design is finalized and ready to go into production. The Failure Modes and Effect Analysis (FMEA) is performed during preliminary design so that any changes identified can be incorporated into the final design. The Fault Tree Analysis (FTA) is performed during the beginning of final design. The Operating Hazard Analysis (OHA) is prepared during the latter portion of the final design.

- The *construction/procurement/installation phase* begins when the fabrication or construction of equipment and facilities starts, and ends with the installation, final inspection, and local testing of individual equipment units. The FMEA may need to be updated if additional hazards are identified during this phase.

- The *integration/test/checkout phase* begins when the equipment is installed and locally tested, extends throughout the period of integrated system test and checkout, and ends when the system begins revenue operation. The OHA may need to be updated if additional hazards are identified during this phase. This process provides necessary documentation required to safety certify the system.

The major output of hazard analyses is the identification and evaluation of hazards and critical failure modes. A uniform interpretation of the severity and probability of hazards is used.

3. DEFINITIONS FOR HAZARD ANALYSES

The following definitions are used to develop hazard analyses for rail systems.

Hazard Severity **-** Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure, or malfunction, as follows:

- Category I: Catastrophic: Death, system loss or severe environmental damage.
- Category II: Critical: Severe injury, severe occupational illness, major system, or environmental damage.
- Category III: Marginal: Minor injury, minor occupational illness, minor system, or environmental damage.
- Category IV: Negligible: Less than minor injury, occupational illness, or less than system or environmental damage.

The assessment of the hazard should also include a probability of occurrence. Assigning a quantitative probability to a hazard is generally not possible early in the design or planning process. A qualitative hazard probability can be derived from research, analysis, and evaluation of historical safety data from similar systems.

Risk Assessment

Hazard analyses establish hazard severity category (I through IV) and hazard probability ranking (A through E) which are combined into a Hazard Risk Index, reflecting the combined severity and probability ranking for each identified hazard. Risk assessment criteria shall be applied to the identified hazards based on their severity and probability of occurrence, to determine acceptance of the risk or the need for corrective action to further reduce the risk.

Frequency of Occurrence	**I**	**II**	**III**	**IV**
	Catastrophic	Critical	Marginal	Negligible
(A) Frequent	IA	IIA	IIIA	IVA
(B) Probable	IB	IIB	IIIB	IVB
(C) Occasional	IC	IIC	IIIC	IVC
(D) Remote	ID	IID	IIID	IVD
(E) Improbable	IE	IIE	IIIE	IVE

Legend	Hazard Risk Index	Acceptance Criteria
	IA, IB, IC, IIA, IIB, IIIA	Unacceptable
	ID, IIC, IID, IIIB, IIIC	Undesirable (decision required)
	IE, IIE, IIID, IIIE, IVA, IVB	Acceptable with review
	IVC, IVD, IVE	Acceptable without review

Descriptive Word	Level	Within Specific Individual Items	Within a Fleet or Inventory
Frequent	A	Likely to occur frequently. MTBE* is less than 1000 operating hours	Continuously experienced.
Probable	B	Will occur several times in life of an item. MTBE is equal to or greater than 1000 operating hours and less than 100,000 operating hours	Will occur frequently.
Occasional	C	Likely to occur sometime in life of an item. MTBE is equal to or greater than 100,000 operating hours and less than 1,000,000 operating hours	Will occur several Times
Remote	D	Unlikely but possible to occur in life of item. MTBE is greater than 1,000,000 operating hours and less than 100,000,000 operating hours	Unlikely but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced. MTBE is greater than 100,000,000 hours	Unlikely to occur, but possible.

*MTBE = Mean time between events

Hazard Analysis and Corrective Action

A. The system safety analyses establish hazard severity category (I through IV) and hazard probability ranking (A through E), which are combined into a Hazard Risk Index, reflecting the combined severity and probability ranking for each identified hazard, before implementation of any corrective action.

B. Risk assessment criteria will be applied to the identified hazards based on their severity and probability of occurrence, to determine acceptance of the risk or the need for corrective action to further reduce the risk.

C. Corrective action for the elimination or control of unacceptable and undesirable hazards will include the following order of precedence:

1. *Design for Minimum Risk.* Design, redesign or retrofit to eliminate (i.e., design out) the hazards through design selection. If an identified hazard cannot be eliminated, reduce the severity and/or probability of occurrence to an acceptable level. This may be accomplished, for example, through the use of fail-safe devices and principles in design, the incorporation of high-reliability systems and components and use of redundancy in hardware and software design.

2. *Safety Device*. Hazards that cannot be eliminated or controlled through design selection will be controlled to an acceptable level through the use of fixed, automatic or other protective safety design features or devices. Examples of safety devices include interlock switches, protective enclosures and safety pins. Care must be taken to ascertain that the operation of the safety device reduces the loss or risk and does not introduce an additional hazard. Safety devices will also permit the system to continue to operate in a limited manner. Provisions will be made for periodic functional checks of safety devices.

3. *Warning Devices*. When neither design nor safety devices can effectively eliminate or control an identified hazard, devices will be used to detect the condition and to generate an adequate warning signal to correct the hazard or provide for personnel remedial action. Warning signals and their application will be designed to minimize the probability of incorrect personnel reaction to the signals and will be standardized within like types of systems.

4. *Procedures and Training*. Where it is not possible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, procedures and training will be used to control the hazard. Special equipment operating procedures can be implemented to reduce the probability of a hazardous event and a training program can be conducted. The level of training, required will be based on the complexity of the task and minimum trainee qualifications contained in training requirements specified for the subject system element and element subsystem. Procedures may include the use of personal protective equipment. Precautionary notations in manuals will be standardized. Safety critical tasks, duties and activities related to the system element/subsystem will require certification of personnel proficiency. However, without specific written approval, no warning, caution or other form of written advisory will be used as the only risk reduction method for Category I and II hazards.

D. Hazards identified as having an unacceptable and undesirable risk will be analyzed using logic network analyses (such as fault tree) to determine effectiveness of corrective action. Unacceptable and undesirable risk will be reduced to an acceptable level before design acceptance, or a decision must be made to dispose of the system.

E. Hazards identified as “acceptable with review” may be accepted in an “as-is” condition with no further corrective action. Alternatively, operating and maintenance procedures must be developed for periodic tests and inspections of the subject item to ensure an acceptable level of safety is maintained throughout the life of the system.

F. Hazards with combination of severity and probability IVC, IVD, and IVE are acceptable.

G. Appropriate support documentation used in the development of the analysis must be identified or referenced in detail as part of each analysis, including but not limited to the following:

- Schematics, drawings, block diagrams
- System description including modes of operation and tasks
- Lists of Line Replaceable Units (LRUs), assemblies, parts and components addressed within each subsystem and system
- Documented reliability, maintainability, and safety data including failure rate data obtained from service use in identical or manifestly similar equipment in similar environment
- Documented reliability, maintainability, and safety data obtained from formal test results, conducted in similar applications.

- Documented reliability, maintainability, and safety data obtained from formal analyses, conducted for equipment in similar applications.

3.1 Safety Principles

The following safety principles shall be followed in the design and operations of the rail transit system:

A. When the system is operating normally there shall be no unacceptable or undesirable hazard conditions.

B. The system design shall require positive actions to be taken in a prescribed manner to either begin or continue system operation.

C. The safety of the system in the normal automatic operating mode shall not depend on the correctness of actions or procedures used by operating personnel.

D. There shall be no single-point failures in the system that can result in an unacceptable or undesirable hazard condition.

E. If one failure combined with a second failure can cause an unacceptable or undesirable hazard condition, the first failure shall be detected and the system shall achieve a known safe state before the second failure can occur.

F. Software faults shall not cause an unacceptable or undesirable hazard condition.

G. Unacceptable hazards shall be eliminated by design.

H. Maintenance activities required to preserve or achieve risk levels shall be performed. Personnel qualifications required to adequately implement these activities shall also be identified.

3.2 Required Hazard Analyses

Hazard analyses shall be employed to assist in the evaluation of potential hazards and to document their resolution. (See section 2.3 “Schedule for Hazard Analyses)

3.2.1 <u>Overview</u>

At a minimum, the following hazard analyses shall be conducted for a transit project:

1) A Preliminary Hazard Analysis (PHA) provides an early assessment of the hazards associated with a design or concept. The PHA identifies critical areas, hazards and criteria being used, and considers hazardous components, interfaces,

environmental constraints, as well as operating, maintenance, and emergency procedures.

2) A Failure Modes and Effects Analysis (FMEA) supports ongoing hazard analysis during preliminary and final design by identifying and analyzing possible failures so that appropriate actions are taken to eliminate, minimize, or control hazards. The FMEA will provide information to evaluate identified hazards, identify safety critical areas, and provide inputs to safety design criteria and procedures with provisions and alternatives to eliminate or control all unacceptable and undesirable hazards, based on their combination of severity and probability of occurrence and to identify critical items.

3) The Operating Hazard Analysis (OHA) identifies and analyzes hazards associated with personnel and procedures during production, installation, testing, training, operations, maintenance, and emergencies. The OHA shall be conducted on all tasks and human actions, including acts of omission and commission, by persons interacting with the system, subsystems, and assemblies, at any level.

For certain safety-critical subsystems such as train control, it may be necessary to also perform a Fault Tree Analysis (FTA). The FTA is a graphical representation of the relationship between specific events and an ultimate undesired event. The undesired event is selected. Interactions and causes of this undesired event are examined and broken down into secondary undesired events and causes.

3.2.2 Hazard Analysis Processes

This section contains instructions and formats for three hazard analyses: the Preliminary Hazard Analysis, the Failure Modes and Effects Analysis, and the Operating Hazard Analysis.

Required Hazard Analyses

A Preliminary Hazard Analysis (PHA), a Failure Modes and Effects Analysis (FMEA), and Operating Hazard Analysis (OHA) shall be performed.

1. PRELIMINARY HAZARD ANALYSIS (PHA)

Purpose: The purpose of the PHA is to provide an early assessment of the hazards associated with a design or concept.

Procedure: The PHA identifies critical areas, hazards, and criteria being used and considers: hazardous components, interfaces, environmental constraints, as well as operating, maintenance, and emergency procedures.

Results: The PHA will provide for verification that corrective or preventive measures or procedures are taken in safety reviews, modification of

specifications, and generation of methods and procedures to eliminate, minimize, or control hazards, and provide inputs to the Failure Modes and Effects Analysis and Operating Hazard Analysis.

Utilize this PHA Form as Follows:

In NO., assign a unique number that identifies each hazard.

In HAZARD DESCRIPTION, describe an immediate condition that could lead to an accident involving potential injury, death, or equipment damage.

In FAILURE RATE, enter a quantitative assessment of the frequency of occurrence of the hazardous event, measured in events per million hours of operation.

In POTENTIAL CAUSE, enter the most likely primary and secondary causes that can potentially contribute to the presence of the hazard.

In EFFECT ON SUBSYSTEM/SYSTEM, describe the effect that the hazardous condition may have on the system element or its element subsystem in terms of safety (e.g. delay, inconvenience, injury, damage, fatality, etc.)

In HAZARD RISK INDEX, enter a combination of the qualitative measures of the worst potential consequence resulting from the hazard, and its probability of occurrence (e.g., IA, IIB, etc.).

In POSSIBLE CONTROLLING MEASURES AND REMARKS, describe actions that can be taken or procedural changes that can be made to prevent the anticipated hazardous event from occurring. Enter name(s) of related analysis and reference number(s), and which approach is being proposed: Design Change, Procedures, Special Training, etc.

In RESOLUTION, describe changes made or steps taken relative to design and/or procedures, training, etc., to eliminate or control the hazard.

Preliminary Hazard Analysis (PHA) Form

System: Subsystem: Drawing No: OHA No.: Rev. No.			PRELIMINARY HAZARD ANALYSIS (PHA) Rev. No:			Sheet Of Prepared by: Date: Reviewed by: Date: Approved by: Date:	
General Description			Hazard Cause/Effect		Hazard Risk Index	Corrective Action	
No.	Hazard Description	Failure Rate	Potential Cause	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution

Sample Preliminary Hazard Analysis (PHA) Form

System: Pumping System Subsystem: Pump Drawing No: 13-R1 PHA No.: 1 Rev. No. 1			PRELIMINARY HAZARD ANALYSIS (PHA) Rev. No: 1			Sheet One Of One Prepared by: Joe Safety Date: 12/8/99 Reviewed by: Supervisor Safety Date: 12/8/99 Approved by: Director Safety Date: 12/8/99	
General Description			Hazard Cause/Effect		Hazard Risk Index	Corrective Action	
No.	Hazard Description	Failure Rate	Potential Cause	Effect on Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
1	Pump, which removes water from tunnel, fails – causing a loss of water removal capability	1×10^{-6}	Mechanical Failure; Maintenance Failure	Water Floods Tunnel	1C	Design Change: Add back-up pump Procedure Change: Provide scheduled maintenance check and testing	1D – Back-up pump added; maintenance and testing procedures developed and implemented, 12/9/99

2. FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

Purpose: The purpose of the FMEA is to determine the results or effects of sub-element failures on a system operation and to classify each potential failure according to its severity. The FMEA will be used to identify and analyze possible failures early in the design phase so that appropriate actions are taken to eliminate, minimize, or control safety.

Procedure: The FMEA will examine the system element by element, using deductive logic to evaluate a system or process for safety hazards and ultimately to assess risk. The FMEA should be conducted on all Line Replacement Units (LRUs) of each system and subsystem and will encompass all identified failure modes and fault conditions. When the FMEA indicates a potential problem, it will be made known to the responsible engineer, in order to initiate proper action. The FMEA will be reviewed on a continuous basis to verify that design modifications do not add hazards to the system.

To perform a FMEA, the following process should be implemented:

- Identify all major system components, functions, and processes
- Determine consequences of interest
- Determine the potential failure modes of interest
- Specify effects of failures of system
- Identify safety provisions to control hazards and failures
- Identify detection methods for failures
- Establish overall significance of each failure

Results: The FMEA will provide information to evaluate identified hazards, identify safety critical areas, and provide inputs to safety design criteria and procedures with provisions and alternatives to eliminate or control all unacceptable and undesirable hazards, based on their combination of severity and probability of occurrence, and to identify critical items.

<u>The FMEA Form is used as Follows:</u>

In LRU NO. & DESCRIPTION, assign a number to each LRU and briefly describe the characteristics of the LRU.

In FAILURE MODE, describe an immediate failure mode or fault condition, which could lead to an accident involving potential injury, death, or equipment damage.

In CAUSE OF FAILURE, enter the most likely primary and secondary causes that can potentially contribute to the presence of the hazard.

In EFFECT OF FAILURE ON SUBSYSTEM/SYSTEM, describe the effect that the failure mode of fault condition may have on the item and the next higher level,

i.e., subsystem or system element in terms of inputs and outputs, and in terms of system safety and operational impact (e.g., delay, inconvenience, injury, damage, fatality, etc.)

In PROBABILITY OF OCCURRENCE, enter the probability of occurrence of the failure mode or fault condition, measured in events per million hours of operation. Give data source, such as experience in similar applications.

In SEVERITY OF OCCURRENCE, enter the potential impact of fault condition or failure mode on system operation (catastrophic, critical to insignificant).

In POSSIBLE CONTROLLING MEASURES AND REMARKS, describe actions that can be taken or procedural changes that can be made to prevent the anticipated hazardous event from occurring. Enter name(s) of related analysis and reference number(s) and which approach is being proposed: Design Change, Procedures, Special Training, etc.

In RESOLUTION, describe changes made or steps taken relative to design and/or procedures, training, etc., to eliminate or control the hazard.

Failure Modes and Effect Analysis (FMEA) Form

System: Subsystem: Drawing No: FMEA No.: Rev. No:			FAILURE MODES AND EFFECT ANALYSIS (FMEA)			Sheet Of Prepared by: Date: Reviewed by: Date: Approved by: Date:	
General Description			Hazard Cause/Effect			Corrective Action	
LRU No. & Description	Failure Mode	Cause of Failure	Effect of Failure on Subsystem/ System	Probability of Occurrence	Severity of Occurrence	Possible Controlling Measures and Remarks	Resolution

Sample Failure Modes and Effect Analysis (FMEA) Form

System: Pumping System Subsystem: Pump Controller, Power Drawing No: 1 FMEA No.: 1 Rev. No: 1			FAILURE MODES AND EFFECT ANALYSIS (FMEA)			Sheet : One Of: One Prepared by: Joe Engineer Date: 12/9/99 Reviewed by: Safety Supervisor Date: 12/9/99 Approved by: Safety Director Date: 12/9/99	
General Description			Hazard Cause/Effect			Corrective Action	
LRU No. & Description	Failure Mode	Cause of Failure	Effect of Failure on Subsystem/ System	Probability of Occurrence	Severity of Occurrence	Possible Controlling Measures and Remarks	Resolution
1 – Pump controller	Shut-off indication not recognized	Electrical malfunction	Pump remains on continuously, burns out and water floods the tunnel	1×10^{-6}	Critical	Provide low water cut-off for pump Provide alarm to trigger when pump is on for more than “X” minutes	Low water cut-off on pump and alarm for “pump on” time in design – 12/7/99

3. OPERATING HAZARD ANALYSIS (OHA)

Purpose: The purpose of the OHA is to identify and analyze hazards associated with personnel and procedures during production, installation, testing, training, operations, maintenance, and emergencies.

Procedure: The OHA will be conducted on all tasks and human actions, including acts of omission and commission, by persons interacting with the system, subsystems and assemblies, at any level. When the OHA indicates a potential safety hazard, it will be made known to the responsible engineer to initiate a design review or a system safety working group action item. The OHA will be reviewed on a continuous basis to provide for design modifications, procedures, testing, etc., that do not create hazardous conditions.

Results: The OHA will provide for corrective or preventive measures to be taken to minimize the possibility that any human error or procedure will result in injury or system damage. The OHA will provide inputs for recommendations for changes or improvements in design or procedures to improve efficiency and safety, development of warning and caution notes to be included in manuals and procedures, and the requirement of special training of personnel who will carry out the operation and maintenance of the system.

Utilize the OHA Form as Follows:

In TASK DESCRIPTION, describe the task being performed.

In HAZARD DESCRIPTION, describe a human act of commission or omission, error, or fault condition that could lead to an accident involving potential injury, death or equipment damage.

In PROBABILITY OF OCCURRENCE, enter the probability of occurrence of the error or fault condition, measured in events per million hours of operations. Give data source, such as experience and statistics in similar applications, human factor studies, etc.

In POTENTIAL CAUSE, enter the most likely primary and secondary causes, including those induced by hardware, software, procedures and the environment, that can potentially contribute to the presence of the hazard.

In EFFECT ON PERSONNEL/SUBSYSTEM/SYSTEM, describe the effect that the human error or fault condition may have on personnel, patrons, the general public, public, equipment, facilities and the entire system, in terms of system safety and operational impact (e.g., delay, inconvenience, injury, damage, fatality, etc.)

In HAZARD RISK INDEX, enter a combination of the qualitative measures of the worst potential consequence resulting from the hazard, and its probability of occurrence (e.g., IA, IIB, etc.).

In POSSIBLE CONTROLLING MEASURES AND REMARKS, describe actions that can be taken or procedural changes that can be made to prevent the anticipated hazardous event from occurring. Enter name(s) of related analysis and reference number(s) and which approach is being proposed: Design Change, Procedures, Special Training, etc.

In RESOLUTION, describe changes made or steps taken relative to design and/or procedures, training, etc., to eliminate or control the hazard.

Operating Hazard Analysis (OHA) Form

System: Subsystem: Drawing No: OHA No.: Rev. No:			OPERATING HAZARD ANALYSIS (OHA)			Sheet Of Prepared by: Date: Reviewed by: Date: Approved by: Date:	
General Description			Hazard Cause/Effect		Hazard Risk Index	Corrective Action	
Task Descri ption	Hazard Description	Probability of Occurrence	Potential Cause	Effect on Personnel/ Subsystem/ System		Possible Controlling Measures and Remarks	Resolution

Sample Operating Hazard Analysis (OHA) Form

System: Preventive Maintenance Procedure Subsystem: Pump Drawing No: 1 OHA No.: 1 Rev. No: 1			OPERATING HAZARD ANALYSIS (OHA)			Sheet: One Of: One Prepared by Joe Maintenance: Date: 12/8/99 Reviewed by: Supervisor Maintenance Date: 12/8/99 Approved by: Director Safety Date: 12/8/99	
General Description			Hazard Cause/Effect		Hazard Risk Index	Corrective Action	
Task Description	Hazard Description	Probability of Occurrence	Potential Cause	Effect on Personnel/ Subsystem/ System		Possible Controlling Measures and Remarks	Resolution
Preventive maintenance on pumping system	Failure to perform power plug reversal; failure to test pump after reversal	1×10^{-6}	Human error	Pump fails; tunnel floods with water	1C	<u>Design Change</u>: Install automatic transfer switch to switch transformer monthly or after specified number of hours <u>Procedure</u>: Add necessary steps to procedures to test pump after plugs have been reversed	1D – Transfer switch added (10/15/99) New maintenance testing procedures approved, added, and training implemented (10/15/99)

4. REFERENCES

The following documents were used as references for these guidelines.

1. Los Angeles County Rail Construction Corporation Guidelines for the Preparation of Safety & Systems Assurance Analyses, RCC 5-001A, May 1992
   One Gateway Plaza, Los Angeles, CA 90017

2. Military Standard 882D, *System Safety Program Requirements*
   Department of Defense, Washington, DC January 19, 1993
   (http://www.afmc.wpafb.af.mil/organizations/HQ-AFMC/SE/ssd.htm)

3. NASA (National Aeronautics and Space Administration)
   System Safety Guidelines for Hazard Identification and Control
   NASA, 300 E. Street, Washington, DC 20456-0001

4. *Automated People Mover Standards – Part I*
   American Society of Civil Engineers
   1801 Alexander Bell Drive
   Reston, VA 20191-4400
   www.pubs.asce.org/pubshom1.html
   Library of Congress Catalog Card: 96-49993
   ISBN 0-78444-016-934

5. Hammer, W. Product Safety Management and Engineering.
   Englewood Cliffs, NJ 07632: Prentice-Hall, Inc., 1980
   www.prenhall.com

APPENDIX A. EXAMPLES OF A GENERIC HAZARD CHECKLIST*

1. BASIC DESIGN DEFICIENCIES

   a. Examples:

      (1) Sharp corners
      (2) Instability
      (3) Excessive weight
      (4) Inadequate clearance
      (5) Lack of accessibility

   b. Causes: Improper or poor design

   c. Control Methods: Improve or change design

2. INHERENT HAZARDS

   a. Examples:

      (1) Mechanical (i.e., rotating equipment, vibration)
      (2) Electrical
      (3) Explosives
      (4) Flammable gases or liquids
      (5) Toxic substances
      (6) Acceleration (flying objects)
      (7) Deceleration (falling objects)
      (8) Temperature

   b. Cause: Integral characteristic which cannot be designed out

   c. Control Methods:

      (1) Safety Devices

         (a) Isolation (separation)
         (b) Barriers (guards)
         (c) Interlocks (deactivation)
         (d) Pressure release
         (e) Temperature sensor (fuse)

* This checklist was developed by Volpe National Transportation Systems Center using material adapted from *Product Safety Management and Engineering* by Willie Hammer, 1980.

(2) Warning Devices (Five Senses)

(a) Visual (eye) – color, shape, signs, light
(b) Auditory (hear) – bell
(c) Tactile (touch) – shape, texture
(d) Olfactory (smell)
(e) Gustatory (taste)

(3) Procedures and Training

(a) Use of safe procedures
(b) Training
(c) Backout/recovery procedures
(d) Protective equipment
(e) Emergency procedures

3. MALFUNCTIONS

a. Examples:

(1) Structural failures
(2) Mechanical malfunctions
(3) Power failures
(4) Electrical malfunctions

b. Causes:

(1) Faulty design
(2) Manufacturing defects
(3) Improper or lack of maintenance
(4) Exceeding specified limits
(5) Environmental effects

c. Control Methods: Design

(1) Fail safe design
(2) Higher safety margins (i.e., reduce stress, increase load strength, etc.)
(3) Redundant circuitry or equipment
(4) Timed replacement

d. Other Control Methods: Safety devices, Warning Devices, Procedures and Training (See Point 2.c 1-3)

4. MAINTENANCE HAZARDS

a. Examples:

(1) Improper connections
(2) Component failures
(3) Equipment damage
(4) Operational delay

b. Causes:

(1) Lack of Maintenance
(2) Improper maintenance
(3) Hazardous maintenance conditions

c. Control Methods:

(1) Design

(a) Simplified design
(b) Fail-safe design
(c) Easy access to equipment
(d) Elimination of need for special tools or equipment

(2) Safety devices

(a) Guards for moving parts
(b) Interlocks

(3) Warning devices

(a) Labels/Signs
(b) Bells
(c) Chimes
(d) Lights

(4) Procedures or Training

(a) Documentation of proper procedures
(b) Improved training courses
(c) Housekeeping

5. ENVIRONMENTAL HAZARDS

a. Examples

(1) Heat
(2) Cold
(3) Dryness
(4) Wetness
(5) Low friction (slipperiness)
(6) Glare
(7) Darkness
(8) Earthquake
(9) Gas or other toxic fumes

b. Causes

(1) Inherent
(2) Foreseen or unforeseen natural phenomena/conditions, which do or could, occur.

c. Control Methods (see also 4.c)

(1) Design

(a) Increased resistance to temperature changes
(b) Increased resistance to dryness or wetness
(c) Fail-safe design

(2) Safety Devices

(a) Sufficient heating or cooling capability
(b) Adequate insulation
(c) Restricted access
(d) Temperature sensor

(3) Warning devices

(a) Visual
(b) Auditory
(c) Smell

(4) Procedures and Training

(a) Use of safe procedures
(b) Protective equipment
(c) Training

6. HUMAN FACTORS

a. Examples: (also see all other items)

(1) Stress (sensory, mental, motor)
(2) Physical surroundings (environment)

(a) Noise
(b) Illumination
(c) Temperature
(d) Energy sources
(e) Air and humidity
(f) Vibration

(3) Errors

(a) Omission
(b) Commission

(4) Non-recognition of hazards
(5) Incorrect decisions
(6) Tasks done at wrong time
(7) Tasks not performed or incorrectly performed

b. Causes:

(1) Inadequate attention to human design criteria
(2) Poor location, layout of controls
(3) Equipment complexity
(4) Inherent hazards
(5) Incorrect installation
(6) Failure of warning devices
(7) Inadequacy of procedure safeguards

(a) Failure to follow instructions
(b) Lack of knowledge of procedures

(8) Inadequate training
(9) Lack of improper maintenance

c. Control Methods:

(1) Design (to address items (1) – (6)
(2) Safety Devices (Redundancy)

(a) Isolation (separation)
(b) Barriers (guards)
(c) Interlocks (deactivation)

(d) Temperature sensor (fuse)

(3) Warning Devices (Five Senses) (Redundancy)

(a) Visual (eye) – color, share, signs, light
(b) Auditory (hear) – bell
(c) Tactile (touch) – shape, texture
(d) Olfactory (smell)
(e) Gustatory (taste)

(4) Procedures and Training

(a) Clear warning labels (nature of hazard, action to avoid injury, consequences)
(b) Use of complete, proper, safe procedures
(c) Adequate training (also refresher training)
(d) Backout/recovery procedures
(e) Protective equipment
(f) Emergency procedures
(g) Proper maintenance procedures

APPENDIX B. DEFINITIONS

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

Hazard Analysis: Any analysis performed to identify hazardous conditions for the purpose of their elimination or control.

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

Life cycle: All phases of the system's life including research, development, test and evaluation, production, development (inventory), operations and support, and disposal.

Occupational illness: Any abnormal condition or disorder, other than one resulting from an occupational injury, caused by exposure to environmental factors associated with employment. It includes acute and chronic illnesses or diseases, which may be caused by inhalation, absorption, ingestion, or direct contact. Examples:

- Occupational skin diseases or disorders
- Dust diseases of the lungs (silicosis, asbestosis, etc.)
- Respiratory conditions due to toxic agents
- Poisoning (systematic effects of toxic materials)
- Disorders due to physical agents (other than toxic materials) heat stroke, sunstroke, etc. Disorders associated with repeated trauma.

Risk: An expression of possible loss over a specific period of time or number of operational cycles. It may be expressed as the product of hazard severity and probability.

System: A composite of personnel, procedures, materials, tools, equipment, facilities, and software, at any level of complexity. The elements of this entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

Subsystem: An element of a system that in itself may constitute a system. Depending on the nature and scope of the contract or subcontract, the connotation of system and subsystem may differ. The system could be the entire rail transit system and the subsystems could be transit system elements such as the passenger vehicle, traction power, train control, and communications, for example. Or for a rail vehicle analysis, the system could be the passenger vehicle and examples of subsystems could be the vehicle propulsion subsystem and friction brake subsystem.

System Safety Program Plan: A description of the planned tasks and activities to be used to implement the required system safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems. (A document adopted by transit agencies detailing its safety policies, objectives, responsibilities, and procedures).

System Safety Concept: The application of special technical and managerial skills to the systematic, forward-looking identification, and control of hazards throughout the life cycle of a project, program, or activity.

Safety Certification Program/Process: A program whose objective is to produce a formal document that ensures at the time of operation, a particular system and all its components is safe for passengers, employees, emergency responders, and the general public. Safety Certification is the process of verifying that certifiable elements comply with a formal list of safety requirements. The requirements are defined by design criteria, contract specifications, applicable codes, and industry safety standards.

APPENDIX C. LIST OF ACRONYMS AND ABBREVIATIONS

FMEA	Failure Modes and Effect Analysis
FTA	Federal Transit Administration
LRU	Line Replaceable Units
MIL-STD	Military Standard
NTSB	National Transportation Safety Board
OHA	Operating Hazard Analysis
PHA	Preliminary Hazard Analysis
SHA	System Hazard Analysis
SSA	Software Safety Analysis
SSPP	System Safety Program Plan