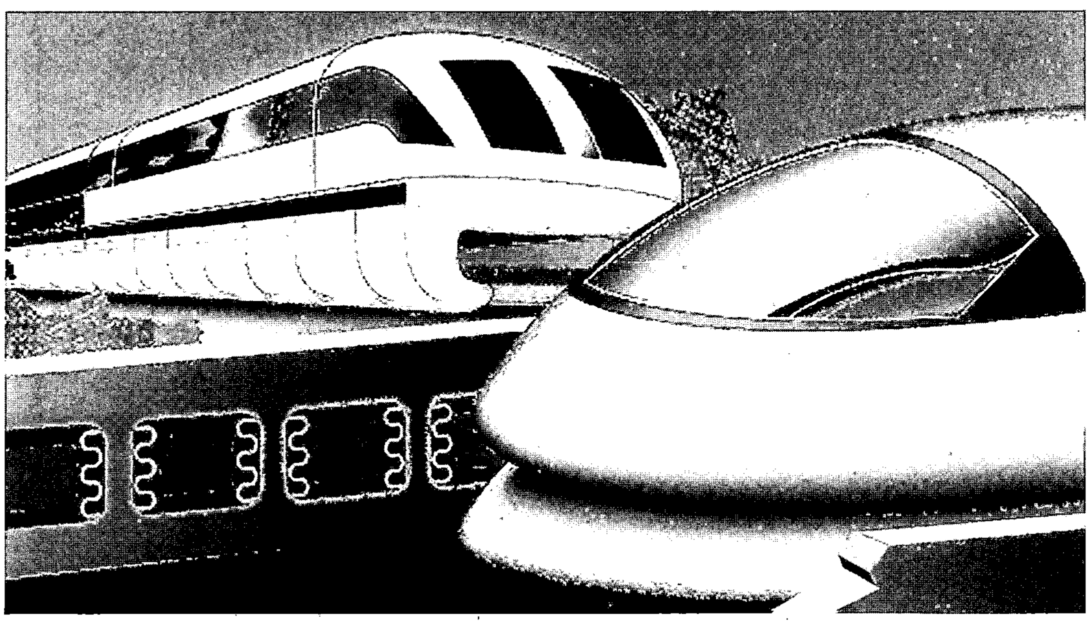
U. S. Department
of Transportation
Federal Railroad Administration

Safety of High Speed Magnetic Levitation Transportation Systems

Office of Research
and Development
Washington, D.C. 20590

U.S. Maglev System Concept Definitions (SCDs) - System Safety Review



DOT/FRA/ORD-93/22
DOT-VNTSC-FRA-93-11

1 - Advanced Systems

Final Report
September 1993

NOTICE

In numerous places, this report discusses whether various aspects of the technologies that are the subject of this report comply with Federal safety laws and regulations. Those discussions, which reflect the seasoned judgment of commentators qualified in their fields, do not constitute rulings by the Federal Railroad Administration's Office of Safety or its Office of Chief Counsel concerning compliance with the law.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1993	Final Report October 1992 - August 1993

4. TITLE AND SUBTITLE Safety of High Speed Magnetic Levitation Transportation Systems: U.S. Maglev System Concept Definitions (SCDs) - System Safety Review

5. FUNDING NUMBERS
R3018/RR393
DTRS-57-89
RA 2068

6. AUTHOR(S) B•A: David L. Gilles, Wayne L. Gilles, Thomas C. Griego, John M. Simon
CIGGT: William F. Hayes

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Booz•Allen & Hamilton, Inc.
523 W. Sixth Street, Suite 650
Los Angeles, CA 90014

The Canadian Institute of Guided Ground Transport, Queen's University
Kingston, Ontario, K7L3N6 Canada

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-FRA-93-11

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Railroad Administration
Office of Research and Development
Washington, D.C. 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT/FRA/ORD-93/22

11. SUPPLEMENTARY NOTES
Under contract to:
U.S. Department of Transportation
Research and Special Programs Administration
John A. Volpe National Transportation Systems Center
Kendall Square, Cambridge, MA 02142

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for U. S. Government use only. Exempted from public availability to protect intellectual property rights of designers. Transmittal of this document outside the U.S. Government must have prior approval of the Deputy Associate Administrator for Technology Development, FRA.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Magnetic levitation (maglev) technology has the potential to provide very high speed travel with the capacity and convenient access of conventional passenger railways, while relieving U.S. highway and airport congestion.

A need exists for the assessment of the safety implications of this new form of guided ground transportation. This is the responsibility of the Federal Railroad Administration (FRA), which is charged with ensuring the safety of maglev systems in the United States under the provisions of the Rail Safety Improvement Act of 1988.

As a part of the National Maglev Initiative (NMI), Magneplane, Foster-Miller, Grumman, and Bechtel prepared detailed system concept definition (SCD) final reports which conceptually define the technical feasibility, performance, and cost of constructing and operating their respective designs in the United States.

The respective SCD contractors were required to meet minimum safety requirements and perform a system hazard analysis to address safety considerations associated with their respective system characteristics.

This report presents the results of the systematic review of the four SCD maglev technologies in terms of major system elements, as documented in each SCD final report. The system safety review was performed in terms of the safety requirements contained in the original SCD statement of work (SOW), as supplemented by additional issues identified by the SCDs, by the FRA/Volpe Center, or by Booz•Allen.

The report is intended to assist the FRA in ensuring that potential safety-critical hazards and unsafe conditions associated with the SCDs and other proposed maglev system designs are identified and resolved early in the life-cycle of U.S. maglev system development.

14. SUBJECT TERMS National Maglev Initiative, NMI, magnetic levitation, maglev, transportation, high speed ground transportation, Federal Railroad Administration, passenger trains, maglev safety, system safety.

15. NUMBER OF PAGES 378

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	Unclassified

SYSTÈME INTERNATIONAL (SI) UNIT DEFINITIONS AND CONVERSIONS USED IN THIS REPORT

DISTANCE (ENGLISH-TO-SI CONVERSION):

1 inch (in)	= 2.54 centimeters (cm)	= 0.025 meters (m)
1 foot (ft)	= 30.5 centimeters (cm)	= 0.305 meters (m)
1 yard (yd)	= 91.4 centimeters (cm)	= 0.914 meters (m)
1 mile (mi)	= 1.61 kilometers (km)	= 1,610 meters (m)

ELECTRICAL QUANTITIES:

Electric Fields

1 volt/meter (V/m)	= 0.01 volts/centimeter (V/cm)
1 kilovolt/meter (kV/m)	= 1000 volts/meter (V/m)
1 kilovolt/meter (kV/m)	= 10 volts/centimeter (V/cm)

Magnetic Flux Densities (English-to-SI Conversion)

10,000 gauss (G)	= 1 tesla (T)
10 milligauss (mG)	= 1 microtesla (μT)
1 milligauss (mG)	= .1 microtesla (μT)
0.01 milligauss (mG)	= 1 nanotesla (nT)

Electromagnetic Frequency Bands

1 cycle per second	= 1 hertz (Hz)
1,000 cycles per second	= 1 kilohertz (kHz)

Ultra Low Frequency (ULF) Band	= 0 Hz to 3 Hz
Extreme Low Frequency (ELF) Band	= 3 Hz to 3 kHz
Very Low Frequency (VLF) Band	= 3 kHz to 30 kHz
Low Frequency (LF) Band	= 30 kHz to 300 kHz

PREFACE

Magnetic levitation (maglev) technology has the potential to provide very high speed travel with the capacity and convenient access of conventional passenger railways, while relieving U.S. highway and airport congestion.

A need exists for the assessment of the safety implications of this new form of guided ground transportation. This is the responsibility of the Federal Railroad Administration (FRA), which is charged with ensuring the safety of maglev systems in the United States under the provisions of the Rail Safety Improvement Act of 1988.

The fourth in a series of reports addressing high speed maglev transportation safety, this report, U.S. Maglev System Concept Definitions (SCDs) - System Safety Review presents the results of an independent system safety review of four proposed U.S. SCD maglev systems. The report is intended to assist the FRA in ensuring that potential safety-critical hazards and unsafe conditions associated with the SCDs and other proposed maglev system designs are identified and resolved early in the life-cycle of U.S. maglev system development.

As a part of the National Maglev Initiative (NMI), Magneplane, Foster-Miller, Grumman, and Bechtel prepared detailed system concept definition (SCD) final reports which conceptually define the technical feasibility, performance, and cost of constructing and operating their respective designs in the United States.

The respective SCD contractors were required to meet minimum safety requirements and perform a system hazard analysis to address safety considerations associated with their respective system characteristics. This report presents the results of the system safety review of the four SCD maglev technologies performed by Booz•Allen & Hamilton, Inc.

ACKNOWLEDGEMENT

This report was sponsored by the U.S. Department of Transportation (US DOT), Federal Railroad Administration's (FRA) Office of Research and Development. The authors wish to thank Robert L. Krick, Deputy Associate Administrator for Technology Development, and Arne J. Bang, Senior Program Manager, for their direction, helpful guidance, and input during the preparation of this document.

The authors wish to extend special thanks to Christopher J. Boon of the Canadian Institute of Guided Ground Transport; and G. Leslie Elliott, Paul Gottfried, Michael P. McDonald, J. Stephen Moore, Ruby T. Sakai, and Gary M. Schulman of Booz•Allen & Hamilton, Inc., for their contributions to the report.

The report was prepared under the direction of Stephanie H. Markos, US DOT/Research and Special Programs Administration/Volpe National Transportation Systems Center (RSPA/Volpe Center). The authors wish to acknowledge her; Robert M. Dorer, Volpe Center Project Leader for the High Speed Guided Ground Transportation Safety Project; Michael Coltman, Volpe Center Maglev Project Leader; David Tyrell, Volpe Center; and Frank L. Raposa; for their technical review and comment. Finally, Arthur H. Rubin, EG&G Dynatrend, provided important editorial support and assistance with report production.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF FIGURES

LIST OF FIGURES (Cont.)

LIST OF FIGURES (Cont.)

LIST OF FIGURES (Cont.)

LIST OF TABLES

1. INTRODUCTION

Magnetic levitation (maglev) technology has the potential to provide very high speed travel with the capacity and convenient access of conventional passenger railways, while relieving U.S. highway and airport congestion.

The U. S. government has organized the National Maglev Initiative (NMI) to determine the technical and economic viability of maglev technology in this country and, if appropriate, to consider incentives for U.S. industry to develop and deploy such systems. As a part of the NMI, four prime contractors were selected to conceptually define the technical feasibility, performance, and cost of constructing and operating their respective designs in the United States. Magneplane, Foster-Miller, Grumman, and Bechtel established working teams (including subcontractors) which prepared detailed system concept definition (SCD) final reports [1, 2, 3, and 4] combining the major elements of their respective maglev technologies into complete transportation systems. It was not the intent of the U.S. government to select a specific maglev SCD for further development, but rather to generate an input to decision-makers in evaluating the future direction of the NMI.

The respective SCD contractors were required to meet minimum safety requirements and perform a system hazard analysis to address safety considerations associated with their respective system characteristics. This report presents the results of an independent system safety review of the SCD maglev concepts performed under a contract to the Volpe National Transportation Systems Center (Volpe Center).

Major elements of the four SCD design and operation approaches (e.g., vehicle and guideway configuration, control system, etc.) proposed by the U.S. contractors are unique. Three of the SCDs propose the use of electrodynamic suspension (EDS) forces using superconducting magnets for levitation. One SCD design proposes the innovative use of a superconducting magnet to achieve electromagnetic suspension (EMS) forces for levitation.

1.1 BACKGROUND

The safety goal of any transportation system is to provide passengers and employees with the highest level of safety consistent with mission requirements. For maglev systems, the minimum design goal is a level of safety equivalent to current conventional U.S. railroad operations. However, because of the high-speed operation and highly automated technology, a higher level of safety may be necessary. In addition, evacuation of the general public and mobility-impaired passengers under emergency conditions is of particular concern due to the anticipated use of elevated and superelevated guideways.

The Volpe Center is assisting the Federal Railroad Administration (FRA) in assessing the safety of new high-speed guided ground transportation technologies proposed for U.S. operations. Current U.S. regulations, standards, specifications, practices, and guidelines (requirements) relating to passenger train safety are primarily technology-specific and based upon years of steel-wheel-on rail operating experience. Many of these requirements can be directly applied to maglev and other high-speed guided ground transportation systems, while others can be applied in concept to achieve a high level of safety. However, a comprehensive FRA standard for evaluating all safety-related aspects of proposed maglev systems for U.S. service does not exist at this time.

Since maglev systems are still under development, it is not possible to identify and resolve all potential system safety hazards. Moreover, operating data are not available to quantify the probability of undesired events for the U.S. environment. In addition, certain hazards can only be identified after the maglev system is built and installed. However, a systematic process can be used to analyze major maglev system elements and identify and resolve the majority of potential safety-critical hazards.

The Department of Defense (DoD) Military Standard System Safety Program Requirements (MIL-STD-882) [5] and Federal Aviation Administration Advisory Circular System Design and Analysis (AC25.1309.1A) [6] describe two similar approaches for ensuring that system safety is considered early in the life cycle of the system; each document provides guidance to the designer in performing hazard analyses.

1.2 PURPOSE

The purpose of this report is to assist the FRA in ensuring that potential safety-critical hazards and unsafe conditions associated with the SCDs and other proposed maglev system designs are identified and resolved early in the life-cycle of maglev prototype development. Accordingly, a major output is the identification of a set of safety issues and requirements related to each type of proposed SCD maglev system design, as well as a generic set of safety issues and requirements applicable to any proposed maglev system.

1.3 SCOPE

This report presents the results of the Booz•Allen & Hamilton (Booz•Allen) systematic review of the four SCD maglev technologies in terms of major system elements, as documented in each SCD final report. The system safety review was performed in terms of the safety requirements contained in the original SCD statement of work (SOW), as supplemented by additional issues identified by the SCDs, by the FRA/Volpe Center, or by Booz•Allen.

Due to the differences in proposed SCD technologies and the depth to which system designs were defined and analyzed in the SCD reports, as well as variations in individual SCD approaches to system safety, it was necessary for Booz•Allen to develop a methodology which could be used to provide a uniform, structured safety review of the SCDs. Chapter 2 further describes the Booz•Allen approach.

The primary source of information used to perform the Booz•Allen work effort consisted of the final reports submitted by the SCD teams in the fall of 1992 [1, 2, 3, and 4]. During the performance of the SCD development effort, presentations at two symposiums were given; three In-Progress Reviews were held; draft interim reports and briefing materials were also prepared. The review of information from those sources was considered outside the scope of this effort. Additional resources included reports relating to the German Transrapid EMS maglev technology [7, 8, 9, and 10] as well as reports relating to collision avoidance and accident survivability [11], and emergency preparedness [12, 13, and 14].

The scope of work did not require an assessment of the technical or operational merit of any of the design approaches, or the cost effectiveness of the respective SCDs.

The Booz•Allen work effort was directed at determining the degree to which each individual SCD final report addresses the following general safety issues: (1) prevention of safety-critical hazards and unsafe conditions, (2) minimization of the effects of such undesired events if they do occur, and (3) effective and timely response to emergencies.

In addition, the identification of safety issues and requirements for each type of proposed maglev system design represented in the respective SCD reports, as well as a generic set of safety issues and requirements considered applicable to any proposed maglev system, was required.

1.4 REPORT ORGANIZATION

Chapter 2 describes the approach developed by Booz•Allen to perform the review of system safety and emergency response provisions, as documented in each SCD final report. Chapters 3 through 6 present the results of the respective SCD safety reviews. Chapter 7 contains the results of the emergency response review and analysis for each respective SCD maglev design and operation. It should be noted that while these chapters contain summary descriptions of respective SCD major system elements, the final SCD reports contain a more comprehensive discussion of SCD maglev technology details. Chapter 8 describes safety issues and requirements for each type of proposed maglev system design represented in the respective SCD reports, as well as a generic set of safety issues and requirements considered applicable to any proposed maglev system.

Appendix A contains a brief description of the system safety process as applied to maglev systems. Appendices B-E contain the detailed matrices which include a review by safety event/issue as addressed in the SCD by specific reference to analysis and specific concept design text for mitigating hazards. Appendix F provides a tabular summary of the preliminary list of ***safety performance goals*** and ***specific design requirements*** and identifies their applicability to specific SCDs and subsystems.

2. SCD SAFETY REVIEW APPROACH

The proposed SCD maglev technologies have features that are unique to this mode of ground transportation. These features include:

- High speed (>482 kmph [300 mph]) at or near ground level;
- Lightweight vehicle structure, more like an airframe than a conventional passenger railcar;
- Propulsion, suspension, and braking systems that are not adhesion dependent;
- Highly automated command, control and communications equipment; and
- Guideway alignments that could make evacuation in an emergency difficult.

Alone and in combination, these features present hazards that are presently outside the experience of the U.S. railroad industry and the FRA regulatory environment.

The systematic process of identifying and resolving hazards before proposed maglev systems are placed into actual operation is required to ensure safety. This process can enable the system developers to modify design and operations to eliminate or minimize safety hazards prior to the final development, construction, and operation of the system, thus minimizing the cost of achieving a given level of safety. In addition, the documentation of the results of this process provides the FRA with important information for use in developing appropriate safety regulations for proposed maglev systems.

This chapter describes the approach used by Booz•Allen to examine the degree to which the SCDs complied with safety-related requirements as contained in the original SCD SOW, and the degree to which system safety was integrated into their respective technologies.

2.1 SCD SAFETY REQUIREMENTS

The SCDs were required to meet the specific safety-related requirements contained in Section C3 of the original SCD SOW, and listed in Table 2-1. In addition, Section C5 of the SCD SOW required the development of a system safety assurance plan, to include a "system hazard analysis." As a minimum, that analysis was to address the following hazardous events and issues:

- Loss of system power
- Loss of control and/or communication system
- Loss of levitation or guidance and levitation/guidance/magnet failures
- Loss of guideway integrity
- Guideway obstruction
- Fire
- Evacuation and rescue
- Operation restrictions
- Manual override, security and training
- Maintenance of safe headway

In addition to the Booz•Allen review of the above basic requirements, the review of the following safety issues was also required: other items identified by the SCD contractors, vehicle/guideway dynamics, electromagnetic interference, and guideway maintenance operations. Finally, Booz•Allen performed a supplementary analysis of each SCD to identify additional safety hazards.

The Booz•Allen scope of work did not require an assessment of the technical or operational merit of any of the design approaches, or the cost effectiveness of the respective SCDs.

2.2 SCD DOCUMENTS REVIEWED

The primary source of information used to perform the work effort consisted of the final reports submitted by the SCD teams in the fall of 1992 [1, 2, 3, and 4]. During the performance of the SCD

TABLE 2-1. MAGLEV SYSTEM CRITERIA RELATED TO SAFETY

SCD RFP S.O.W. SECTION C PART 3		SCD REQUIREMENTS RELATED TO SAFETY
3.1	Maglev System Criteria	
3.1.1	System Requirements	
3.1.1(e)	Magnetic Fields	– (DG) Human exposure to steady and fluctuating magnetic fields shall be minimized and consider current research findings.
3.1.1(f)	Weather	– (DG) Operation compatible with all common U.S. weather conditions (e.g., wind, snow, rain, fog, icing, heat, lightning, etc.) with minimal degradation in system performance.
3.1.1(g)	Controls	– (MR) All controls must be fully automated and fail-safe. (DG) A central facility will operate the system, receiving and integrating data regarding the status and integrity of all vehicles and guideways, the locations of all vehicles, guideway power requirements, vehicle routing requests, etc. (MR) The system control software must also be fail-safe, equivalent to the level of reliability defined by the Federal Aviation Administration (FAA) for flight control software for military and civilian aircraft. See Federal Aviation Regulation 25.1309, Amendment 25-23 and Advisory Circular 25.1309-1.
3.1.1(h)	Safety	– (MR) A system safety plan must be included which discusses possible failure modes, human operation considerations, evacuation procedures, system restart, equipment and software availability, safety inspections, consequences of vandalism and trespassing, etc. The central control facility will log all operations and communications for subsequent analysis in the event of a failure. Consideration must be given to safe use of materials and construction methods, and to the safety of other users of the rights-of-way.
3.1.1(l)	Communications	– (DG) The system will include provisions for non-vital voice, data, and video communication capability.
3.1.1(m)	Human Factors	– (DG) Human factors considerations, including the operator, passengers and maintenance considerations shall be evidenced in the design.
3.1.2	Vehicle Requirements	
3.1.2(b)	Braking System	– (MR) Vehicles must have redundant braking systems which are fail-safe. Normal braking of up to 0.2g should be considered.
3.1.2(c)	Structural Integrity	– (MR) Vehicles must safely withstand high-speed impacts with small objects such as birds, debris, snow and ice. Vehicles must also have adequate fatigue life and low-speed crash worthiness and shall sustain only minimum damage in a 2.2 m/s (5 mph) impact.
3.1.2(d)	On-Board Power	– (DG) All power for normal hotel functions, controls, levitation, etc. should be transferred from the guideway. (MR) The Vehicle must be equipped with emergency power for operation, as appropriate within the system safety plan.

(DG) – Design Goal
(MR) – Minimum Requirement

TABLE 2-1. MAGLEV SYSTEM CRITERIA RELATED TO SAFETY (Cont.)

SCD RFP S.O.W. SECTION C PART 3		SCD REQUIREMENTS RELATED TO SAFETY
3.1.2(e)	Emergency Systems	– (MR) Vehicles must include emergency systems for fire fighting, lighting, HVAC, evacuation, communication, etc. as appropriate within the system safety plan.
3.1.2(f)	Instrumentation and Controls	– (MR) The system shall include instruments which monitor the integrity of the guideway (presence of debris, snow and ice, misalignment or deterioration of guideway, etc.) and the status of on-board systems (propulsion, levitation, guidance, power, safety, etc.). Data acquired should be recorded and fully integrated into vehicle and overall-system controls to allow appropriate response in emergency and normal operations. In normal operations, vehicles will be monitored or controlled from a central facility. However, vehicles will include manual controls for emergency and maintenance operations.
3.1.3	Guideway Requirements	
3.1.3(a)	Structural Integrity	– (MR) Civil structure (foundation and structure supporting the guideway) shall have a minimum 50-year life. Consideration shall be given to structural integrity under earthquake and high-wind conditions.
3.1.3(e)	Instrumentation and Controls	– (MR) The system shall include instruments which monitor guideway integrity (presence of debris, snow and ice, misalignment or deterioration of guideway, etc.), the status of its subsystems (propulsion, levitation, guidance, power, entries/exits, etc.) and the locations and velocities of all vehicles. Data acquired should be fully integrated into guideway and overall-system controls to allow response in both emergency and normal operations.
3.1.3(f)	Tunnels	– (MR) Design of tunnels shall address issues of comfort, noise and safety, with special attention to vehicle entry and passing vehicles.
3.1.3(g)	Power Systems	– (DG) Power systems should be sized to provide vehicle acceleration and braking capacity for all operating conditions and should be capable of meeting requirements for system capacity. Guideway power systems should be capable of sustaining vehicles at full cruising speed up sustained grades of 3.5:100, and provide vehicle propulsion at reduced speeds up a maximum grade of 10:100.
3.1.3(h)	Superelevation	– (MR) Superelevated (banked) guideways must provide for safe operation of vehicles at all speeds from zero to the maximum design speed of the curve. Emergency evacuation must be possible from vehicles stopped in a curve.
3.2	SCD Elements	– The contractor shall, as a minimum, address following elements:
3.2.1	Vehicle	
3.2.1(a)		– Levitation and guidance systems including magnet design and configuration, cooling, control system requirements, power requirements, and failure modes.
3.2.1(c)		– Structural design considerations, including weight and crash worthiness considerations.

(DG) – Design Goal
(MR) – Minimum Requirement

TABLE 2-1. MAGLEV SYSTEM CRITERIA RELATED TO SAFETY (Cont.)

SCD RFP S.O.W. SECTION C PART 3	SCD REQUIREMENTS RELATED TO SAFETY	
3.2.1(d)		– Braking system, including regenerative, aerodynamic, mechanical or other suitable means.
3.2.1(e)		– Active and/or passive banking, including the minimum horizontal and vertical radii of curvature as a function of vehicle velocity.
3.2.1(f)		– Aerodynamics, including calculated internal and external noise intensities, and innovative design techniques to reduce drag and/or noise.
3.2.2	Guideway	
3.2.2(a)		– Civil structural elements, including piers, footings, columns, spans and materials used and adjustability of structure to maintain required alignment.
3.2.2(b)		– Maglev active/passive elements, including propulsion, guidance and levitation system components, mounting and means of alignment adjustment, and optimum material properties.
3.2.2(c)		– Alignment tolerances, and sources of disturbances (expansion gaps, thermal distortion, warpage, differential settlement of substructure, wear, etc.).
3.2.2(d)		– Entry/exit method, including maximum speeds, impact on headway, physical size and configuration.
3.2.2(f)		– Power requirements, proposed distribution method, lightning protection and grounding.
3.2.2(i)		– Instrumentation for sensing guideway integrity and vehicle positions.
3.2.3	System Considerations	
3.2.3(a)		– Communications and control systems, including overall philosophy, principal elements, software hardware integration and verification and validation methodology.
3.2.3(h)		– Reliability plan for assuring safety and high availability, including the major subsystems (vehicle, infrastructure, power distribution, communications and control) and their primary functions (propulsion, levitation, guidance, braking, etc.).

(DG) – Design Goal
(MR) – Minimum Requirement

development effort, three In-Progress Reviews were held; draft interim reports and briefing materials were also prepared. The review of those documents was considered outside the scope of this effort.

2.3 REVIEW METHODOLOGY

Since maglev systems are still under development, it is not possible to identify and resolve all potential system safety hazards. Moreover, operating data are not available to quantify the probability of undesired events for the U.S. environment. In addition, certain hazards can only be identified after the maglev system is built and installed. However, a systematic process can be used to analyze major maglev system elements and identify and resolve the majority of potential safety-critical hazards. The Department of Defense (DoD) Military Standard System Safety Program Requirements (MIL-STD-882) [5] and Federal Aviation Administration Advisory Circular System Design and Analysis (AC25.1309.1A) [6] describe two similar approaches for ensuring system safety is considered early in the life cycle of the system and each document provides guidance to the designer in performing hazard analyses.

The four maglev system concepts differed in technology and the depth to which the system design was defined and analyzed in the SCD reports. Similarly, the SCDs were not consistent in their approach to system safety, hazard identification, and hazard resolution. The approach used by the SCD teams did not uniformly comply with the original SCD SOW safety requirements, the type and level of system hazard analyses performed varied greatly, and means of addressing emergency response varied. Moreover, although the SCDs made references to MIL-STD-882B (MIL-STD-882B was superseded by MIL-STD 882C on January 19, 1993.) and AC 1309.1A, the SCD contractor interpretations of these documents varied. As a result, it was necessary for Booz•Allen to develop a uniform methodology which could be used to provide a structured safety review of the SCDs, despite these variations. The remainder of this chapter describes the Booz•Allen approach in more detail.

2.3.1 SCD Maglev Technology Review

Each SCD final report was examined to determine the type of overall system safety approach used by the respective SCD. A description was then developed of the major system elements for each respective SCD maglev technology. The SCD reports were then reviewed in terms of the requirements in Sections C3 and C5 of the original SCD SOW (supplemented by the items listed previously in section 2.1). These requirements were reviewed in a matrix format, as illustrated in Figure 2-1.

Other documents which were reviewed relating to maglev system safety included reports relating to the German Transrapid EMS maglev technology [7, 8, 9, 10,] as well as reports relating to collision avoidance and accident survivability [11].

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
RFP REQUIRED SAFETY ISSUES	HOW RESOLVED IN THE CONTRACTOR'S SAFETY ANALYSIS	HOW RESOLVED IN OTHER SECTIONS OF THE SCD	OPEN ISSUES OR COMMENTS

FIGURE 2-1. EVENT/ISSUE MATRIX

For each event/issue, the respective SCD system hazard analysis was reviewed for accuracy and completeness, and the "resolution" or "control method" was documented. For ease of reference, paragraph numbers used in the SCD reports are indicated in the matrices contained in Appendices B-E by parenthesis with an abbreviation of the prime contractor: Magneplane (MP), Foster-Miller (FM), Grumman (GM), and Bechtel (BEC). The remainder of each SCD was then reviewed to:

- Confirm the inclusion of the relevant design feature proposed in the system hazard analysis;
- Identify any system features that "control" hazards but were not covered in the safety analysis; and
- Identify safety issues such as safety-critical hazards that were not addressed, hazard classifications that were inconsistent, and ambiguities that will require further system development.

Category I and II hazards were identified for each event/issue and subsystem element. Hazards were evaluated in terms of the severity categories defined in the FRA report Safety of High Speed Magnetic Levitation Transportation Systems: Preliminary Safety Review of The Transrapid Maglev System [7]:

- **CATEGORY I (Catastrophic):** Death to passenger or employee, loss of maglev system.

- **CATEGORY II (Critical):** Severe injury to passenger or employee; hazard or single point failure may lead to catastrophe if action is not taken to control situation or rescue individual. Critical systems are involved, and the maglev vehicle is unable to move to an evacuation area. Time of response is important in preventing death or system loss.

- **CATEGORY III (Marginal):** Minor injury not requiring hospitalization or the hazard present does not by itself threaten the safety of the maglev system or passengers. No critical systems are disabled, but could be if additional failure(s)/malfunctions(s)/ hazard(s) occur.

- **CATEGORY IV (Negligible):** Less than minor injury. Does not impair any of the critical systems.

Narrative text was then prepared for each SCD major maglev system element to summarize the results of the detailed review contained Narrative text was then prepared for each SCD major maglev system element to summarize the results of the detailed review contained in the matrix tables. In addition, the general overall SCD approach to safety associated with each SCD maglev technology was reviewed and unresolved safety issues were highlighted.

2.3.2 <u>Emergency Response Review</u>

The emergency response provisions for each respective SCD were reviewed and analyzed in terms of the requirements contained in appropriate sections of Table 2-1. Several published documents relating to rail transportation emergency preparedness were used as resources during the review [12, 13, and 14].

For each SCD, the emergency capabilities were reviewed in terms of communications, on-board power supply, different vehicle evacuation strategies, and vehicle cabin/passenger compartment layout and exits. Advantages and concerns associated with each approach are highlighted.

2.4 DEVELOPMENT OF SAFETY ISSUES AND REQUIREMENTS

2.4.1 <u>Application of Requirements to Resolve Safety Issues</u>

Safety requirements must address generic maglev safety issues while at the same time be applicable to any proposed maglev system technology. They must also be stringent enough to ensure safe maglev operation while not limiting the innovative engineering effort required to maximize this new technology. The use of traditional methods to create technology-specific requirements is currently not possible because U.S. maglev system development is still in the concept definition phase.

To allow for design innovation, requirements should be specified as ***safety performance goals;*** such as, ***complete loss of braking capability shall be shown to be improbable through the use of*** *appropriate analyses*. However, if design innovation is allowed to progress with unlimited freedom, there is a danger that very nonconventional designs will be proposed, resulting in an extended concept definition phase. In addition, if only *safety performance goals* are specified, then proven technologies and design solutions which are known to be safe, may be excluded from proposed designs. Reference 11 provides further discussion of the need to combine *safety performance goals* and *specific design requirements* in safety requirements. As a result of the SCD system safety review, safety requirements for maglev systems were identified as defined below:

- *Safety performance goals* provide for design innovation while controlling the level of safety in the end product. These are stated in terms of top level events, e.g., *complete loss of braking capability shall be shown to be improbable through the use of appropriate analyses*.

- *Specific design requirements* require the designer to incorporate specific design characteristics which will reduce the severity and/or probability of known hazards. For example, *the cryogenic cooling system shall incorporate redundant pressure relief valves to prevent system overpressurization*.

By combining both types of requirements, safety requirements can be developed that provide for U.S. maglev system safety while encouraging design innovation. Chapter 8 of this report describes safety requirements for each major maglev system element. Appendix F provide a tabular summary of the preliminary list of *safety performance goals* and *specific design requirements* and identifies their applicability to specific SCDs and subsystems.

2.4.2 Developing Safety Performance Goals

The Preliminary Hazard Analysis (PHA) is a systematic tool for developing *safety performance goals*. The PHA is a high-level examination of a proposed system's functions. The PHA identifies and categorizes potential hazards and undesired events that the functions can cause or contribute to, not only due to malfunction, but also in normal operation. A PHA addresses the vulnerability of system functions; it is not an assessment of any particular hardware or software design.

A PHA is qualitative analysis and is conducted using experienced engineering judgment. For complex functions requiring new designs, such as many maglev subsystems (e.g., propulsion, levitation, guidance, guideway switch, C^3, etc.), a new formal PHA should be prepared to provide a thorough identification of potential hazards. For functions that are not complex, evidence of satisfactory service experience of similar functions based on other high speed rail, conventional railroad, or transit applications may provide sufficient information.

The purpose of the PHA is to develop ***safety performance goals*** for the system and to establish the framework for subsequent safety analysis and a certification plan (see Appendix A). For systems containing software, the PHA provides the foundation for establishing software development and documentation requirements. The PHA provides information about potential hazards and undesirable events and assigns severity categories. A probability requirement is assigned to each severity category.

Design standards relate the severity of the hazard/undesirable event (e.g., mishap) to the probability of it occurring. In order to assign severity and probability categories, these categories must be defined. MIL-STD-882, AC 1309.1A, and previous studies completed for the FRA [7, 8, and 11] discuss methods for assessing the causes, severities, and likelihood of potential mishaps. The severity category descriptions previously described could be applied to the maglev NMI prototype development program. The following definitions used to describe the probability of mishaps are those cited in Reference 7:

- **FREQUENT** mishaps are not unusual events. They could occur several times in annual operations.
- **PROBABLE** mishaps could occur several times in the lifetime of the maglev system.

- **OCCASIONAL** mishaps are expected to occur at least once in the lifetime of the maglev system.
- **REMOTE** mishaps are unlikely to occur during the lifetime of the maglev system.
- **IMPROBABLE** mishaps are those so unlikely that they are not expected to ever occur during the lifetime of the maglev system.

Using these definitions, maglev systems should be designed and constructed so that:

- **FREQUENT** and **PROBABLE** mishaps are no more severe than **CATEGORY IV**
- **CATEGORY III** mishaps are at least **OCCASIONAL**
- **CATEGORY II** mishaps are at least **REMOTE**
- **Category I** mishaps are **IMPROBABLE.**

To provide guidance forr determining a probability requirement for each category, the safety record of existing transportation systems provides a suitable source of data. A comprehensive study of accident rates for passenger railroad systems and domestic air travel was recently completed which provides a basis for developing probability goals for maglev subsystems [11]. However, the probability goals developed in this study are stated in "accidents per passenger-km (ft)" and should be converted into more useful requirements for design guidance, such as "probability of occurrence per operational hour."

2.4.3 General Design Principles for Resolving Hazards

There are many design principles or techniques which can be used to promote safe design. The use of only one of these principles or techniques is seldom adequate for resolving a Category I or II hazard; a combination of two or more is usually needed. Several techniques are listed below:

GPO Form 2511
(R 1-89) P. 57870-3

cover dummy

CHARLES E. REED #1150 Rec. 11/24

PRINT ORDER

You are hereby authorized to manufacture and ship the following described product in accordance with the purchase order and specifications indicated.

DEPARTMENT: DOT/FRA	REQ. NO: 4-00253/4-60028	DATE: 11-24-93	PURCHASE ORDER NO.: 93815	PRINT ORDER NO.: 80419
CONTRACTOR: FRY COMMUNICATIONS, INC.		JACKET NO.: 301-717	ESTIMATED COST: $	SHIP/DEL DATE: 12-06-93 MUST AT DEST
TITLE: SAFETY OF HIGHSPEED		OBJECT CLASS: 2400 / STATE CODE: 370	CONTR'S CODE: 34690	PROGRAM NO.: 659-S
PROOFS: Galley / Page / Blues; SETS; DATE DUE TO GOVT; DAYS GOVT WILL HOLD; RETURN DATE TO CONTR.		APPROPRIATION CHARGEABLE	BILLING ADDRESS CODE (BAC): 491001	QUANTITY: 107
		COMPOSITION: Phototype / Cold Type / Hot Metal	QUALITY LEVEL: III	TRIM SIZE: 8 1/2 X 11
MATERIAL FURNISHED TO CONTRACTOR: Manuscript; Halftones; Line Illus.; Camera Copy: 367		Negatives; Binders	Other	
TEXT STOCK: OFFSET-WHITE-SUB 50	COVER STOCK: VELLUM-WHITE-SUB 50	NO. OF TEXT PAGES (Including Blanks): 376	FOLD-IN STOCK	
FOUR COLOR PROCESS PRNTG.: Cover 1 2 3 4 Text	COLOR OF INK: Cover BLUE PMS-300; Text BLACK	COVER PRINTS: 1 2 3 4 — NC X X X X (1st LC NG)	FOLD-INS/FORMS: Face Only / Face & Back	STRIP-INS; NEGATIVES (No. Required)

BINDING

1 ULC	Sew	Band units of	Drill ___ round holes ___ " in diameter on ___ side ___ inches c. to c.
Saddle	Trim 4 Sides	Shrink Film Wrap units of	Center of holes ___ inches from ___ edge of sheet
Side	Perf. on Fold	Other	Pads of ___ sheets/sets each. Pad on the ___ " side. Chipboard required.
Perfect X	Adhesive Strip		Pack ___ per shipping container. ☐ Pallets required.

DISTRIBUTION

RETURN NEGS TO GPO FOR STORAGE NO XX YES ☐

1 DOT/OST, M482.2, RM 2311
ATTN: CR
400 7TH ST SW WASH., DC 20590

RETURN ORIG. AND/OR NEGS. TO: DOT/FRA, RAD-32, RM 8222
ATTN: TRIGONOPLOS
400 7TH ST SW WASH., DC 20590

90 DOT/WAREHOUSE, INITIAL DISTRI
ARDMORE EAST BUSINESS CENTER
3341Q 75TH AVE LANDOVER, MD 20785

SHOOT: S/S MARGINS: FOLLOW CC
PRINT: H/H
ASSEMBLE: PERFECT BIND WITH PRINTED SPINE COVER; CIRCLE FOLIO 1 THRU 376 ALL

16 SEE ATTACHED MEMORANDUM

NOTE: FOLLOW SAMPLE FOR STYLE AND COLOR SCHEME OF COVER 1, 4, AND SPINE.

SUPT OF DOCS DOES RIDE

Departmental Authority (Signature and Title)	Purchase Obligation	DATE SENT TO CONTRACTOR
Chief Contract Admin. [signature]	69 X 4520(01)	11-26-93

CONTRACTOR TO COMPLETE BOTTOM PORTION AND MAIL ENTIRE FORM TO: COMPTROLLER-FME, FINANCIAL MANAGEMENT SERVICE, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, D.C. 20401

Contractor Invoice No. ____________ Date Prepared ____________

Date of Delivery/Shipment ____________ Discount Terms ____________

ARTICLES OR SERVICES	QUANTITY	COST	UNIT PRICE PER	AMOUNT
IF ADDITIONAL SPACE IS REQUIRED, USE STD. FORM 1034, 1035, OR ATTACH YOUR INVOICE.			TOTAL	

I CERTIFY THAT THE MATERIAL, GOODS, OR SERVICES HAVE BEEN DELIVERED/SHIPPED ON THE DATE INDICATED ABOVE AND THAT PAYMENT OR CREDIT HAS NOT BEEN RECEIVED.

... to the Government is prescribed in 18 USC 1001 *U.S. GPO: 1993-342-107/80560 (Signature of person authorized to sign)

DUC 12-3 301-717 PT 3rd

CODES
HT - *Halftone*
NF - *Neg. Fum.*
FO - *Fold-out*

FINISH SIZE	PUB. NO./TITLE	QUANTITY	JOB NO.
☐ 8 x 10½ ☒ 8½ x 11 ☐ ______	SAFETY OF HIGHSPEED	—	80419-659

FACE	PAGE NUMBER Cov 1	CODE	REMARKS	BACK	PAGE NUMBER Cov 2	CODE	REMARKS
01	REPORT DOCUMENTATION			02	ii		
03	iii / iv			04	—		
05	v / vi			06	—		
07	vii			08	viii		
09	ix			10	x		
11	xi			12	xii		
13	xiii			14	xiv		
15	xv			16	xvi		
17	xvii			18	xviii		
19	xix			20	xx		
21	1-1			22	1-2		
23	1-3			24	1-4		
25	1-5 / 1-6			26	—		
27	2-1			28	2-2		
29	2-3			30	2-4		
31				32			
33				34			
35				36			
37				38	2-12		
39	2-13 / 2-14			40	—		
41	3-1			42	3-2		
43				44			
45				46			
47				48			
49	3-9			50	3-10		

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
51	3-11			52	3-12		
53				54			
55				56			
57				58			
59				60			
61				62	3-22		
63				64			
65				66			
67				68			
69				70			
71				72	3-32		
73				74			
75				76			
77	3-37			78	3-38		
79	4-1			80	4-2		
81				82			
83				84			
85				86			
87				88			
89				90	4-12		
91				92			
93				94			
95				96			
97				98			
99	4-21			100	4-22		

RECAP	TOTAL PAGES	BLANK PAGES	PRINTED PAGES	FOLDOUTS	HALF TONES	COVERS	PAGE NO.
	376	10	366			4 (1.2.4 ASP)	1 OF 4

CODES
HT - *Halftone*
NF - *Neg. Furn.*
FO - *Fold-out*

FINISH SIZE
☐ 8 x 10½ ☐ 8½ x 11
☐ ____________

PUB. NO./TITLE

QUANTITY

JOB NO. 80419-659

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
01	7-27			02	7-28		
03				04			
05				06			
07				08			
09				10			
11				12	7-38		
13				14			
15				16			
17				18			
19				20			
21				22	7-48		
23				24	7-50		
25	7-51/7-52			26	—		
27	8-1			28	8-2		
29				30			
31				32			
33				34			
35				36			
37				38	8-12		
39				40			
41				42			
43				44			
45				46			
47				48	8-22		
49	8-23			50	8-24		

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
51	8-25			52	8-26		
53	8-27			54	8-28		
55	9-1			56	9-2		
57	9-3			58	9-4		
59	A-1			60	A-2		
61				62			
63				64			
65				66			
67				68			
69				70	A-12		
71	A-13			72	A-14		
73	A-15/A-16			74	—		
75	B-1			76	B-2		
77				78			
79				80			
81				82			
83				84			
85				86			
87	B-13			88	B-14		
89	C-1			90	C-2		
91				92			
93				94			
95				96			
97				98			
99	C-11			100	C-12		

RECAP	TOTAL PAGES	BLANK PAGES	PRINTED PAGES	FOLDOUTS	HALF TONES	COVERS	PAGE NO.
							3 OF 4

CODES	FINISH SIZE	PUB. NO./TITLE	QUANTITY	JOB NO.
HT - *Halftone* NF - *Neg. Furn.* FO - *Fold-out*	☐ 8 x 10½ ☐ 8½ x 11 ☐ ________			80419-659

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
01	7-27			02	7-28		
03				04			
05				06			
07				08			
09				10			
11				12	7-38		
13				14			
15				16			
17				18			
19				20			
21				22	7-48		
23				24	7-50		
25	7-51/7-52			26	—		
27	8-1			28	8-2		
29				30			
31				32			
33				34			
35				36			
37				38	8-12		
39				40			
41				42			
43				44			
45				46			
47				48	8-22		
49	8-23			50	8-24		

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
51	8-25			52	8-26		
53	8-27			54	8-28		
55	9-1			56	9-2		
57	9-3			58	9-4		
59	A-1			60	A-2		
61				62			
63				64			
65				66			
67				68			
69				70	A-12		
71	A-13			72	A-14		
73	A-15/A-16			74	—		
75	B-1			76	B-2		
77				78			
79				80			
81				82			
83				84			
85				86			
87	B-13			88	B-14		
89	C-1			90	C-2		
91				92			
93				94			
95				96			
97				98			
99	C-11			100	C-12		

RECAP	TOTAL PAGES	BLANK PAGES	PRINTED PAGES	FOLDOUTS	HALF TONES	COVERS	PAGE NO.
							3 OF 4

CODES
HT - *Halftone*
NF - *Neg. Fum.*
FO - *Fold-out*

FINISH SIZE ☐ 8 x 10½ ☐ 8½ x 11 ☐ ______

PUB. NO./TITLE

QUANTITY

JOB NO. 80419-659

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
01	D-1			02	D-2		
03	↓			04	↓		
05				06			
07				08			
09				10			
11				12	D-12		
13				14	↓		
15				16			
17				18			
19				20			
21				22	D-22		
23				24	↓		
25				26			
27				28			
29				30			
31				32	D-32		
33				34	↓		
35				36			
37				38			
39				40			
41				42	D-42		
43				44	↓		
45	D-45			46	D-46		
47	E-1			48	E-2		
49	E-3			50	E-4		

FACE	PAGE NUMBER	CODE	REMARKS	BACK	PAGE NUMBER	CODE	REMARKS
51	E-5			52	E-6		
53	↓			54	↓		
55				56			
57				58			
59	E-13			60	E-14		
61	E-15 / E-16			62	——		
63	F-1			64	F-2		
65	↓			66	↓		
67				68			
69				70			
71				72			
73				74			
75	F-13			76	F-14		
77				78	Cov 4		
79				80			
81				82			
83				84			
85				86			
87				88			
89				90			
91				92			
93				94			
95				96			
97				98			
99				100			

RECAP	TOTAL PAGES	BLANK PAGES	PRINTED PAGES	FOLDOUTS	HALF TONES	COVERS	PAGE NO.
							4 OF 4

BLANKS (10)

IMP= 9A4

2D2 — 5F5 —
2F2 — ~~6C5~~
2B5 — ~~7C5~~
2D4 — 9C5
4C2 —
4A4 —

- **Redundancy or Backup Systems** - to enable continued functioning after any single failure or other defined number of failures. Redundancy is the presence of more than one independent means for accomplishing a given function or operation. Each means need not necessarily be identical.

- **Isolation or Independence of Systems, Components, and Elements** - so that the failure of one system, subsystem, or component does not cause the failure of another.

- **Failure Warning or Indication** - to provide early detection of failures.

- **Procedures** - for use after failure detection, to enable continued safe operation by specifying corrective action.

- **Checkability** - to assess a component's condition periodically. This involves pre-trip checks and maintenance checks at defined periods of time.

- **Proven Reliability** - so that multiple, independent failures are unlikely to occur during the same trip.

- **Margins or Factors of Safety** - to allow for any undefined or unforeseeable adverse conditions.

3. BECHTEL SCD

The Bechtel baseline, illustrated in Figure 3-1, is an electrodynamic system (EDS) using vehicle-mounted flux canceling coils which provide liftoff at speeds as slow as five to ten m/s (11.3 to 22.5 mph). Below these speeds, the vehicle operates on air-bearing pads. The vehicle consists of a single 120-passenger car. The single car configuration will meet the 4,000 passengers-per-hour requirement operating at 108 seconds or on shorter headways. The vehicle is constructed with an outer aluminum shell surrounding an inner cabin shell. The inner cabin can be tilted up to 15 degrees relative to the outer fixed shell without disturbing the aerodynamic outer surface. Bechtel proposes guideway banking up to 15 degrees that, with the vehicle inner cabin tilt, will allow the vehicle to negotiate a 3,000 m (9090 ft) radius curve at 134 m/s (300 mph) with negligible lateral acceleration force on the passengers. Switching is by a bendable beam constructed of fiber-

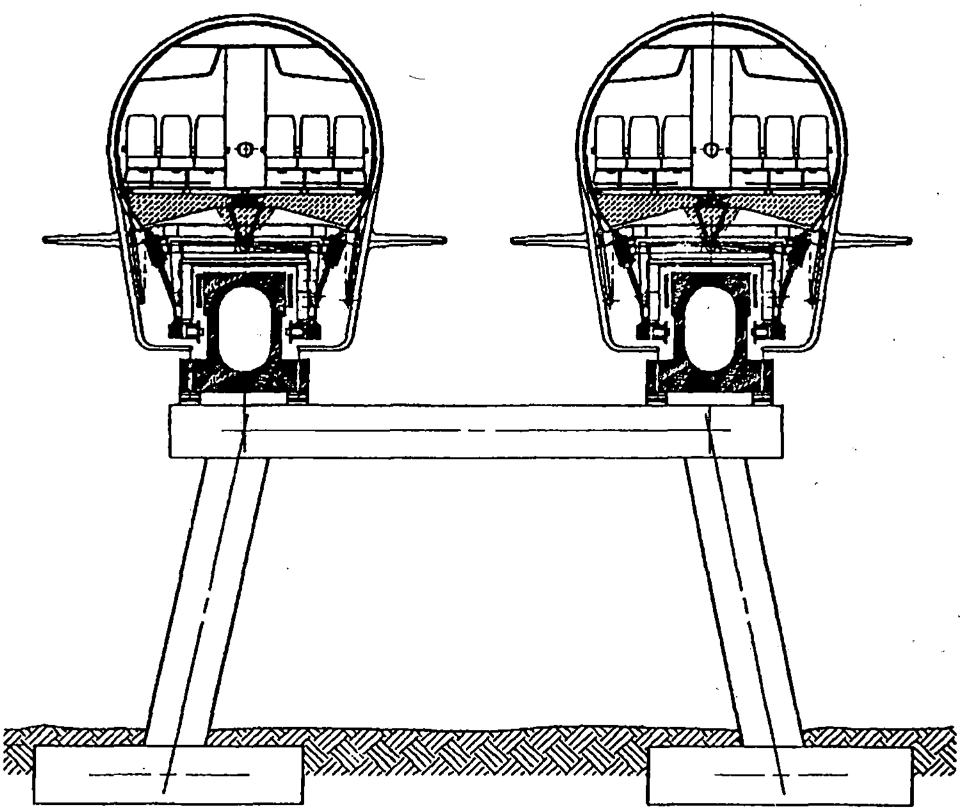


FIGURE 3-1. BECHTEL GUIDEWAY AND VEHICLE CROSS-SECTION

reinforced plastic. The guideway consists of a post-tensioned, eight-span box girder supported on concrete piers. Levitation is provided by the onboard superconducting magnets (SCM) arranged in coil sets distributed along each side of the vehicle. These coils interact with an aluminum ladder-like structure mounted on each side face of the guideway. Guidance is provided by null-flux coils mounted inside and outside of each ladder reacting against the levitation coils on the vehicle. The propulsion coils are located on the outside sidewalls of the box beam and interact with the onboard SCMs to produce thrust.

This chapter presents the results of the safety review of the Bechtel system based on the approach described in Chapter 2. The design features of each major system element are described and safety-related issues are identified. The narrative discussion of safety issues within the following subsections represent the results of the detailed safety review contained in the matrices in Appendix B. Information used for this review is derived from the final Bechtel SCD report [1].

3.1 BECHTEL OVERALL SAFETY APPROACH

The stated Bechtel safety approach is to eliminate safety-critical hazards through design; when the hazard cannot be totally eliminated, the probability of its occurance has been reduced to a minimum through use of fault avoidance and fault tolerant techniques. The process Bechtel uses is (1) establish the hazard severity categories to be used and assign an allowable probability value for hazards of each category, (2) identify specific potential hazards associated with maglev rapid transit, and (3) develop design approaches which mitigate the hazards or reduce their probabilities to acceptable levels.

The Bechtel approach recognizes the key distinction (yet connection) between reliability and safety. Bechtel defines reliability as the probability of successfully completing a mission without mishap. Safety is defined as the probability of successfully completing a mission without mishap, but failure is allowed as long as safety is maintained. However, with the exception of air bearings, the SCD text does not explicitly identify reliability items which are related to safety issues.

To resolve identified hazards resulting from system faults and failures, Bechtel states that the following specific design techniques have been considered:

- **Fault Avoidance** - Elimination of the fault or limiting the probability that the fault occurs.
- **Fail Safe** - If a hazardous fault occurs, the system reverts to a known, safe state.
- **Fail Degraded** - If a hazardous fault occurs, the system reverts to a degraded or restricted operating mode.
- **Fail Operational** - A single fault has no operational effect, and a second fault is fail safe or degraded.
- **Fail Operational Squared** - There is no operational effect with more than one fault.

Bechtel proposes to develop safety plans during later program phases which will detail specific analyses to be used for certification, and reporting requirements. These plans will implement formal MIL-STD-882B type safety programs. Bechtel provides a table listing MIL-STD-882B tasks by program phase, showing when each task will be applied.

Eight hazard severity categories were selected which were adapted and expanded from MIL-STD-882B, and an allowable probability was assigned to each category. However, no quantitative analyses of any specific design features were provided. Bechtel's primary effort was to develop a preliminary hazard list (PHL) of the baseline system.

High-level generic design techniques are listed for each of the identified hazards that are to be "employed to minimize the hazard probability." However, while many of the listed techniques are intended to mitigate the hazard effect, they have no influence on its probability of occurring. As an example, for the hazard of

"Fire aboard vehicle," a design technique recommendation is "Fully automated detection and suppression systems designed into vehicle;" this type of recommendation does not reduce the probability of the fire occurring, i.e., through preventing ignition, through use of materials which resist flame spread.

The majority of the hazards identified by Bechtel cover the baseline hazards/issues specified in the SCD SOW and identified in Chapter 2 of this report. These identified hazards were grouped by Bechtel into the following types:

- Fire/Explosion
- Vehicle Collision
- Vehicle Leaves Guideway
- Sudden Stop
- Vehicle does not Slow/Stop at Station
- Vehicle Stranded Between Stations or Safe Evacuation Points
- Unable to Rescue Passengers
- Passenger Illness or Injury

Manual operation, security, training, maintenance operations, and passenger evacuation are considered procedural hazards, and are not addressed in the PHL. Bechtel indicates these procedures will be developed during later phases of the maglev program. However, these topics are addressed to a limited extent in Part E, Operations and Maintenance Plan, of the Bechtel report. Also, no PHL entries are included for tunnels or electromagnetic interference (EMI) hazards.

In addition to the baseline hazards listed in the SCD SOW, Bechtel addresses seven other hazards in the PHL. They are:

- Vehicle exterior breached by object, a Category I event.
- Passenger injured by high voltage, a Category II event.
- Passenger injured by automatic door, a Category II event.
- Door opens at high speed, a Category II event.

- Passenger trips while entering or leaving vehicle, a Category II event.
- Passenger trips while inside vehicle, a Category II event.
- Sudden high negative acceleration, a Category II event.

Specific design approaches proposed to mitigate the hazards addressed by Bechtel in the PHL are summarized in Appendix B of this report.

3.2 VEHICLE STRUCTURE AND INTERIOR DESIGN

3.2.1 System Description

Bechtel proposes a monocoque-type vehicle structure, using high strength aluminum for the skin and structural members. A cross-section of the vehicle is shown in Figure 3-2. Bechtel asserts this type of construction has a low weight-to-strength ratio and is amenable to energy-absorbing controlled deformation-type collision protection. A separate internal tilting coach is used to reduce interior aerodynamic noise while having minimal impact on vehicle mass and aerodynamic drag.

The coach resembles the passenger compartment of a Boeing 737 but with more doors and wider aisles to facilitate rapid loading and unloading. The passenger capacity is 120 in six-abreast seating with luggage carried on the same level as the passengers. Additional space is available for high priority freight. A configuration providing some four-abreast business or first class seating can also be used, resulting in a 106-passenger single vehicle.

Six bogies provide the structural connection between the propulsion and levitation systems and the body. The bogie frames house the magnet modules, support the vehicle weight through coil springs and hydraulically controlled dampers, and transmit forces between the guideway and vehicle. The bogie frames also house elements of the air-bearing system for very low speed suspension.

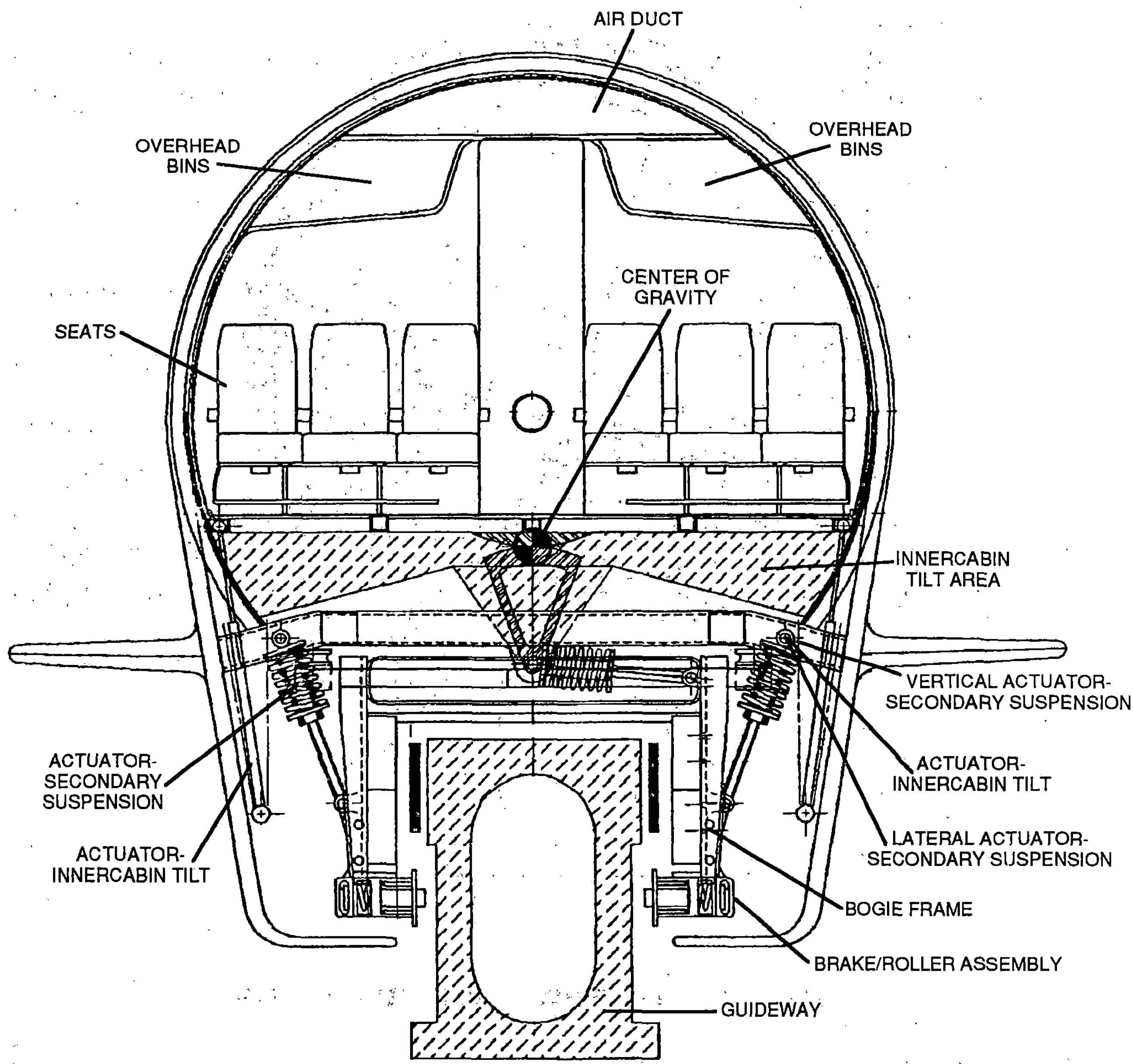


FIGURE 3-2. BECHTEL VEHICLE

The vehicle design uses an internal coach structure which can be tilted up to 15 degrees to either side relative to the vehicle outer shell structure as shown in Figure 3-3. The internal coach contains all passenger seats, toilets, and galleys. The tilting coach utilizes ball bearing supports along the pivot center line at

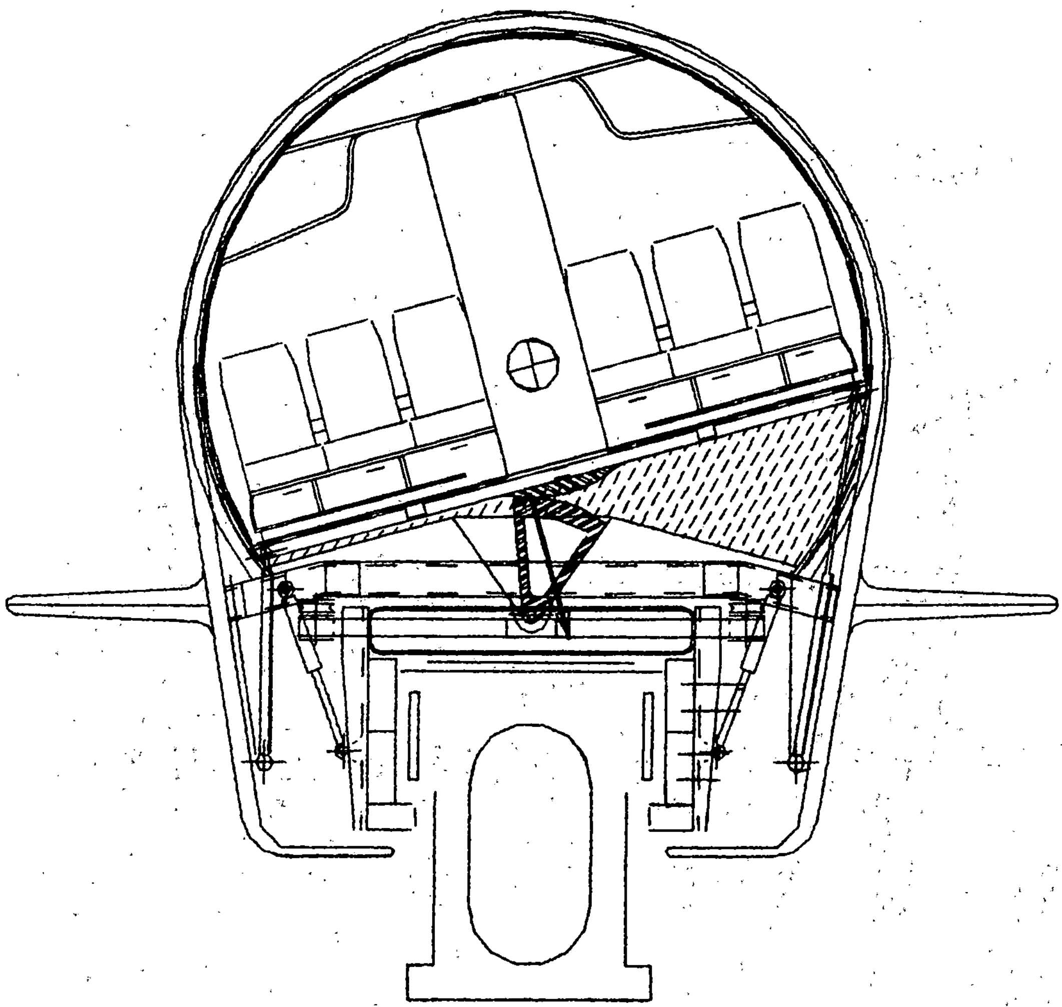


FIGURE 3-3. INTERNAL CABIN TILT SYSTEM

each end of the coach. The bearings are attached to the outer shell structure with a spider-web support. Underneath the floor, the structure is supported on rollers with rotation controlled by spur gears. Tilting force is supplied by hydraulic actuators on each side of the vehicle. The guideway may also be banked up to 15 degrees, so the total coach bank angle can be as great as 30 degrees to facilitate coordinated high-speed banked turns.

3.2.2 Safety Issues

The aluminum monocoque construction for the vehicle structure incorporates known and proven technology. There should be no significant safety issues related to the basic vehicle structure. Failure of the hydraulic actuating system or jamming of the tilting cabin due to collision damage or foreign objects can result in evacuation hazards due to misalignment of inner and outer doors that are discussed in Chapter 7 of this report. In addition, depending on the speed of the vehicle, standing passengers may fall down if a critical failure occurs while the train is negotiating a curve. A complete failure modes analysis is needed to identify failures that may result in the following unsafe conditions:

- Tilting system fails to return to the upright position after negotiating a curve (Category III hazard)
- Tilting mechanism fails such that the carbody tilts in the opposite direction prior to entering a curve (Category II hazard)
- Tilting mechanism fails to tilt (Category II hazard).

3.3 PROPULSION, NORMAL BRAKING, AND EMERGENCY BRAKING

3.3.1 System Description

The vehicle is propelled by a Linear Synchronous Motor (LSM). Utility substations are located at 20 to 30 km (12.4 to 18.6 mi) intervals along the guideway, normally near existing high voltage power transmission lines. At the substations, ac power is transformed and rectified to produce lower current dc which is fed to underground dc transmission lines running along the entire length of the guideway. Inverters spaced at about 4 km (2.5 mi) intervals tap the dc transmission lines and produce variable voltage, variable frequency ac power. This ac power is applied to the LSM windings on the guideway and creates a traveling magnetic wave that propels the vehicle. The guideway is divided into zones with at least one inverter station located near the center of each zone. A vehicle is propelled through a zone by independent six-phase inverters driving separate port and starboard motor windings. In the event of a failure in either the port or starboard motor systems, the other system can provide enough thrust to allow for full speed operation. Additionally, Bechtel states that the use of six phases allows considerable fault tolerance since a failure of any one phase will allow power in the remaining phases to provide continued operation until repairs can be made. The vehicle uses 12 separate independent SC magnet modules so that a failure in one or two modules will not produce a serious problem for vehicle propulsion, suspension, or guidance.

For safety and availability, a separate guideway is used for each direction of travel. However, the LSM is capable of moving vehicles equally well in either direction. In case of failure or blockage in one guideway lane, the opposite direction lane could be used for two-way travel.

Five separate braking systems are included in the baseline design vehicle concept. Two are the inherent aerodynamic and electromagnetic drag on the vehicle. The other three are system-controllable methods consisting of the normal regenerative braking system, a deployable aerodynamic speed brake system, and an emergency drag chute.

Regenerative braking, in combination with aerodynamic and magnetic drag, will be used for normal braking and all emergency stops up to deceleration levels of about 2.5 m/s^2 (8.2 ft/s^2). Battery backup is provided for the guideway inverters' control system, allowing regenerative braking even in the case of total system power failure. The baseline concept for most emergency stops is to allow the vehicle to coast to, and stop at a preferred stopping zone located at intervals along the guideway.

Aerodynamic speed brakes are provided which can add up to 0.2 g deceleration to the normal regenerative braking at high operating speed where braking is most critical. The Bechtel design is a deployable plug-type flat plate speed brake which is stored entirely inside the vehicle.

For extreme emergencies, a mortar-launched, ribbon-type drag chute is also provided which can add another 0.2 g deceleration at high speeds. Combined with normal and aerodynamic braking, the addition of a drag chute can bring total vehicle braking deceleration to over 0.6 g.

A parking brake is provided to keep a stationary vehicle stable. It functions by applying a clamping force between the bogies and the sides of the guideway beam.

3.3.2 Safety Issues

The Bechtel design approach provides considerable redundancy to assure a high degree of fault tolerance in the propulsion and regenerative braking system. The most likely cause of loss of propulsion power may be the utility power sources. For this reason, the self-contained on-board backup power system should be appropriately designed to assure that the vehicle can continue to a station or a safe stopping location.

None of the emergency braking devices proposed by Bechtel involves friction between the vehicle and the guideway beam. There is no design consideration given to the effect of the bogies inadvertently coming into contact with the beam. Considerable damage could occur if no skid pads or other provisions are incorporated.

Inadvertent deployment of the speedbrakes or drag chute would cause a sudden deceleration of up to 0.2 g depending on the amount of counteracting propulsion force present. Also, if the parachute deployed, the guideway would be obstructed until maintenance personnel detached the parachute. These braking devices must be designed to ensure such failures have a very small probability of occurring.

3.4 SUSPENSION, LEVITATION, AND LATERAL GUIDANCE

3.4.1 System Description

The Bechtel design uses "flux canceling" based on alternating the polarity of the vehicle SC magnets. Levitation forces are generated by the SC magnet fields interacting with a guideway beam side-mounted ladder conductor. Guidance forces are generated by these fields interacting with guideway-mounted null-flux loops. The levitation system also provides some guidance but Bechtel states it is more efficient to provide the majority of the guidance force by the separate null-flux loop system. Two coil system modules (cryostats), each with eight SC windings, are carried by each of the six bogies located along the length of the vehicle. There are 96 such windings on one vehicle.

Cryogenic cooling is provided by liquid helium which is circulated through a cable-in-conduit-conductor utilized by the magnets. A single helium inlet and outlet is used for each cryostat, and the winding conduits are connected to helium manifolds within each cryostat. The liquid helium is stored in a tank located in the bow, and is recycled once each day during stops at special stations located about every 400 km along the guideway. Since the helium is not vented, no helium is lost, and the recycled helium is cooled at wayside refrigeration plants. No on-board helium refrigeration system is used.

The magnets on the bogies, as illustrated in Figure 3-4, interact with ladder-like conductors on the guideway, providing primary suspension and some guidance forces. This concept can provide high efficiency with large magnetic fields in the vicinity of the guideway and negligible fields in the vehicle cabin because the field falls off rapidly with distance. This design has the ability to provide magnetic levitation and guidance down to very low speeds of about 9 m/s (20 mph). The system is totally passive so that, as long as the vehicle is above the takeoff speed, it is suspended and guided independent of the successful operation of any system power

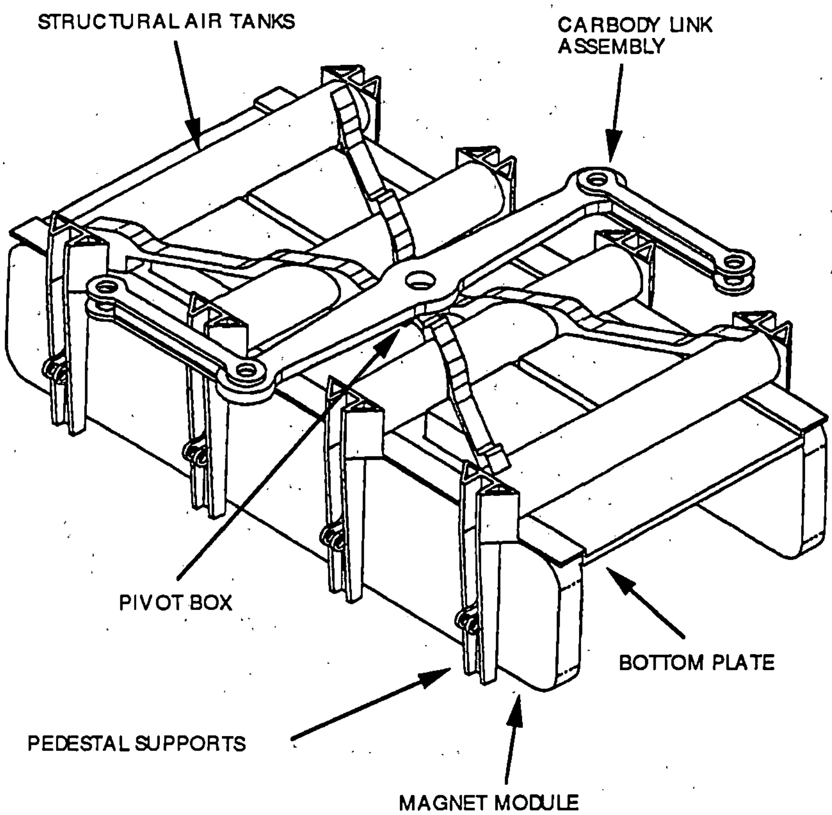


FIGURE 3-4. BOGIE STRUCTURE

source or active control system. At designated stopping places and at stations, special active coils in the guideway provide suspension and propulsion down to zero speed, so the vehicle will be able to stop without the use of wheels or skids. For emergency stops along the guideway, air bearings are incorporated in the bogies and provide suspension at speeds below 9 m/s (20 mph) down to zero speed as shown in Figure 3-5.

A hydraulically powered, actively controlled, secondary suspension transfers the forces from the bogies supporting the SC magnets to the vehicle body to reduce vibration in the vehicle caused by imperfections in the guideway. Additional control is provided by small winglets located at the bow and stern of the vehicle. These surfaces are actively controlled by the onboard hydraulic system to

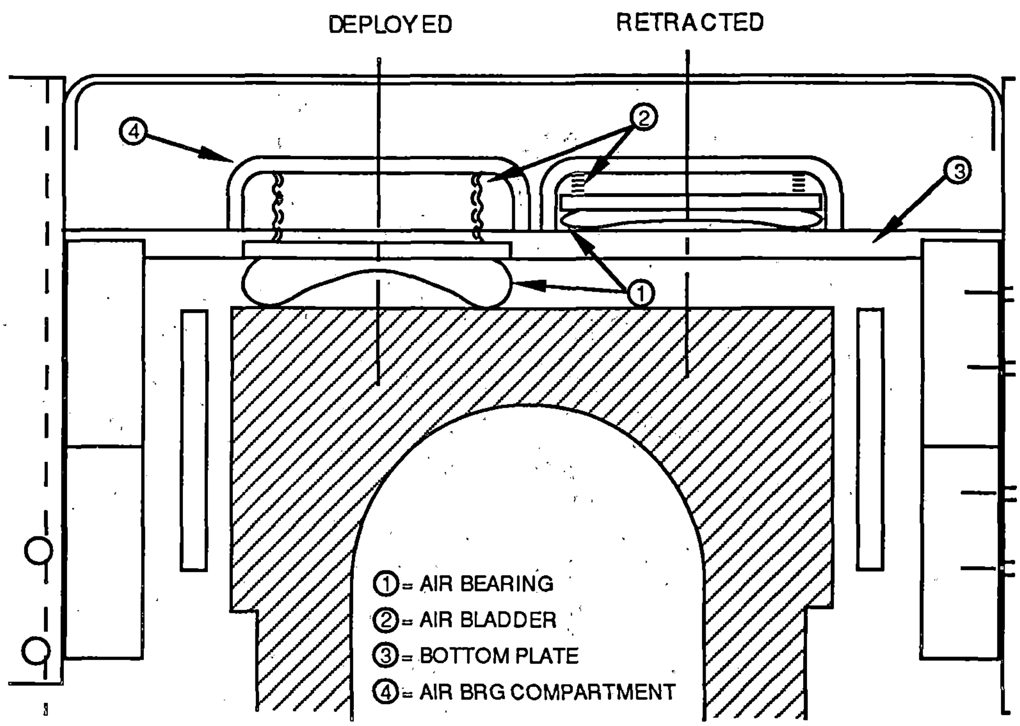


FIGURE 3-5. AIR BEARING IN BOGIE

provide additional improvements in ride quality with only a modest increase in aerodynamic drag. No aerodynamic controls are used for primary vehicle guidance. The direction and magnitude of secondary suspension forces is regulated by sensors on the vehicle. Bechtel states that this actively controlled secondary suspension system provides for an improved vehicle ride quality. The internal cabin tilt system described in Section 3.2.1 of this report is independent of the secondary suspension system.

According to Bechtel, the primary lateral guidance forces become ineffective at very slow speeds and when stopped. At low speeds, the vehicle uses the air bearings to achieve low friction between the beam and the vehicle, but the air bearings do not provide any guidance forces. Small wheels mounted in the parking brake assemblies are used to provide low speed lateral guidance.

3.4.2 Safety Issues

The premise of the Bechtel suspension concept is to never have contact between a moving vehicle bogie and the guideway beam. No landing wheels or friction pad skids are provided. The reliability and performance of the EDS and air-bearing system are critical to the success of the Bechtel concept. With no provisions for contact between vehicle and guideway, the extent of the damage that might occur, if such contact does occur at various speeds, has not been assessed. Bechtel considered this to be a Category II critical event in its Preliminary Hazard List.

Loss of the Bechtel vehicle passive electrodynamic primary suspension system can result from superconducting magnet quenching or from magnet winding/dewar component failure but not from failure of the on-board power supply system. The magnets are persistent current-mode operated and require only infrequent charging. Also, these superconducting magnets do not require on-board refrigeration power for their cryogenic cooling system because the magnet winding cryocooling is based on an on-board supply of helium to absorb the generated heat load.

Not having the cooling system on the vehicles simplifies and lightens the vehicles and is generally safer. However, the location of the liquid helium storage sphere in the forward compartment should be reviewed for hazards, such as effects of vapor leaks, and collision-caused rupture of the helium system. These could be Category I or II hazards because of the effect on passengers.

There are three physiological hazards associated with employing cryogenic materials. One is asphyxiation, referred to as cryogenic Oxygen Deficiency Hazard (ODH), caused by allowing the temperature of the cryogenic fluid to rise in a confined space. The oxygen in the space would then be displaced by the cryogenic material due to thermal expansion. This is potentially a Category I hazard and an annunciation of this failure condition should be provided so that an emergency evacuation can be initiated. Two other physiological hazards associated with cryogenic helium gas are "cold burns" and possible lung damage caused by gas clouds. Such clouds are known to be highly dangerous prior to dispersal.

Materials embrittlement is potentially a Category II hazard that may be caused by cryogenic systems. The selection of materials is critical in properly designing the installation of an on-board cryogenic system. Materials surrounding the cryogenic system will be exposed to extremely low temperatures which may result in embrittlement. Therefore, a systematic approach, similar to a zonal analysis, should be taken to ensure that materials that may come into contact with the system are compatible.

3.5 ON-BOARD POWER SYSTEMS

3.5.1 System Description

On-board electrical power is provided by a redundant pair of methanol-powered fuel cells. Two separate circuits (port and starboard) are used, each powered by one of the fuel cells. Figure 3-6 shows a schematic of the electrical power system. The system is sized to provide enough power to operate the heating, ventilating and air-conditioning equipment, the hydraulic actuators, the on-board computer, and vehicle lighting. A crossover device allows both circuits and their loads to be served, at reduced capacity, if one fuel cell fails.

Additionally, Bechtel states that half capacity operation of all subsystems is possible from one circuit because all electrically-powered subsystems are dual. There are also two nickel-cadmium battery banks that can provide peak power and emergency power for up to one hour in the event of failure of both fuel cells.

An on-board hydraulic power system is required to operate the vertical and lateral bogie dampers, the winglets, the parking

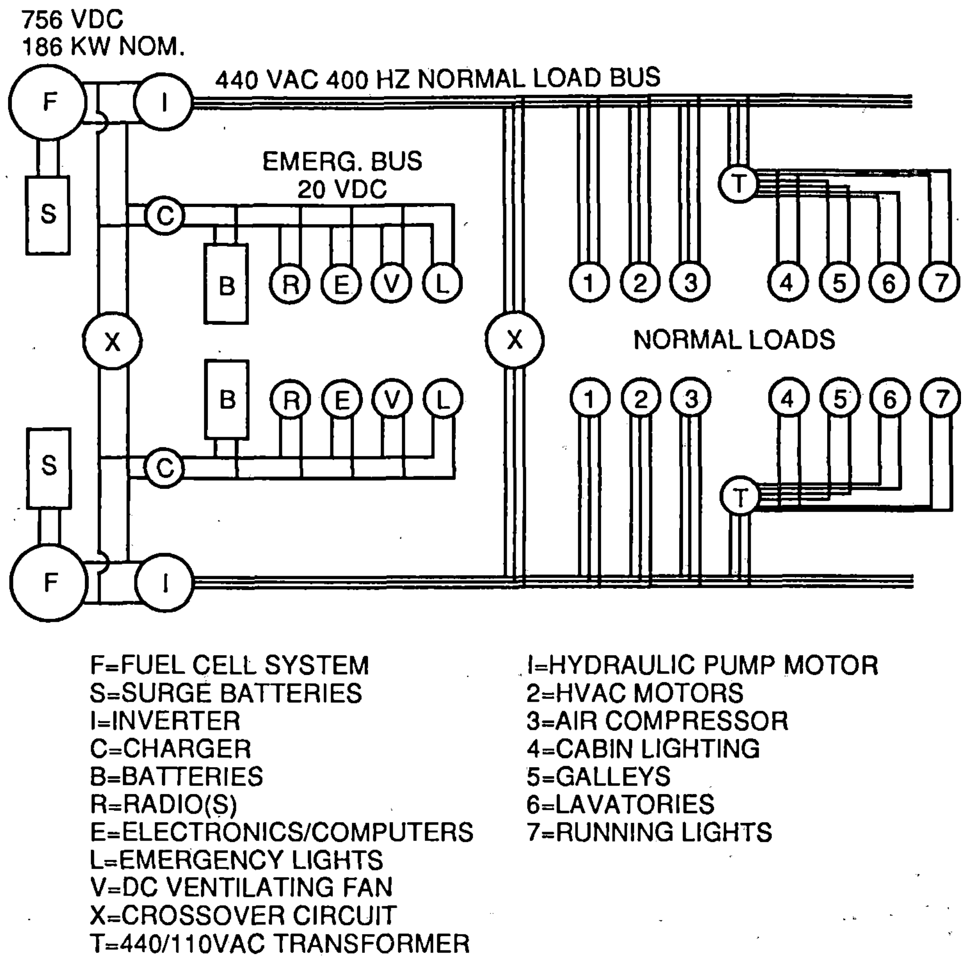


FIGURE 3-6. ELECTRICAL SYSTEM SCHEMATIC

brake/lateral wheel sets on each bogie, and the passenger compartment tilt actuators. All of these actuators derive their hydraulic power from lines supplied by two motor/pump sets located in the forward compartment. Figure 3-7 shows a schematic diagram of the hydraulic system.

An on-board compressed air system is required to supply the air bearings which provide emergency low speed lift for the vehicle. Toilets and galleys also require small amounts of compressed air intermittently. The system consists of two motor-driven air compressors, one at each end of the vehicle, supplying compressed air to four air tanks built into each bogie. Figure 3-8 shows a schematic diagram of the compressed air system.

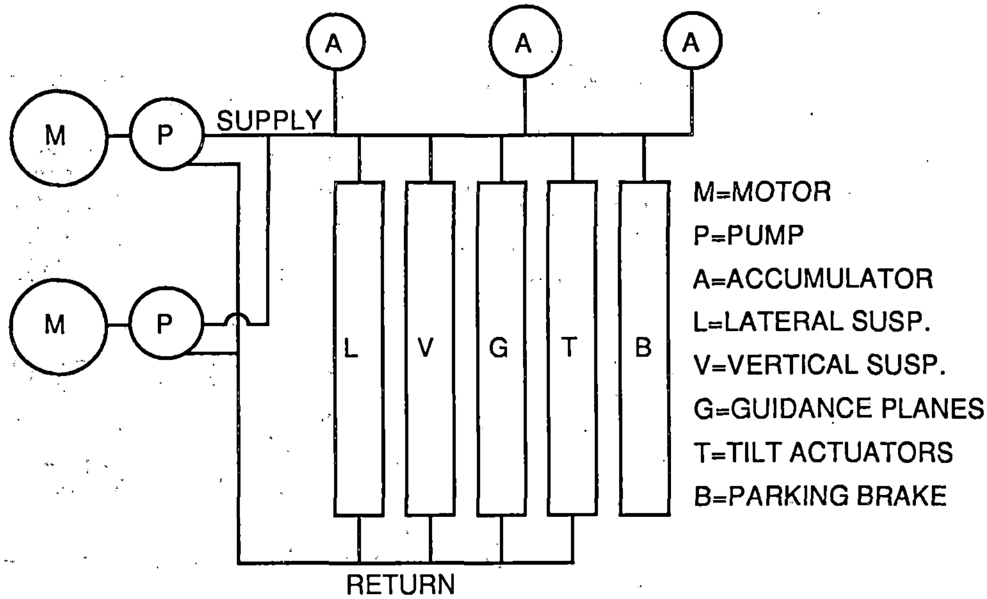


FIGURE 3-7. HYDRAULIC SYSTEM SCHEMATIC

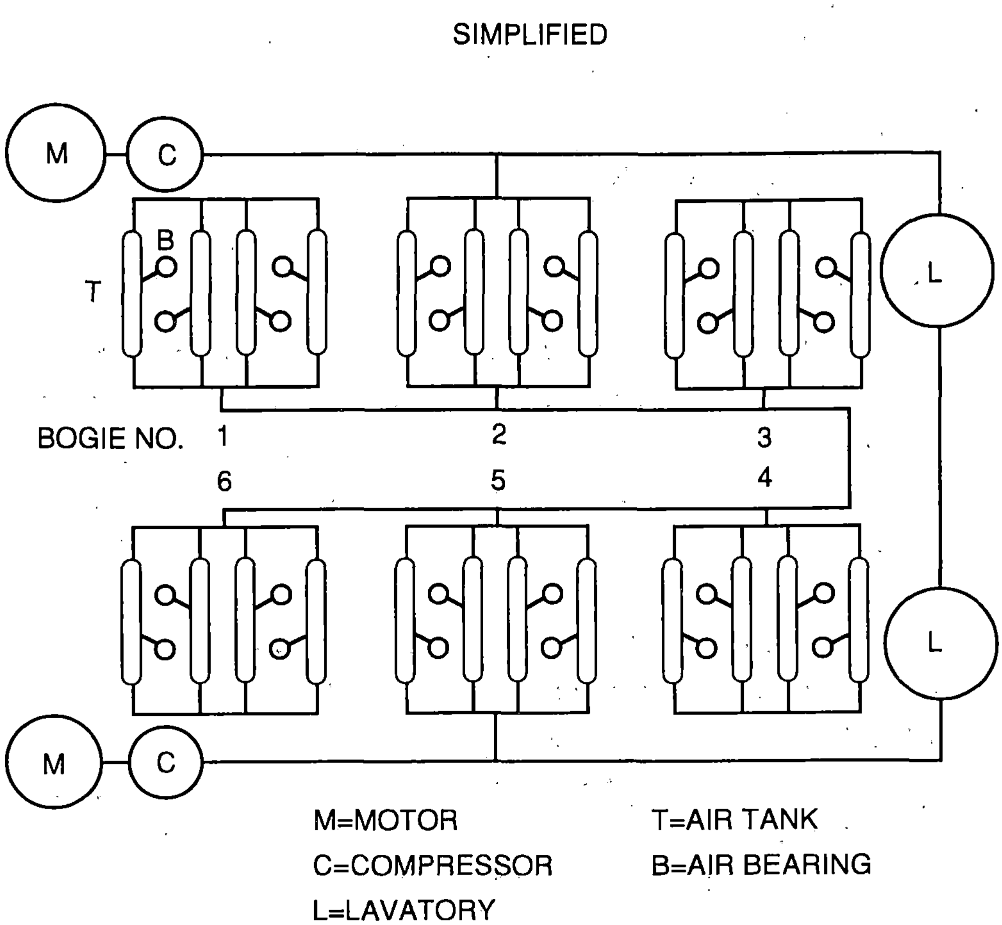


FIGURE 3-8. AIR SYSTEM SCHEMATIC

3.5.2 Safety Issues

Normal suspension, guidance, and propulsion all depend on a set of independent SC magnets on the vehicle. These coils are operated in the persistent current mode and are designed to operate for many minutes without any external power input. Therefore, Bechtel states that total loss of onboard power should not cause immediate loss of suspension and guidance.

Bechtel considered a number of methods for providing on-board electrical power, and chose methanol fuel cells for the baseline design. Bechtel's proposed use of methanol-powered fuel cells introduces unique hazards. Fuel cells are a relatively new technology and have not been in widespread use for ground transportation applications.

Methanol fuel cells utilize a reformer unit to convert methanol into hydrogen, carbon dioxide and carbon monoxide. Reformer units have associated hazards that arise from the high operating temperatures and the emissions of carbon dioxide and carbon monoxide. Fuel cell equipment operates at extremely high temperatures (180 to 200° C [356 to 392° F]), and care must be taken to ensure isolation of the equipment from the passenger and operator compartments. The end products of the reformer, the hydrogen, carbon dioxide and carbon monoxide gases, must also be kept out of the passenger and personnel areas.

Methanol is extremely toxic and must be safely separated from passenger and operator cabins. Additionally, unadulterated methanol burns invisibly, thus delaying response time if the fire is undetected for some period. The methanol used in automobiles and other vehicles is adulterated with a contaminant to create a visible flame, so the use of methanol in the maglev project would require a similar treatment. Bechtel has recognized that special design and operational precautions will be necessary to address the fire hazard problem; however, the SCD does not address the other hazards.

3.6 MAGNETIC SHIELDING

3.6.1 System Description

The Bechtel "flux canceling EDS" concept should concentrate the dc magnetic fields towards the vicinity of the guideway, causing the fields to attenuate rapidly with distance from the source. Bechtel has stated that this design allows a number of relatively low-cost mitigation options to be used to reduce the dc magnetic fields in the vehicle to one gauss or less. However, no specific approach was proposed in the SCD because Bechtel states that the extent of the hazard to humans, if any, has not yet been determined.

Bechtel does indicate, however, that there does not appear to be a cost effective way to avoid having the fields interact with ferromagnetic material within guideway girders. Bechtel's position is that steel girders cannot be used at all, except as part of a more complex structure. Even concrete girders must be carefully designed to avoid unacceptable magnetic interaction with the steel reinforcing. The concern is that the moving vehicle can induce currents in electrical conductors on the guideway, and these currents will produce power dissipation and forces on the guideway.

3.6.2 Safety Issues

Although a universal safe level for passenger exposure to dc fields has not been determined, the SCD SOW set goals of 50 gauss, 5 gauss, and 1 gauss levels to be studied with respect to cost and potential mitigating measures. As defined by Bechtel, the design and location of the windings are such that electromagnetic fields in the vehicle cabin should be negligible without shielding. Shielding can be added if necessary, but Bechtel's view is that such protection will not be needed to achieve levels allowed by current EPA rules. However, Bechtel's analysis did not consider effects on personnel in the vicinity of the guideway or in stations or maintenance yards. Further examination of these areas should be done as the design progresses.

3.7 FIRE PROTECTION

3.7.1 System Description

The Bechtel approach to fire detection and extinguishment requirements is to apply concepts similar to those used on most passenger aircraft. Bechtel proposes the use of fixed systems for detecting and extinguishing fires in non-cabin areas, and portable systems for extinguishing fires in cabin areas. Bechtel did consider the relative flammability of fuels when determining that methanol would be used for the on-board fuel cells. The locations of the fuel cells and ancillary equipment were also selected to provide some degree of protection from collision damage that could result in a fire.

3.7.2 Safety Issues

Although Bechtel states the potential for collision damage was considered in choosing the fuel cell location, the selected location in the most forward part of the vehicle appears to be quite vulnerable to damage from major guideway obstructions. Further, if a fire occurs in the forward compartment of a maglev vehicle traveling at high speed, the natural draft on the fire may encourage its spread in the direction of the cabin. Further study should be conducted to determine whether restrictions are needed for locations of fuel cells on maglev vehicles.

Most of the information provided by Bechtel dealt with fire detection and suppression methods. More consideration should be given to prevention, such as materials selection, control of ignition and fuel sources, and operating policies and procedures. Although Bechtel considered fire in a passenger station in its PHL, no significant design discussion on stations is provided in the SCD.

Methods for monitoring and detecting fires in isolated, unstaffed wayside locations are discussed, but no information on suppression methods for such fires is provided. Automatic fire suppression techniques usable in these wayside locations should be evaluated.

3.8 GUIDEWAY DESIGN

3.8.1 System Description

The guideway structure consists of box-beam reinforced concrete girders, transverse support frames, columns and foundations as shown in Figure 3-9. The guideway propulsion/levitation/guidance system components are mounted on both sides of the upper girder section. The vehicle straddles the guideway girder and its bogie-mounted magnets interact with the girder-mounted equipment providing propulsion, levitation, and guidance.

On curved track, the girders are banked up to 15 degrees. A vehicle stopped on a curved track section would expose passengers to a substantial lateral force and impair evacuation of elderly and/or physically challenged passengers. However, as discussed in Section 3.2, the vehicle cabin floor can be rotated 15 degrees in either direction. This feature provides for a level cabin if stopped on a banked guideway section, but may also impair evacuation because of door misalignment.

The girder is a hollow, reinforced concrete box-beam design. The upper half of the girder section is exposed to magnetic fields generated by the vehicle magnets. This necessitates the use of fiberglass-reinforced-plastic (FRP) reinforcement in this part of the girder section. Steel reinforcement is used in the lower girder section.

The suspension, guidance, and propulsion systems require substantial amounts of aluminum and copper conductors mounted on the guideway girders. Propulsion and braking are provided by two six-phase cable windings on either side of the girder. The guidance system consists of aluminum coils supported within FRP

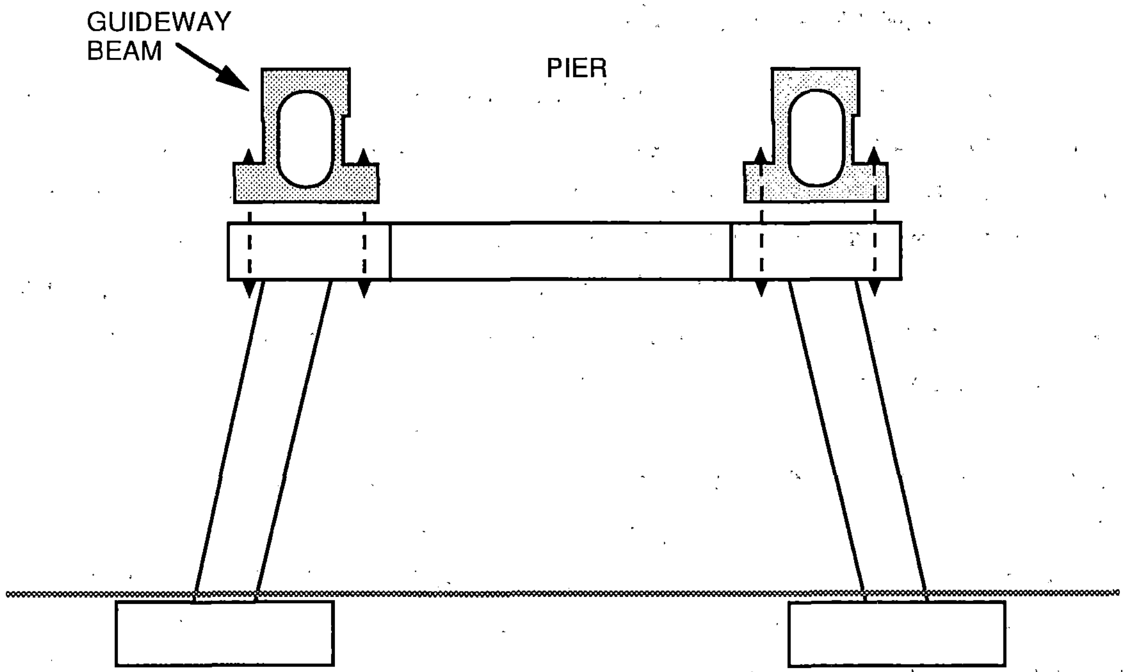


FIGURE 3-9. GUIDEWAY CROSS-SECTION

frames attached to the girder. The levitation ladder is fabricated from aluminum alloy.

3.8.2 Safety Issues

The box-beam monorail design of the guideway provides limited vehicle "wrap around" of the guideway. Gravity and the magnetic levitation and guidance system are the only forces preventing the vehicle from departing the guideway. The safety certification of this design will require substantial analysis and testing of the levitation and guidance system to assure that a vehicle departing the guideway is an extremely improbable event under all foreseeable conditions.

Structural failures or guideway movement will be detected by fiber optic and standard strain gauges. These are discussed in Section 3.10.

3.9 GUIDEWAY SWITCH

3.9.1 System Description

The Bechtel baseline switching concept is based on a flexible switch beam as shown in Figure 3-10. A flexible beam is laterally deformed to line up with a turnout section of the guideway. The existing systems have generally been constructed of high strength aluminum, but because of the presence of strong magnetic fields in the upper area of the maglev guideway girder, FRP materials have been applied in the Bechtel concept.

In maintenance yards and cross-over structures where speeds of less than 11 m/s (25 mph) are required, Bechtel states that standard guideway girders can be used by forming a polygon in the switching section. The vehicle has the capability to negotiate angular changes of about three degrees.

3.9.2 Safety Issues

Bechtel's switch concept has been successfully used for several decades on operating monorail systems in Japan. The primary difference in this application has to do with the higher operating speeds of the vehicles. The switch operating speed and the allowable vehicle speed through a switch may become factors in establishing safe headways.

3.10 GUIDEWAY MONITORING

3.10.1 System Description

The Bechtel design incorporates an extensive set of guideway sensors as illustrated in Figure 3-11. The functions of the sensors are to monitor and detect the following:

- Guideway movement and alignment
- Locations of vehicles on the guideway
- Size and location of foreign objects on the guideway

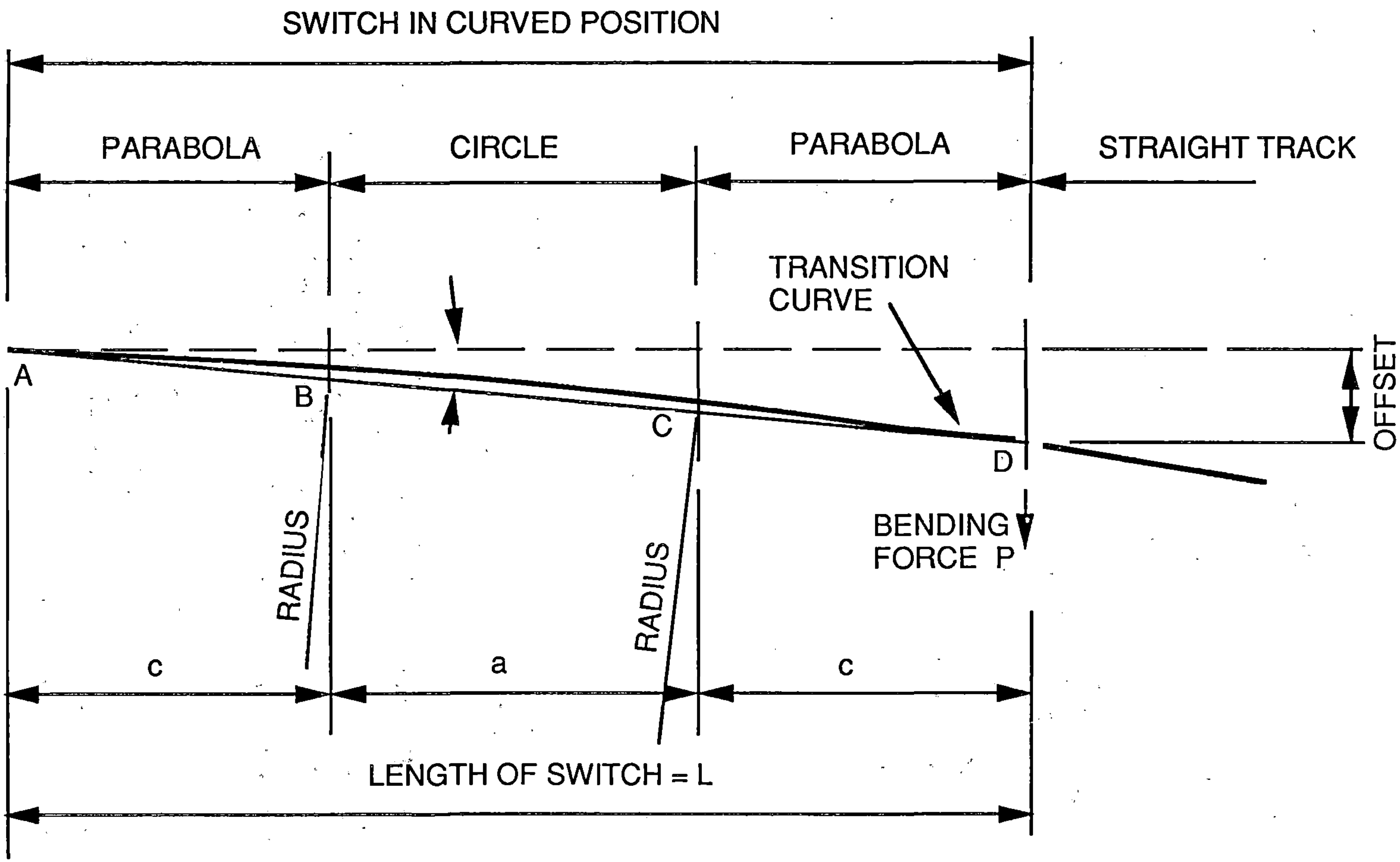


FIGURE 3-10. BASELINE SWITCHING CONCEPT

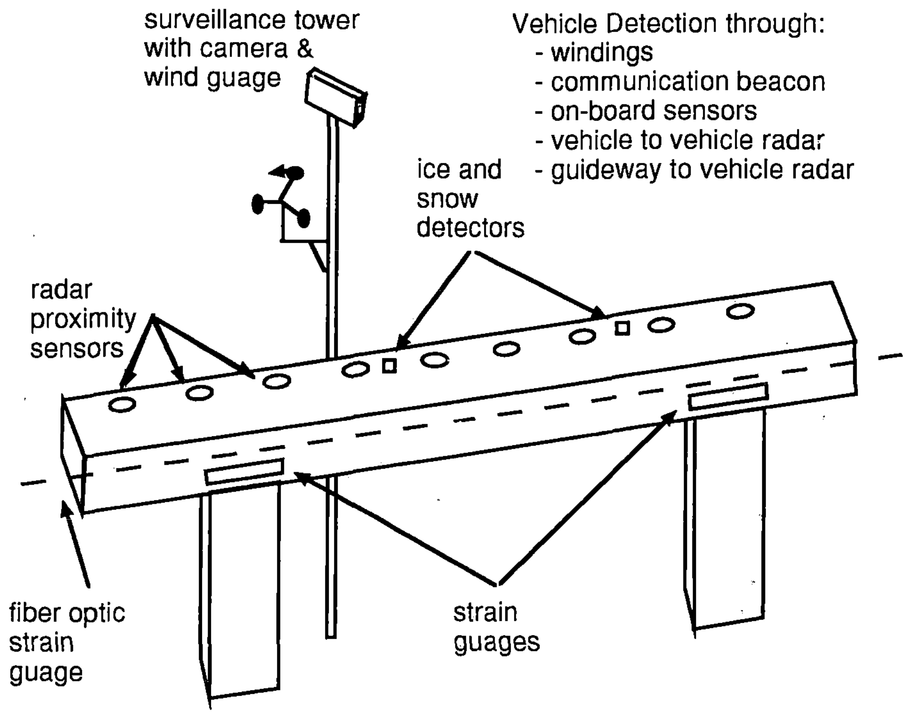


FIGURE 3-11. GUIDEWAY SENSORS

- Amount of snow and ice accumulation
- Magnitude of wind velocity.

The general Bechtel philosophy for reaction to sensor warnings is to automatically stop any vehicles which could be in danger. Only after a visual inspection is made and the guideway declared safe, would movement of the vehicles be allowed to resume.

Bechtel states that guideway movement (e.g., due to an earthquake or the guideway structure being struck during a traffic accident) is detected by fiber optic and standard strain gauges. The fiber optic gauge is embedded in the FRP reinforcement bars of the guideway beam. The fiber optic light path will become distorted if the reinforcement bar experiences excessive strain. Standard strain gauges are mounted across guideway beam junctions. Any movement of either beam will be detected by these strain gauges.

Radar proximity detectors are mounted along the guideway beams to detect any intrusion onto the guideway. These detectors operate on the principle that the volume surrounding the guideway should normally be static except for the passage of scheduled maglev vehicles. Whenever the radar detects a disturbance of sufficient magnitude to indicate the intrusion of a hazardous object, vehicle movement is halted until the guideway is inspected. The inspection would normally be conducted by central control operators using the television surveillance system. The surveillance cameras are located at intervals such that the entire guideway can be observed.

Bechtel plans to use snow and ice detectors where necessary, but no specific design has been proposed at this time.

The presence of another vehicle in close proximity is detected by several methods which cross-check each other. The primary means of locating vehicles is the guideway propulsion equipment that tracks the movement of each vehicle through the LSM windings. This method is accurate to within a few centimeters and is needed for the phase control of the motor. Sensors located onboard the vehicle are able to use the same method to determine its own position. Periodic updates of vehicle position are provided, both to the guideway and to the vehicle, each time a communications beacon is passed. Finally, radar-ranging sensors are used both by the vehicle, to detect other vehicles in line of sight, and by the guideway to detect the location of a vehicle as it approaches the station berthing sites.

3.10.2 Safety Issues

Monitoring and assuring that the guideway is both sound and clear are vital to the safe operation of a high speed maglev system. Bechtel has provided a variety of methods to monitor conditions, but, since no evasive maneuver is possible, the key to safety is the ability to stop a vehicle short of a detected hazard. Bechtel has recognized this in the SCD. Further study of the lead time required for identifying hazards, operating procedures, automation required, etc. is needed to assure safety without generating a large number of nuisance service interruptions.

3.11 POWER SYSTEM AND DISTRIBUTION

3.11.1 System Description

Utility power substations are located at approximately 20 to 30 km (12.4 to 18.6 mi) intervals, normally in the vicinity of existing high voltage power transmission lines. At the substations, ac power is transformed and rectified to produce lower voltage (about 30 kV) dc which is fed to underground dc transmission lines running along the entire length of the guideway. Inverters spaced at about 4 km (2.5 mi) intervals tap this dc transmission line and produce variable voltage, variable frequency ac power for exciting the LSM guideway windings.

Fault tolerance is provided within each inverter and in each utility power substation to allow normal or reduced speed operation during the repair of a failed component. The multiple-feed guideway power distribution provides substantial fault tolerance because an outage on one transmission line can be compensated for by power from adjacent substations.

In the event of total power loss from the utilities, Bechtel states that all vehicles would be regeneratively braked simultaneously using resistor banks located near each substation to dissipate the regenerated energy. The inverter controllers are equipped with standby power that can provide control power in the event of normal power system failure. The control system would attempt to stop each vehicle at a passenger station or in a preferred stopping area on the guideway. Bechtel states that each passenger station will have an emergency battery backup power source that can provide enough power to propel a vehicle that has stopped near the station the remaining distance to the station.

3.11.2 Safety Issues

The Bechtel power distribution concept is quite fault tolerant and contains several innovative features that should enhance safety. The dc distribution cables are installed underground which should provide greater reliability and protection from severe weather. The multiple power feed for the guideway distribution prevents a power interruption at any one substation from halting operation. Battery backup is provided for all control electronics so the inverters can operate to brake the vehicle when there is a power failure.

3.12 COMMUNICATIONS, COMMAND, AND CONTROL

3.12.1 System Description

Vehicle control is fully automated and has three spatially distributed hierarchical levels: onboard vehicle computer system, wayside zone control computer system, and a Central Control Facility (CCF). Data is acquired, transmitted, and processed at all three levels. Figure 3-12 illustrates the Bechtel maglev control concept.

A zone is a physically distinct section of guideway. The zone controller is located in an unmanned facility near the center of a zone. It controls vehicles traversing the zone by controlling the inverters and dynamic braking. The zone controller also gathers and maintains current data about the guideway in its zone, and transmits vehicle position, velocity, and power information to higher level controllers. Higher level controllers are responsible for safe operation of the entire guideway system, but the zone control acts autonomously to provide protection and to mitigate the effect of failures that occur at higher levels. All wayside controllers communicate with each other through a fault tolerant network of fiber optic cables installed in the guideway. Each vehicle contains a number of systems that require on-board control. These include such functions as power, braking, suspension, doors, etc. which are discussed in other sections of

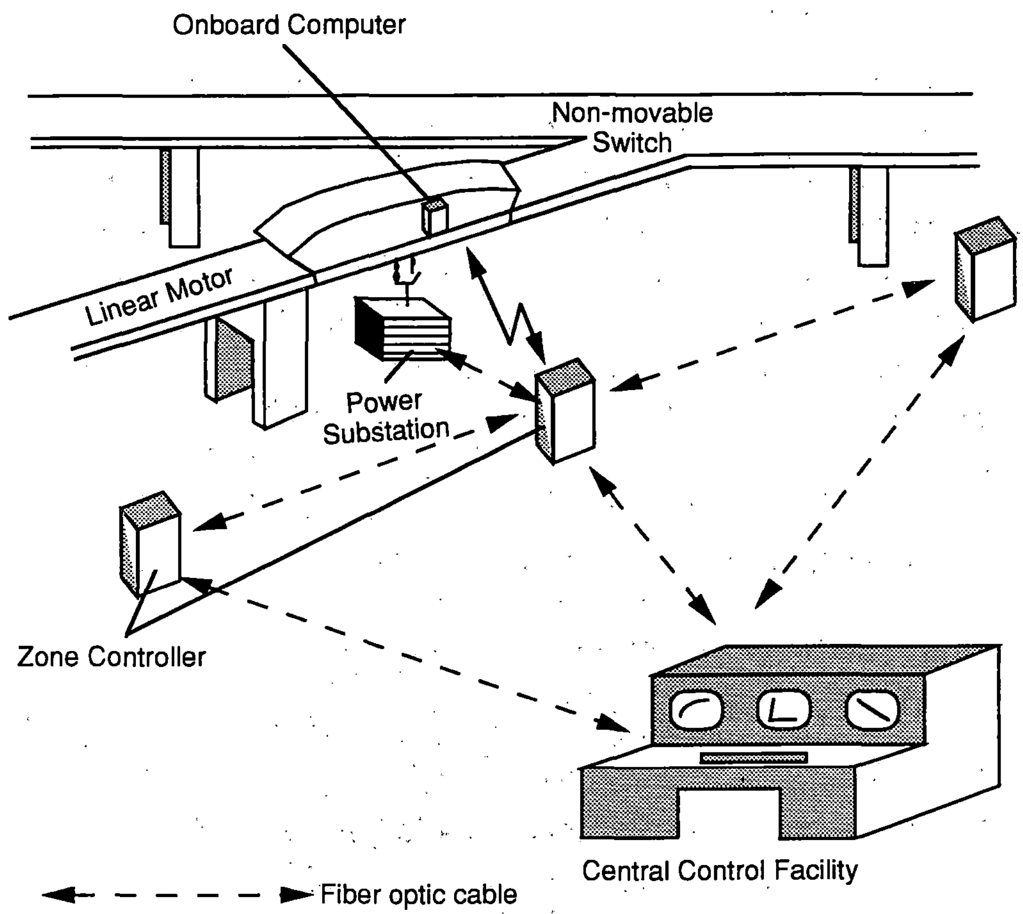


FIGURE 3-12. OPERATION CONTROL SYSTEM ELEMENTS

this report. The vehicles also have sensors that determine their precise position, and these data are provided to the wayside controllers as a backup source of vehicle position and velocity information. The vehicles use radio links to communicate with the zone and station controllers.

Every utility power substation has a controller for monitoring and providing protection for the transformers, rectifiers, and dc distribution system. Protection is provided by circuit breakers on the primary side of the high voltage transformers. These allow total isolation of the guideway from the power grid.

Each passenger station has a control system that monitors neighboring zone controllers and directs the docking and dispatching of vehicles. The stations are the lowest level of off-vehicle control that is manned at all times. The personnel are trained to deal with common types of control problems, operate rescue vehicles, and effect minor repairs.

The CCF is the highest level of control. A single CCF can manage all traffic in corridors up to a few hundred kilometers long. Bechtel states that the CCF computer will have a high level of fault tolerance, and the facility will be manned 24 hours-per-day with personnel who can make repairs as needed.

Global level control of the zones and vehicles will be exercised from the CCF. However, if a station detects that the CCF is not operational, the stations will assume responsibility for controlling the zones and vehicles. In the event of multiple failures involving the CCF and one or more stations, individual zone controllers, working with adjacent zone controllers, will still be able to move vehicles from station to station, but at a reduced frequency.

3.12.2 Safety Issues

The reliability requirements of systems whose failures could result in the loss of human life are very demanding, and such failure conditions must be extremely improbable. Bechtel has provided an extensive discussion of the design approach used to develop control and communication hardware architecture. The approach is based on what Bechtel refers to as a fault tolerant parallel processor (FTPP).

Bechtel recognizes that exhaustive failure modes and effects-type analyses of digital computers are not feasible due to the extremely large number of possible failure modes and combinations that must be analyzed. The maglev control computer is such a device, and its failure modes cannot be exhaustively enumerated. Therefore, to achieve correct outputs from the maglev computing platform with acceptably high probability, the platform must be designed to tolerate arbitrary failure behavior. Bechtel refers to this form of fault tolerance as Byzantine Resilience, a term which comes from a fault tolerance theory that drew an analogy between computer network communication and communication among generals in the Byzantine Army while laying siege to an enemy city. It is a set of mathematically determined rules for establishing an architecture that is capable of functioning correctly in the presence of a specified number of faults. Bechtel applies this logic to the maglev control computers and communication network designs.

While the philosophy of FTPP design and Byzantine Resilience appears sound for hardware, it may not resolve the issues of common-cause multiple fiber optic breaks and common-mode software errors that can defeat the hardware fault tolerant redundancy schemes. Bechtel does not address its approach to achieving the required safety levels in software as is done for hardware. Further study of methods for assuring software integrity should be conducted, and requirements for developing and controlling safety-critical software should be defined early in the system development.

3.13 SYSTEM OPERATIONS AND MAINTENANCE ISSUES

3.13.1 System Description

Bechtel has considered the three possible limits to headway: a headway distance minimum due to linear motor zone length; a headway time minimum due to control-related issues such as switching; and a safety limit determined by the ability to stop in the clear distance ahead. Bechtel states that its design is based on the ability to handle 100 vehicles-per-hour at an average speed of 125 m/s (280 mph), and 90 vehicles-per-hour at average speeds from 100 to 135 m/s (224 to 302 mph). For the Bechtel baseline design, the 100 vehicle-per-hour limit requires a minimum headway time of 36 seconds, while the 90 vehicle-per-hour limit requires a minimum of 40 seconds.

At low speeds, the minimum headway distance is controlled by the inverter spacing along the guideway because each inverter can propel only one vehicle at a time. Thus, to allow a vehicle headway of 40 seconds at an average speed of 100 m/s (224 mph), the inverter spacing must be no more than 4 km (2.5 mi). This is the nominal spacing used in the Bechtel baseline, but it is reduced in regions where an average speed of 100 m/s is not possible, such as in tight curves or steep grades.

At the highest speeds, the minimum headway is imposed by safety considerations. Bechtel states that it is necessary to apply either a maximum deceleration value or a maximum stopping distance to establish the required safety-related headway for any vehicle speed. For example, using a 2 m/s^2 (6.6 ft/s^2) deceleration limit and a 2-second reaction time, the required stopping distance varies from 5 km (3.1 mi) at 150 m/s (337 mph) to 2 km (1.2 mi) at 75 m/s (168 mph).

Using the 36-second headway and 100 vehicle-per-hour limit, the baseline 106-passenger vehicles provide a theoretical capacity of over 10,000 people-per-hour. Allowing for statistical variations in headway and switching speed limits, this capacity will be somewhat less. Bechtel is proposing a conservative initial minimum headway of 60 seconds. Reductions will be allowed only after operational experience indicates shorter headway is safe. Considering statistical variations and extra headway requirements for switching, Bechtel calculated a practical limit of about 45 vehicles-per-hour can be sustained with the nominal 60-second minimum headway. This equates to 4770 passengers-per-hour in 106-passenger vehicles.

3.13.2 Safety Issues

Bechtel has generally applied conservative factors in calculations for safe headways. The desired headway is maintained by monitoring vehicle position and adjusting speeds as required to control relative speeds and distances between vehicles. Collision avoidance is achieved through the proper operation of the control systems, braking systems, monitoring systems, etc. which are discussed in other sections.

3.14 ENVIRONMENTAL EFFECTS

3.14.1 Environmental Considerations

Routes that are primary candidates for maglev systems in the United States provide a broad range of environmental and climatic conditions. These include high and low temperatures, wind, rain, snow, ice, earthquakes, fog, lighting, dust, and sand. Operational safety can be significantly degraded depending on the severity of the conditions. Bechtel uses sensors to evaluate these conditions and relays the appropriate data both to the zone controllers and the vehicles. For each condition, a look-ahead distance from 30 to 100 miles is used. Figure 3-11 illustrates the guideway sensors proposed by Bechtel. They are discussed in Section 3.10 of this report.

The general Bechtel philosophy for reaction to sensor warnings is to automatically stop any vehicles which could be in danger. Movement would be allowed to start again only when the hazardous condition has been eliminated.

Snow, ice, and accumulations of other forms of guideway debris can hinder operation if they are too large for the vehicle to pass over without impact, or if they alter the magnetic fields substantially. Plow-type devices commonly used on the front of lower speed trains are not feasible for the high speed maglev train. Fortunately, the Bechtel guideway consists for the most part of an isolated, elevated structure with little horizontal surface to accumulate debris. In addition, normal prevailing winds will, in many cases, blow most lightweight material from the track before it accumulates. The potential hazard comes from material that either accumulates rapidly or is of such size and weight that it will not be blown away and is not easily passed over or dispersed by the vehicle. Bechtel proposes to have a fleet of dedicated service vehicles that will run the full length of the system daily (in segments between stations) to clear the guideway of any accumulated material before full operations can begin.

Extreme high winds or gusts could potentially de-stabilize the vehicle or possibly cause contact between the vehicle and guideway beam, a Category II hazard. Bechtel has taken wind force loads into account in the design of the magnetic forces produced to levitate and guide the vehicle along the beam. Thus, Bechtel states that no special precautions are needed to handle high side wind forces when the vehicle is levitated by magnetic forces. In some very severe conditions, reduced speed may be necessary for ride quality. The lateral-wheel parking brake system is used when the vehicle is stationary to prevent vehicle rocking due to wind or other disturbances.

Lightning and static charges can be guarded against using the same methods. While there is no danger of electrical shock to passengers from lightning for the same reasons airplane passengers are not at risk, Bechtel states that there is a high probability of damage to the propulsion and levitation subsystems. The closest structures to the vehicle are the propulsion coils, the levitation ladder, and the nonmetallic cover over them. Lightning will usually travel the easiest path to ground after striking the outer vehicle shell. The lightning will most likely arc over from the SC magnet module to the propulsion coils and/or the levitation ladder. Considerable damage can occur if this is allowed to occur. To prevent such arcing, the vehicle frame structure is cabled to a flying beryllium wire hung from the bottom surface of the bogie. The flying wire drags lightly along a cadmium-plated copper strip attached to the top of the guideway beam.

3.14.2 <u>Safety Issues</u>

The box-beam monorail design of the girder supporting the vehicle does not provide any protection from crosswinds acting on the vehicle. Bechtel has considered these loads in determining required magnet forces; however, Bechtel efforts to lighten the vehicle weight have caused the center of gravity to become higher than that used in the baseline calculations. Therefore, revised calculations may be necessary to re-evaluate the required magnet forces and ensure protection from cross-winds.

The vehicle grounding scheme using the flying wire should be evaluated for the effect on its functioning of various thicknesses of ice on the copper strip on the beam.

The sensor systems that have the authority to cause the vehicle to automatically stop must be designed to have a very low probability of false alarm. Frequent unnecessary disruptions to normal operations are themselves safety hazards.

3.15 SUMMARY OF FINDINGS - BECHTEL

The Bechtel stated approach to safety during system concept definition is consistent with the philosophy of MIL-STD-882. However, the documentation provided in the Bechtel SCD report is too limited to assess how thoroughly the approach was actually applied to the baseline design that evolved, and whether that baseline can meet Bechtel's self-imposed probability criteria. Bechtel states that the probability of a mishap resulting from a hazard will not be allowed to exceed the allowed probability assigned to the hazard's level of severity. Probabilities are assigned to each level with no discussion of their source of derivation, although they are in the same general range as those applied in the commercial airplane industry. There are no data or analyses provided to indicate whether the baseline design can meet the safety criteria established for each hazard.

The Bechtel approach recognizes the key distinction (yet connection) between reliability and safety. However, with the exception of air bearings, the SCD text does not explicitly identify reliability items which are related to safety issues.

Bechtel's approach to the design safety effort implemented during the SCD phase consisted of identifying potential hazards through means of a Preliminary Hazard List (PHL), and developing system design approaches to eliminate or mitigate the hazards.

The Bechtel PHL can be considered appropriate for the SCD phase of maglev system development. Bechtel addressed 25 hazards that include those specified in the SCD SOW. However, several safety-related issues remain. These issues are reviewed in previous sections and are summarized below.

The Bechtel approach to levitation, guidance, and braking does not involve any in-motion contact between vehicle and guideway using wheels, air bearings, or skids. No provision has been made for inadvertent contact due to system faults or environmental conditions. Contact at high speeds is identified as a Category II event by Bechtel and could result in significant damage to the vehicle or guideway. This damage level and its consequences have not been addressed, although Bechtel has stated that it is a probable event.

The probability of superconducting magnet quenching can be made extremely low by appropriate magnet design practice such as that applied by the Bechtel SCD baseline magnet design. The design uses a winding current density of only 24% of the critical current so as to provide an operational quenching margin of four. Also, 96 separate superconducting magnet windings are used, contained within 12 separate dewar modules, providing a high degree of operational redundancy. Nevertheless, cable-in-conduit style superconductors have never been used in a transportation environment, and have seen only limited application in only very large-scale magnets. Detailed FMECA-type analysis of the possible failure modes is required during the design phase to determine whether a safety lockup function is required for the levitation system.

Liquid helium and methanol fuel are stored in the nose section of the vehicle. Bechtel states that collision damage and fire were considered in the location selection, but further study should be conducted to determine the safest location for hazardous materials carried aboard the vehicle.

The box-beam monorail guideway design provides limited vehicle "wrap around" of the guideway. Gravity and the magnetic levitation and guidance system are the only forces preventing the vehicle from departing the guideway; this is a Category I event and must be extremely improbable. Feasibility studies of locking flange design concepts should be considered.

Bechtel provides aerodynamic speed brakes and a drag chute for emergency braking. The effect of inadvertent deployment of these devices on vehicle stability and control should be evaluated.

The Bechtel philosophy for responding to guideway and vehicle sensor warnings is to automatically stop any vehicles which could be in danger. The sensor systems that have the authority to cause the vehicles to stop must be designed to have a very low probability of false alarms. Frequent unnecessary disruptions to normal operations are themselves safety hazards.

Bechtel has provided an extensive discussion of the hardware architecture used for control and communication computers to assure a safe fault tolerant design. However, the approach needed to achieve the required safety levels in the computer software is not addressed. Further study of methods for assuring software integrity should be conducted, and appropriate requirements should be defined.

Bechtel uses a unique double-shell vehicle structure where the inner shell can be rotated 15° in either direction relative to the outer shell. This scheme requires doors in both shells. The inner and outer doors move out of alignment when the inner shell rotates. Failure of the actuating system or jamming when in the tilted position may have a safety impact on evacuation procedures. This condition should be evaluated.

Bechtel addressed fire hazards by discussing approaches for detecting and suppressing fires, primarily on the vehicles. More consideration should be given to fire prevention, such as materials selection, control of ignition and fuel sources, and operating policies and procedures. Methods for fire prevention, detection, and suppression in system equipment and facilities other than the vehicle should also be evaluated, particularly unstaffed wayside locations which may require automatic systems.

4. FOSTER-MILLER SCD

Foster-Miller's approach to defining a maglev concept is to provide alternative system designs and to specify the advantages and disadvantages associated with each design. However, it is not always clear from the SCD report which design concept will constitute the Foster-Miller baseline system.

The Foster-Miller vehicle consists of 75 passenger modules and nose sections that can be configured as single-car or multiple-car consists. A two-car train meets the 4,000 passenger-per-hour requirement by operating at 130-second headways. The vehicle structure is made of lightweight composite materials and is designed to operate in a U-shaped guideway. The guideway consists of two parallel post-tensioned concrete beams joined transversely by precast concrete diaphragms. Figure 4-1 is a cross-section view of the Foster-Miller baseline vehicle and guideway. Each beam possesses an integral sidewall that carries the null-flux levitation coils and the propulsion coils. The vertical null-flux system consists of four superconducting (SC) magnets on each side

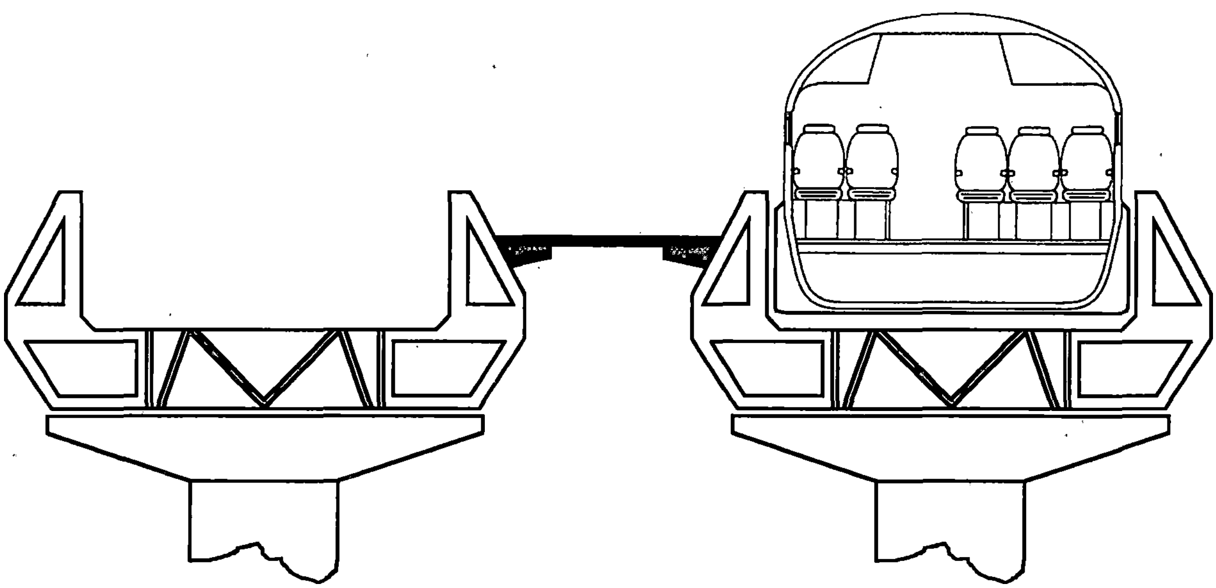


FIGURE 4-1. FOSTER-MILLER DUAL GUIDEWAY AND VEHICLE CROSS-SECTION

of a vehicle-mounted bogie, interacting with eight corresponding coils on the guidewall sidewall. Propulsion coils are located in the sidewall below the levitation coils. The SC magnets on each side of the bogie interact with the sidewall propulsion coils to provide guidance.

This chapter presents the results of the safety review of the Foster-Miller system based on the approach described in Chapter 2. The design features of each major system element are described and safety-related issues are identified. The narrative discussion of safety issues within the following subsections represent the results of the detailed safety review contained in the matrices in Appendix C. Information used for this review is derived from the final Foster-Miller SCD report [3].

4.1 FOSTER-MILLER OVERALL SAFETY APPROACH

Foster-Miller states that they intend to adopt an "Integrated Analytical Approach" which will aggregate the treatment of safety, reliability, and maintenance activities in subsequent design phases. However, their integrated approach is not clearly defined.

Foster-Miller does describe a Safety Hazard Screening approach to identify external hazard causes, estimate the probability and severity of each hazard cause and, depending on the consquences of the hazard, nullify the hazard with design or prevent the hazard with physical measures or procedures/safety regulations. However, the detailed analysis, as indicated by Foster-Miller, itself is incomplete; only propulsion and cryogenic systems are examined in detail.

Foster-Miller places hazards into four categories: Human Origin, Weather Related, Vehicle/Guideway Interaction, and Miscellaneous. With the exception of vehicle/guideway hazards, this approach identifies only hazards that originate outside of the maglev system rather than analyzing malfunctions and failure modes of maglev systems that impact safety. The system design descriptions provided elsewhere in the Foster-Miller SCD are more useful for understanding the safety features of the baseline design. Although Foster-Miller does indicate hazard "effects" for each cause, the effects are not classified by category, i.e., catastrophic, crtical, etc.; thus, there is no means to prioritize the hazard causes. Booz•Allen's recommended hazard severity classifications appear in the following sections.

4.2 VEHICLE STRUCTURE AND INTERIOR DESIGN

4.2.1 System Description

Foster-Miller presents two alternative concepts for construction of the vehicle carbody:

- Aluminum
- AS4/EP Composite Material

Foster-Miller proposes the composite material for its baseline design. Foster-Miller states that the composite material was selected because of high stiffness and strength combined with better sound attenuation, corrosion immunity, and repairability. The vehicle carbody shell is a two-inch thick honeycomb sandwich with a Nomex core and AS4/EP composite face sheets, as shown in Figure 4-2. The frontal nose structure incorporates a graduated stiffness honeycomb structure designed to improve the accident survivability properties of the vehicle. Additional studies with respect to adding a bumper system to the vehicle are to be conducted during subsequent design phases.

The proposed seating arrangement will include first class, two-by-two seating; and coach class, two by three seating. Each vehicle car will accommodate 75 passengers, and have luggage space and restrooms. Multi-vehicle configurations of up to eight connected 75-passenger cars can be developed.

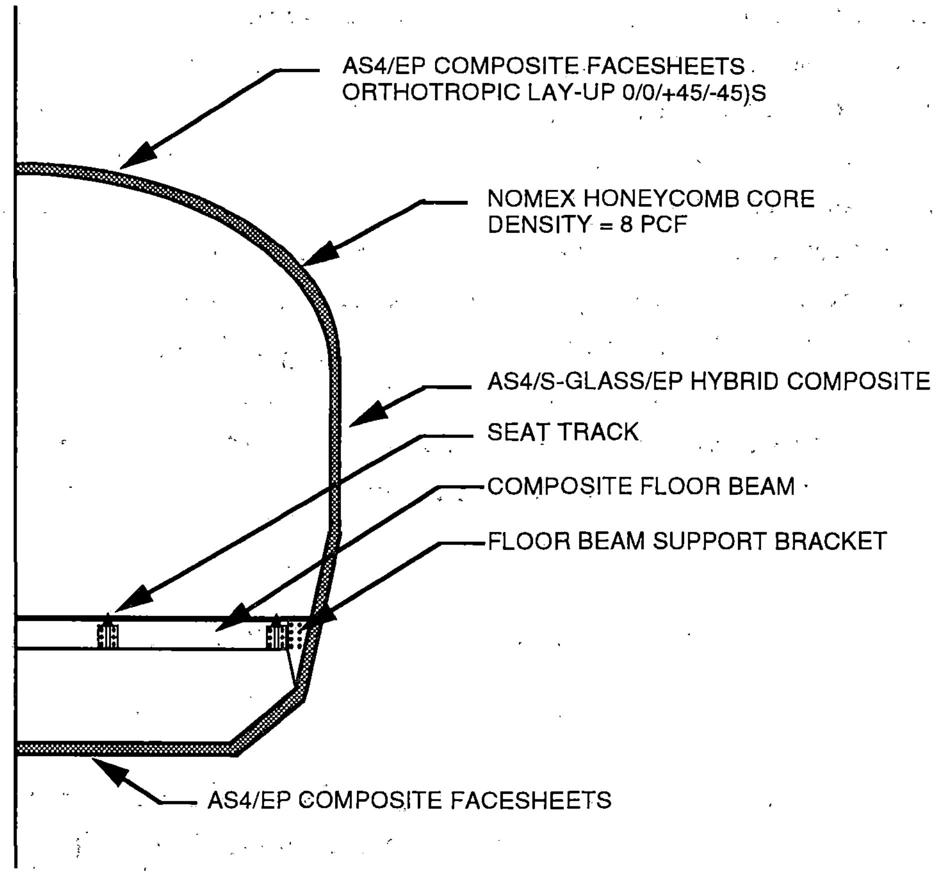


FIGURE 4-2. FOSTER-MILLER CONSTRUCTION DETAILS

4.2.2 Safety Issues

Foster-Miller did not sufficiently address inter-car collisions that could result in one car overriding the top of an adjacent car (i.e., incorporation of an "anti-climber" device). This is a Category II hazard.

Further analysis of the connection between the carbody and bogie should be performed to demonstrate that the bogies will remain attached to the car under all conditions.

Similarly, the forces on the vehicle created by a high speed landing require further analysis to verify the safety of the proposed vehicle structure. Failure of primary vehicle structure at high speed is a Category I hazard.

The composite materials approach to structures has the advantage of being lightweight while meeting the specified load factors. However, existing high speed rail and maglev systems currently under development use only conventional steel or aluminum material for the carbody structural shell. Composite materials have a limited experience base and have the potential for hazardous events that have not yet been fully addressed. In particular, critical composite material failures are not always detectable. Expensive Non-Destructive Inspections (NDIs) are periodically required to ensure the integrity of the structure. Undetected failures could lead to critical structural failures resulting in potentially Category I vehicle failures.

4.3 PROPULSION, NORMAL BRAKING AND EMERGENCY BRAKING

4.3.1 System Description

System propulsion is achieved by providing variable frequency ac power to sidewall-mounted linear synchronous motor (LSM) windings. The three-phase LSM windings are installed vertically on the inside walls of the U-shaped cross-section guideway, directly below the levitation null-flux loops. As the vehicle traverses along the guideway, the LSM windings are energized from a wayside variable current/variable frequency power conditioning source. The energized windings interact with on-board SC magnets. This interaction generates vehicle longitudinal forces that cause the vehicle to move along the guideway.

The unique feature of the Foster-Miller approach is the method in which the LSM coils are energized. As the vehicle traverses along the guideway, only the LSM windings that are aligned at any given instant with the on-board SC magnets are energized, as illustrated in Figure 4-3. As the forward bogie approaches a de-energized LSM winding, a high speed bridge-switching circuit provides ac power at the winding. After the bogie passes, the switching circuit deactivates the LSM winding. The same winding is then re-energized, via the switch, as the rear bogie approaches.

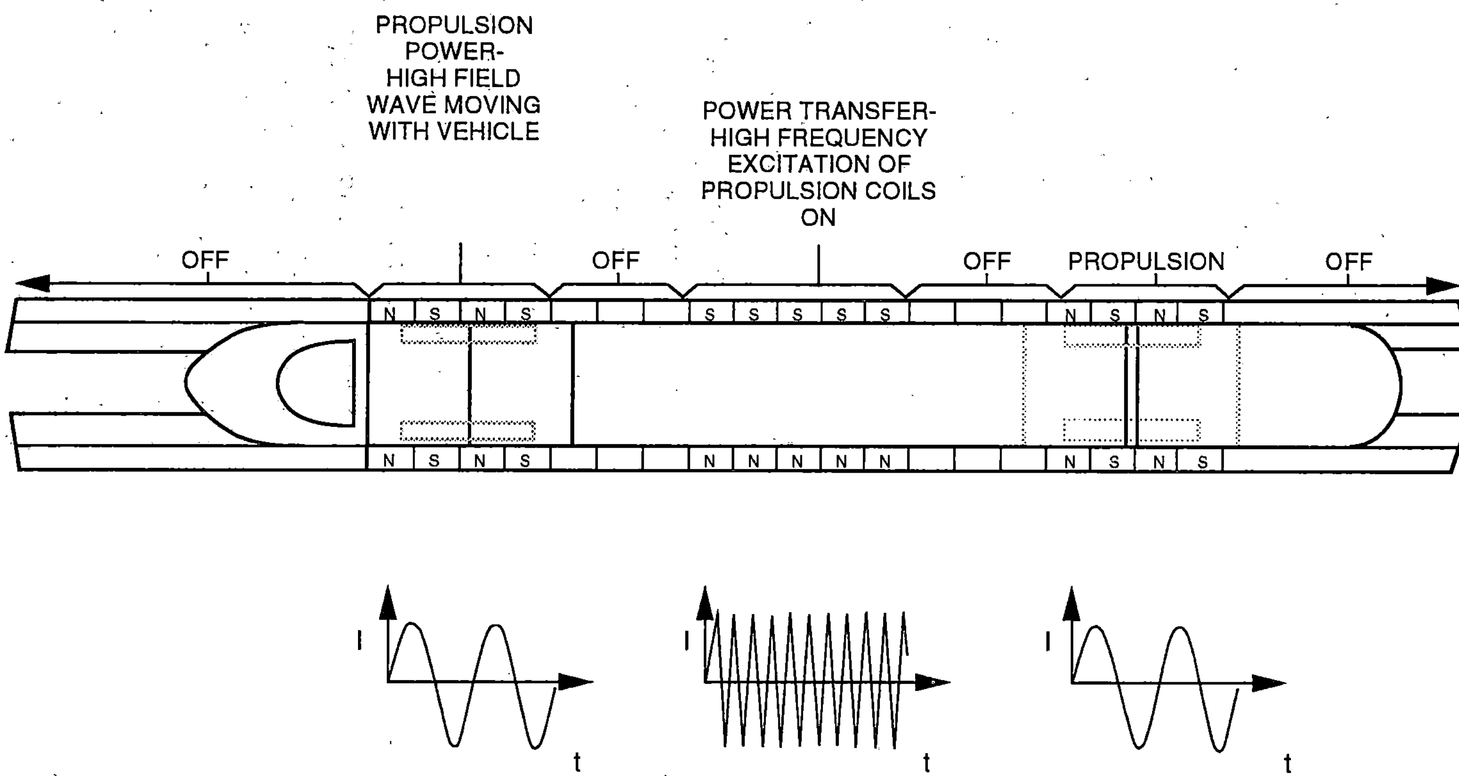


FIGURE 4-3. FOSTER-MILLER VEHICLE TOP VIEW SHOWING PROPULSION AND POWER TRANSFER

Foster-Miller calls this system a locally commutated linear synchronous motor (LCLSM). The LCLSM control system must identify and accurately track the location of the vehicle bogies at all times.

To provide normal non-emergency braking, two methods are proposed by Foster-Miller. Primary braking will be provided through reverse magnetic traction. Secondary braking will be provided through wheel brakes attached to a landing gear, similar to aircraft braking systems.

To provide braking during emergency situations, four skids are provided in the Foster-Miller baseline design. If the landing gear cannot be deployed, the skids will be extended 150 mm (6 in) below the vehicle, contacting the guideway. In the event of an instantaneous loss of magnetic levitation, the undeployed skids will still protrude sufficiently below the magnetic bogies for support. Foster-Miller also asserts that, if the LCLSM power supply fails but the magnetic suspension remains functioning properly, semi-controllable braking can be achieved by deploying the skids and reducing the levitation effect.

4.3.2 Safety Issues

The proposed LCLSM propulsion system relies on high speed power switching that has no similar transportation system applications. The control system must identify the exact location of the vehicle at all times and energize only that section of LSM that is aligned with the bogies. If the LCLSM and vehicle drop out of synchronization, the magnetic forces exerted on the vehicle by the motor may become uncontrollable and cause the vehicle to strike the guideway. This event is potentially a Category II hazard. Since there is no applicable reliability data available, a substantial amount of testing will be required to show that all failures are fail-safe.

4.4 SUSPENSION, LEVITATION AND LATERAL GUIDANCE

4.4.1 System Description

To provide levitation, suspension, and guidance, Foster-Miller proposes a passive null-flux loop system in which the LSM winding loop pairs are interconnected to form lateral guidance null-flux loops. Additionally, passive levitation null-flux loops with a figure-of-eight configuration are mounted in the walls of the guideway. These loops interact with the magnetic field of the on-board SC magnets to electro-dynamically generate levitation forces as a function of the vehicle downwards displacement. The general layout of the levitation, suspension and guidance systems is illustrated in Figure 4-4.

The vehicle bogie assembly contains eight identical SC magnets mounted four on each side of the bogie. The SC magnets interact with coils mounted in the vertical walls of the guideway. Each

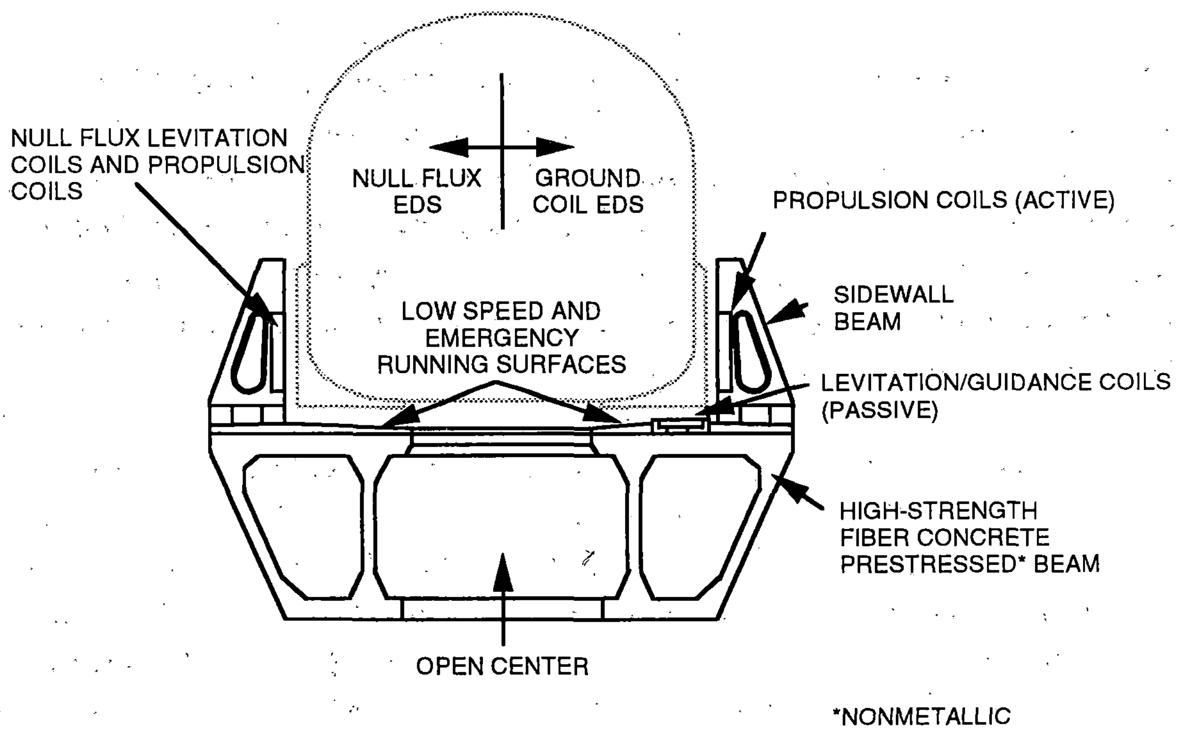


FIGURE 4-4. FOSTER-MILLER GENERAL LAYOUT OF TYPE I GUIDEWAY

magnet includes a helium dewar mounted immediately above the magnet casing. At low speeds, an aircraft-type landing gear will be deployed to support the vehicle.

Operationally, these null-flux loops generate vertical lift forces as a result of the difference between electrically induced currents in the cross-connected conductor coils that form the null-flux loop. When the on-board SC magnet windings are vertically centered between the guideway walls, the current induced in the upper and lower loops will be equal in magnitude and opposite in direction. Therefore, the currents induced in the coils will cancel and no net flux will exist. At that time, in the absence of circulating current, no vehicle levitation force will be generated. However, a downward vertical displacement of the vehicle toward the guideway induces a circulating current within the loops, causing a magnetic field to be generated. The direction of the null-flux loop current will result in the upper coil attracting the on-board magnets while the lower loop repels the magnets. This attraction toward the upper loop and repulsion of the lower loop results in levitation.

The lateral guidance system is also produced by the null-flux loops in the same manner. Increasing the lateral displacement from the center of the guideway results in increasing the magnetic flux generated by one sidewall coil while the flux generated by the loop on the opposite wall is decreased. The induced current in the loops results in a force that pushes and pulls the on-board magnets back towards the guideway center.

The selected SC system provides sufficient levitation force to support the vehicle weight at speeds as low as 5 m/s (11 mph). However, to improve system performance and to overcome magnetic drag, Foster-Miller proposes a delay in magnetic levitation until the vehicle reaches 50 m/s (111 mph). During deceleration, an aircraft type landing gear will be deployed and contact the guideway at 20 m/s (44 mph).

To provide cooling for the SC magnets, Foster-Miller proposes an open-cycle helium cryogenic system. Liquid helium is introduced into the magnet cryostat where vapor forms by the capture of heat from the surfaces of the magnet. The vapor is then vented to the ambient air through trace cooling lines attached to the supports. The SCD drawings indicate that the liquid helium storage system will be located on the bogies which are isolated from passenger compartments by a bulkhead.

To provide passenger comfort through superelevated guideway curves, Foster-Miller proposes a vehicle carbody tilting mechanism, as shown in Figure 4-5.

4.4.2 Safety Issues

Foster-Miller proposes to operate the vehicle SC magnets in persistent current mode so that no external current source will be required except for very infrequent topping-up current charging.

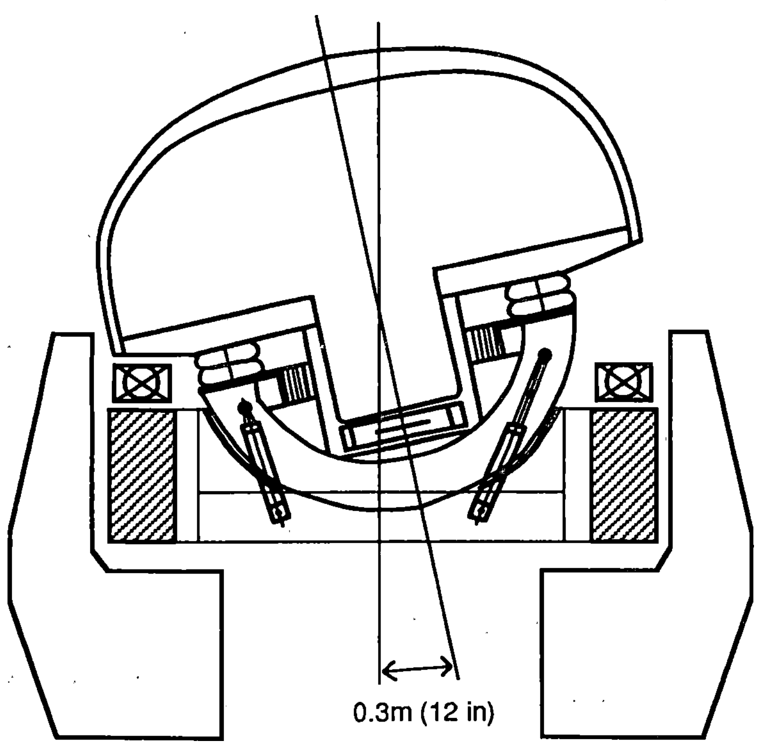


FIGURE 4-5. FOSTER-MILLER TILTING MECHANISM

Therefore, the proposed vehicle suspension and levitation system should continue to operate normally in the event of a power system failure.

In the event of an LSM failure, the maglev vehicle will decelerate at a rate regulated by the aerodynamic and magnetic drag acting against the vehicle. The vehicle magnetic drag induced by the guideway loops is generally lower than those forces induced by floor-mounted discrete levitation coils or sheets. This reduction in drag results in a much smaller jerk force exerted on passengers, as compared to failures of suspension systems incorporating floor-mounted levitation coils or sheets.

The vertical and lateral stiffness of the Foster-Miller concept is expected to be high. This should reduce the risk of the vehicle impacting the guideway walls or floor under extreme adverse conditions such as those caused by extreme cross-wind gusts, gross guideway misalignments, excessive null-flux loop misalignments and inadvertent desynchronization of the LSM under maximum power conditions.

A failure of the on-board magnets will result in immediate loss of levitation and guidance. This is potentially a Category II hazard. The most common cause of SC magnet failure is a propagation of magnet quenching. Potential causes of magnet quenching include loss of magnet cryostat vacuum, mechanical failure of magnet winding load transfer support columns, loss of winding cooling, and mechanical vibration or electromagnetic stress.

To mitigate the effects of such failures, Foster-Miller proposes the following design requirements:

- A failure of two magnet pairs per bogie will result in the deployment of the landing gear and a station stop.

- A system failure that would result in the loss of more than one magnet pair must be avoided.
- The cryogenic cooling system must continue to operate for at least 16 hours after a helium refrigeration unit failure.
- Port/starboard magnets will quench instantaneously as a pair for balanced guidance.

In addition to these requirements, it is important to note that an undetected failure of the first magnet pair will result in a degraded system that is vulnerable to a Category II single point failure. Therefore, the first pair failure should be indicated to the operator or Central Control Facility (CCF).

To assist in minimizing the quenching hazard, future design considerations should include applying a safety factor for the winding current relative to the SC critical current. In addition, a disciplined quality control program during the winding manufacturing process is essential.

By incorporating an aircraft-type landing gear, the Foster-Miller system benefits from several million cycles of service history experienced by these landing gear systems. However, there are three potential hazards associated with installing an aircraft rubber tire type landing gear. First, there is a potential for tire failure within the wheel well resulting in damage to equipment installed in or near that area, potentially a Category II hazard. Second, landing gear braking systems require airflow for cooling. The Foster-Miller guideway design appears to limit air cooling capacity because of the close sidewall design. Reduced braking effectiveness due to overheating is a Category II hazard. Finally, at high speeds, the friction created between rubber tires and the landing surface is sufficient to ignite the tires and create a fire hazard. To resolve these hazards, a zonal analysis of the installation of both the gear on the guideway, and in the interior of the wheel well must be performed.

On-board cryogenic systems have potential Category I and II hazards that should be identified and mitigated during the preliminary design phase. They include the effects of "cold" burns, cryogenic oxygen deficiency, and materials embrittlement. These hazards are applicable for Foster-Miller as for the other SCDs and have been described in detail in Section 3.4 of this report.

Although the tilting mechanism provides a way to increase train speed through curves, Foster-Miller acknowledges that the mechanism reduces passenger safety. Depending on the speed of the vehicle, standing passengers may fall down if a critical failure occurs while the train is negotiating a curve. A complete failure modes analysis is needed to identify failures that may result in the following unsafe conditions:

- Tilting system fails to return to the upright position after negotiating a curve (Category III hazard)
- Tilting mechanism fails such that the carbody tilts in the opposite direction prior to entering a curve (Category II hazard)
- Tilting mechanism fails to tilt (Category II hazard).

4.5 ON-BOARD POWER SYSTEM

4.5.1 System Description

To provide on-board electrical power, on-board coils are excited by high frequency induction from the LCLSM windings. This is achieved by an air core resonant transformer with the on-board coils acting as a secondary and the LCLSM acting as the primary winding. As the SC magnets pass a given guideway coil, this LCLSM coil is switched to provide propulsion force. As the on-board resonant transformer coils pass a given guideway coil, this LCLSM coil is switched to provide electrical power transfer. Two redundant coil systems are installed in parallel, one port and the other starboard, and are excited simultaneously. In stations, electrical power is provided by external station power, and during emergencies, batteries are used. The on-board power loads include passenger amenities, HVAC, galley service, and lighting.

4.5.2 Safety Issues

The Foster-Miller on-board power system does not support any safety-critical equipment. The proposed on-board electrical power system uses the LCLSM windings which are also used for vehicle propulsion. This design requires a high degree of precision timing in switching from low to high, and back to low frequency. Foster-Miller acknowledges that more studies are required in future development programs to demonstrate the effectiveness of the power transfer system.

4.6 MAGNETIC SHIELDING

4.6.1 System Description

Although not discussed in the Foster-Miller Safety Hazard Screening process, the SCD does acknowledge that the magnetic fields of the SC magnets may create safety hazards for passengers and crew, particularly to passengers with cardiac pacemakers. To develop a shielding criteria, Foster-Miller applies standards incorporated by the Magnetic Resonance Imaging (MRI) industry; the external field is to be maintained below 0.5 mT (5 gauss).

Foster-Miller defines and studies several methods for mitigating the magnetic exposure hazard. Foster-Miller will use octupole-aiding flux magnets on the ends of the vehicle bogies to decrease the passenger cabin magnetic field to less than 2 mT (20 gauss) of dc field. In addition, a ferromagnetic shell will be installed around five sides of the vehicle cabin to achieve a 0.1 mT (1 gauss) maximum field, and a less massive ferromagnetic shell to shield the passengers to a 0.5 mT (5 Gauss) level will be incorporated.

4.6.2 Safety Issues

Since the proposed shielding is passive, the methods should be effective for reliably shielding passengers from magnetic fields. The Foster-Miller analysis of the LCLSM windings shows that the nearest passenger will be exposed to only 0.02 mT (0.2 gauss) of ac field, which is below the 0.1 mT (1 gauss) level but higher than 0.01 mT (0.1 gauss) ac level required in the SCD SOW. According to Foster-Miller, the most effective and only method that will protect passengers below the 0.1 mT (1 gauss) level is a ferromagnetic shell.

4.7 FIRE PROTECTION

4.7.1 System Description

To provide fire protection, Foster-Miller proposes using the fire requirements defined by the Federal Railroad Administration codes (regulations). According to Foster-Miller, the FRA requirements include installing heat detectors, multiple fire extinguishers, and escape windows on the vehicle. Foster-Miller states that according to conventional practice, the materials used for vehicle construction will be low smoke foam padding, and fire retardant fiberglass reinforced plastic (FRP) liners.

4.7.2 Safety Issues

Foster-Miller incorrectly cites the FRA regulations. These regulations do not address heat detectors or the installation of fire extinguishers. The use of "conventional practice" in reference to materials construction is vague; at a minimum, the FRA fire safety guidelines for selecting interior materials should be used as a baseline. A complete fire protection approach should include fire prevention, containment, detection and suppression. Foster-Miller should give further consideration to the selection and placement of electrical cables, terminals and equipment to preclude the initiation of a fire as well as its spread. In addition, methods for detecting and suppressing fires in isolated, unstaffed wayside locations should be addressed by Foster-Miller.

4.8 GUIDEWAY DESIGN

4.8.1 System Description

The Foster-Miller selected guideway configuration and layout consists of modular construction twin hollow beams connected by structural transverse diaphragms. The transverse diaphragms are spaced every five to six meters. This guideway design provides suspension support at the outermost corners of the vehicle where the bogie magnets are mounted. The guideway high-stiffness, multi-celled box beam incorporates structural support beams and sidewalls. LCLSM windings and levitation null-flux loops are located in the guideway sidewalls.

4.8.2 Safety Issues

The twin hollow beam design of the guideway provides limited vehicle "wrap around" of the guideway. Gravity and the magnetic levitation and guidance system are the only forces preventing the vehicle from departing the guideway. The safety certification of this design will require substantial analysis and testing of the levitation and guidance system to assure that a vehicle departing the guideway is an extremely improbable event under all foreseeable conditions.

To preclude animals, trespassers, and snow from the guideway, Foster-Miller states that the guideway will be designed with slanted surfaces. There are two concerns with this approach:

- It is possible for snow and ice to build up on slanted surfaces.
- The guideway design depicted by Foster-Miller in its SCD report does not have slanted surfaces.

By designing a twin hollow beam guideway, obstructions and debris are not likely to accumulate on the guideway. However, since the guideway is open in the center, it is conceivable that an earthquake potentially could cause both beams to move independently. This may result in loss of levitation and cause the vehicle to strike the guideway.

4.9 GUIDEWAY SWITCH

4.9.1 System Description

To provide lateral guidance through switches, Foster-Miller proposes a very high speed vertical switch with stationary vertical sidewall levitation coils, as shown in Figure 4-6. Switching is accomplished by implementing wound figure-of-eight coils that provide two optional paths for the vehicle. Coils in the desired direction are cross-connected by switches that also open coil circuits in the undesired direction. The coils which are cross-connected provide levitation through the vertical switch while the open circuited coils do not interact with the vehicle magnets. Foster-Miller states that this allows for a switching system that, in principle, does not rely on any moving mechanical or structural components.

The Foster-Miller proposed guideway design provides limited vehicle wrap-around of the guideway. Gravity and the magnetic levitation

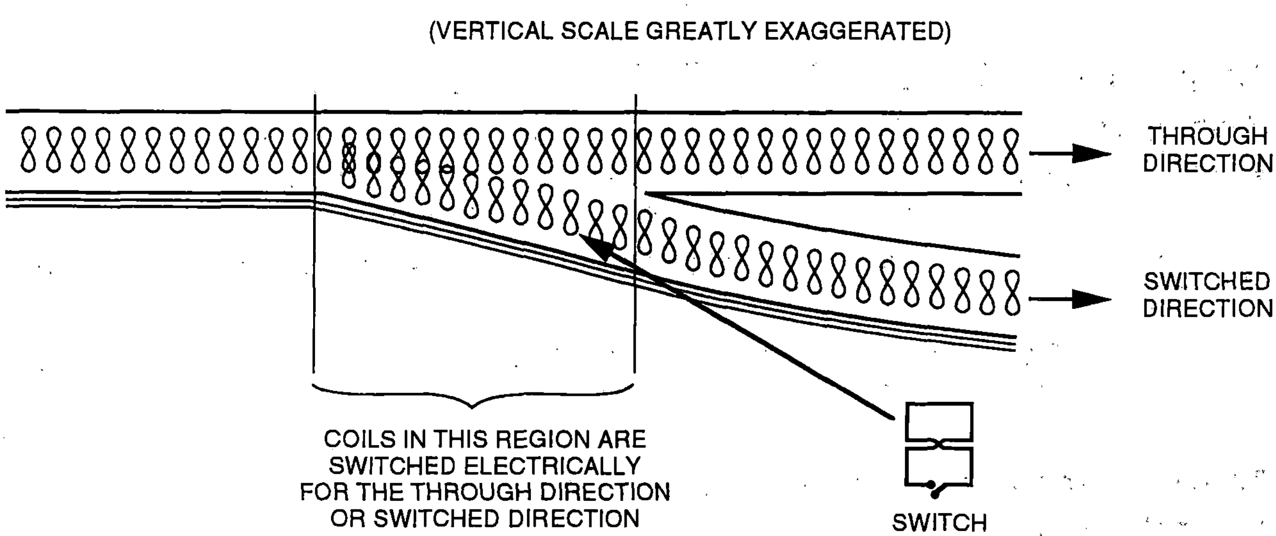


FIGURE 4-6. FOSTER-MILLER NULL-FLUX OPERATION IN VERTICAL SWITCH

and guidance system are the only forces preventing the vehicle from departing the guideway. The safety certification of this design will require substantial analysis and testing of the levitation and guidance system to assure that a vehicle departing the guideway is an extremely improbable event under all foreseeable conditions.

4.9.2 Safety Issues

As the vehicle goes through the turnout direction of the switch, there is a time period in which the vehicle is exposed to an open bottom guideway. If there is a loss of levitation while the vehicle is in this region, the vehicle will fall to the guideway below, a Category I event. To mitigate this hazard, Foster-Miller states that a movable beam floor can be provided. However, providing a movable floor eliminates the improved reliability and cost savings associated with the purely electro-magnetic coil switch scheme proposed by Foster-Miller.

4.10 GUIDEWAY MONITORING

4.10.1 System Description

To provide guideway obstacle monitoring, Foster-Miller proposes several methods. Guideway protection will be provided by security fencing and, in areas of direct overhead access, by overhead roofing. To maintain a high level of safety, Foster-Miller proposes a system defined as a "risk contour approach." The overall premise of this approach is to segmentally characterize the route based on various population and geographical factors to determine the associated risk of natural or man-made foreign object intrusion. Appropriate detection and prevention measures are then selected based on the risk.

In the highest risk areas, a machine vision system will be installed. This system will digitally record an initial image using charge-coupled device cameras and compare that image to images continuously being monitored. Any change in the image is interpreted as a foreign object and proper action can be taken. In the next highest risk area, infrared motion detection will be utilized. This system will monitor movement along the guideway. Finally, in the lowest risk area, standard security cameras will be installed and monitored.

A drone inspection will be used over the entire system at a minimum of once per day before beginning operation. Additional inspections may be required and are planned to be implemented as needed.

4.10.2 Safety Issues

Collisions with obstacles are potentially Category I events. Foster-Miller's proposed guideway monitoring concept does not ensure that the entire system is monitored continuously over the entire route. Although the likelihood of an object landing on the guideway may be greater in congested areas, the probability of an animal, snow, or debris landing on the guideway in less populated areas is substantial. Therefore, the "risk contour approach" to guideway monitoring may not be effective.

In addition, the charge-coupled device and closed circuit television systems defined by Foster-Miller are dependent upon light for effectiveness. Night operation will be dependent upon artificial lighting. Infrared detection systems may not be effective since they are prone to nuisance warnings. Accordingly, the Foster-Miller approach to guideway monitoring requires further development.

4.11 POWER SYSTEM AND DISTRIBUTION

4.11.1 System Description

Foster-Miller uses a three-phase connection from the utility to the substation. The substation power distribution system, as shown in Figure 4-7, includes a transformer, an automatic physical disconnect, secondary ac circuit breakers, a GTO rectifier and an H-Bridge configuration switch circuit used for guideway propulsion.

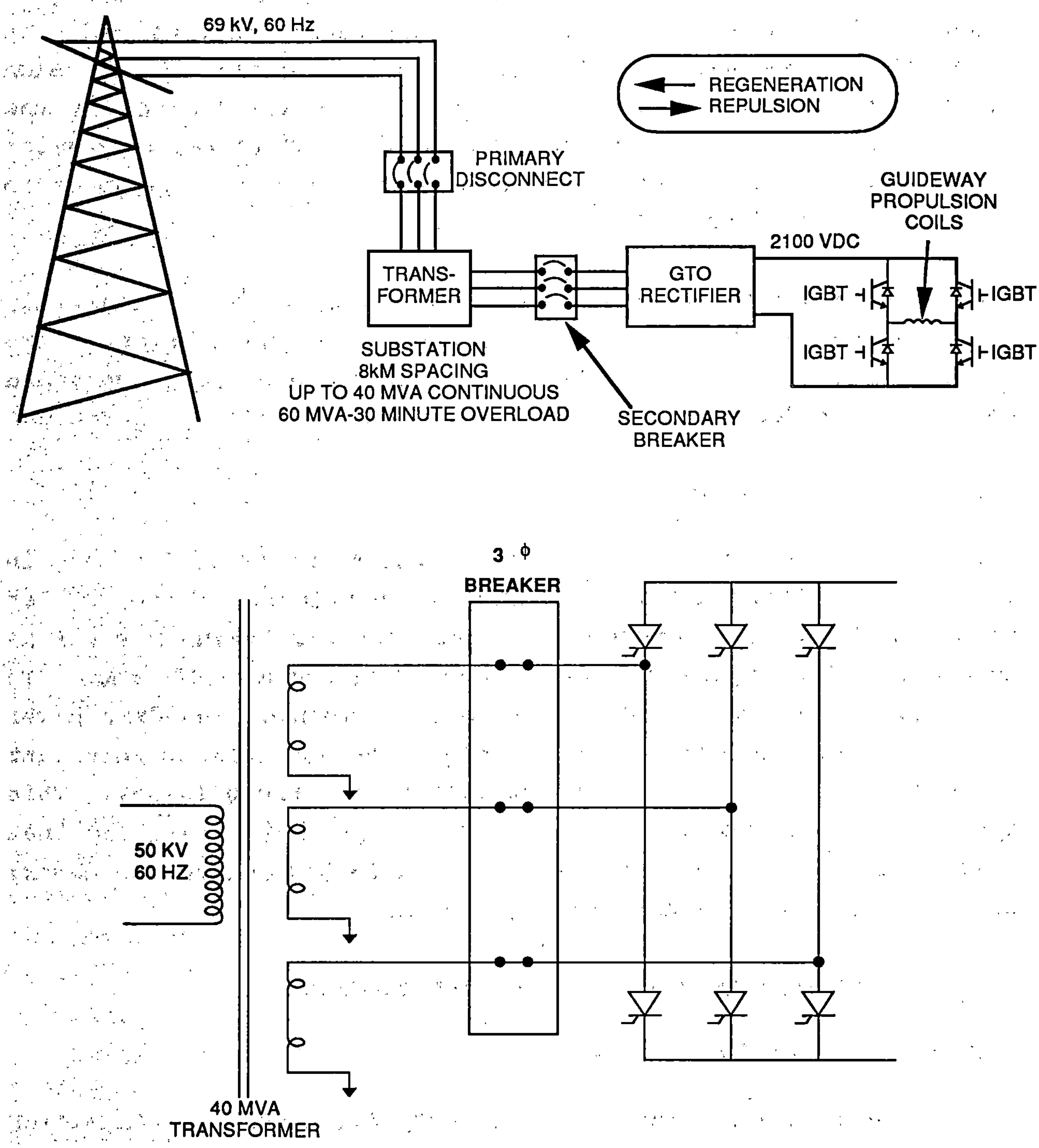


FIGURE 4-7. FOSTER-MILLER POWER DISTRIBUTION SYSTEM

The input to the substation transformer is 69,000 volts, 60 cycle power. The transformer and GTO rectifier converts this to 2,000 vdc. Because of the high power requirement at each substation, the GTOs are connected in parallel to handle the required current. Foster-Miller states that each of these parallel connections would be fused so that the substation could continue to operate if one of the GTOs fails.

The power required for each of the guideway coils is approximately 300 kw and each of these coils is supplied by an H-bridge. The circuit breaker Foster-Miller proposes to use is a standard commercial product.

4.11.2 Safety Issues

Foster-Miller indicates that loss of primary power will result in loss of propulsion and normal braking functions. Foster-MIller states that during primary power loss, heavier trains may strike the rear of the lighter trains because of momentum difference. To mitigate these hazards, Foster-Miller recommends redundant power stations. However, the concept design does not include redundant connections between the power substations and the guideway. This approach exposes power substations to single point failures that result in primary power loss along the affected substation block; this is potentially a Category II hazard.

4.12 COMMUNICATIONS, COMMAND, AND CONTROL

4.12.1 System Description

To provide automatic train control (ATC) functions, Foster-Miller proposes a microprocessor-based automated moving block system. At the highest level of communications, a CCF will perform dispatching and automatic train supervision (ATS) functions, as illustrated in Figure 4-8. The basic control unit along the guideway will be the wayside control microprocessor (WCM). The WCM will be a redundant computer system responsible for automatic train operation (ATO) and automatic train protection (ATP) functions.

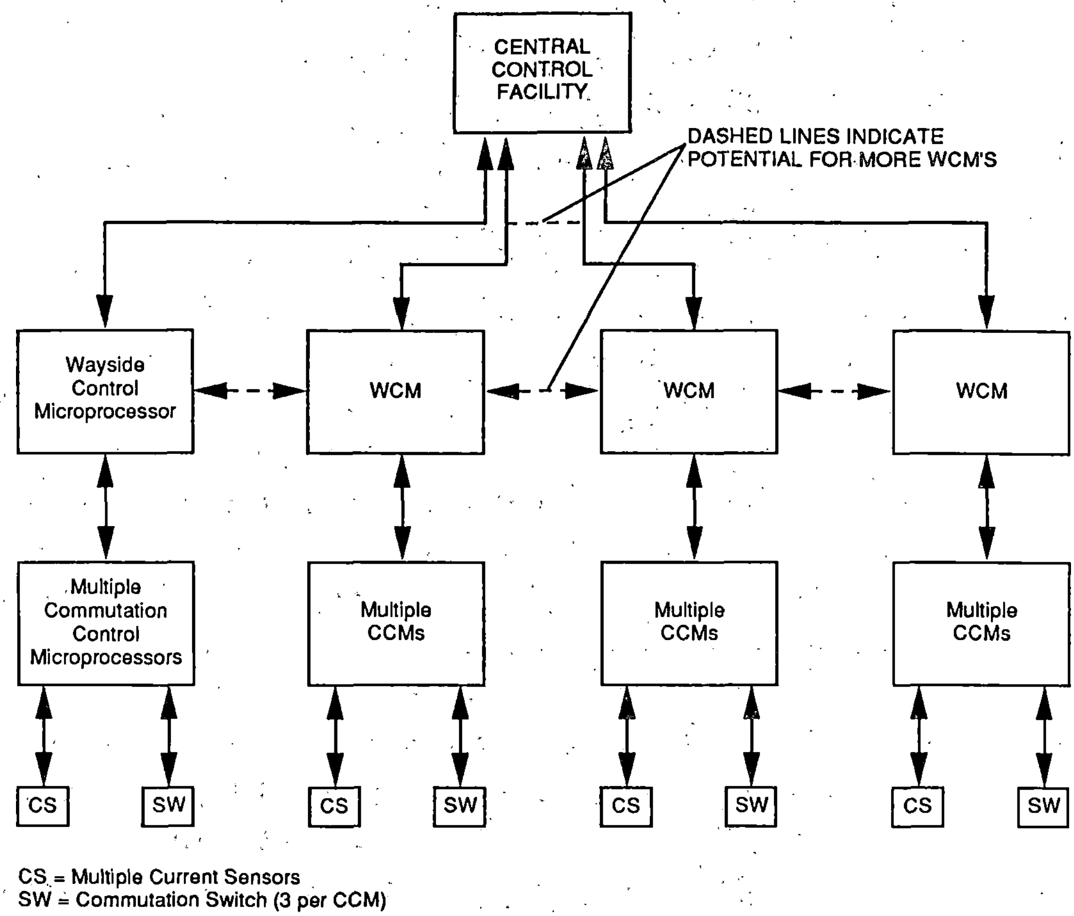


FIGURE 4-8. FOSTER-MILLER PROPOSED HIGH-LEVEL CONTROL SYSTEM ARCHITECTURE

Redundant fiber optics communications will transmit signals between the CCF and WCMs. At the lower levels, there will be four major interfaces: 1) sensors for various conditions along the guideway will provide information directly to the WCMs; 2) the micro-processor-based propulsion system will report vehicle speed and position to the WCMs; 3) interlocking control systems will assure that conflicting routes cannot be set at control points (i.e., guideway switches) and each interlocking system will communicate to a WCM via the fiber-optic network; and 4) vehicles will report their status to WCMs via a digital radio link.

4.12.2 Safety Issues

The system configuration is similar to a number of ATC systems in operation today. One deviation from existing systems is the incorporation of vital processes into the propulsion control system. The determination of correct vehicle speed and position is a safety-critical function. The software responsible for this function must be partitioned from the non-vital functions of the propulsion control. The hardware configuration is also expected to be checked redundant. In the event of an overspeed condition being detected, or entry into an unauthorized zone, the onboard system must be able to implement a brake application, over-riding the propulsion system. It is also necessary to achieve some form of motion control following an ATP intervention. This may necessitate the ATP system being independent from the braking and propulsion systems on board the vehicle. Further analysis is needed as the design of the system progresses to demonstrate that all potential Category I events are extremely improbable. In addition, further study of methods for assuring software integrity should be conducted, and requirements for developing and controlling safety-critical software should be defined early in the system development.

4.13 SYSTEM OPERATIONS AND MAINTENANCE ISSUES

4.13.1 System Description

The minimum safe headway is based on both the vehicle speed and "worst case" braking capabilities. Foster-Miller acknowledges that at short headways, there are certain events that create risks that cannot be effectively countered. Natural disasters or acts of sabotage that result in massive obstructions on the right-of-way will always present a risk. In addition, Foster-Miller states that at short headways, secondary collisions with succeeding vehicles may be difficult to avoid, potentially resulting in multi-vehicle incidents similar to those reported on high speed freeways. With longer headways, the risk of secondary collisions is much smaller or virtually eliminated. Therefore, Foster-Miller asserts that for the same system passenger capacity, longer car consists with longer headways will prove to be safer than fewer vehicle consists at shorter headways.

4.13.2 Safety Issues

The operation of longer car consists is desirable if it minimizes the possibility of secondary collisions. The need to operate with realistic station dwell times while minimizing the number of platforms and complex switching arrangements at the stations must be included in headway determination.

4.14 ENVIRONMENTAL EFFECTS

4.14.1 Environmental Considerations

Foster-Miller states that snow and ice accumulation will be eliminated by incorporating slanted surfaces in the guideway design. To mitigate water damage due to rain, electrical boxes will be watertight and non-slip floors will be incorporated. The nose section of the vehicle will be reinforced to protect against hail. To protect against strong winds, hurricanes and tornadoes, Foster-Miller states that the guideway will be designed to withstand high winds and the vehicle suspension will be designed to allow for high crosswind-induced loading without the risk of contacting the guideway. The system will be protected from lightning strikes by proper grounding of equipment using proven methods. Finally, the system will be designed using California construction codes for earthquakes.

4.14.2 Safety Issues

The relative importance of environmental effects will depend primarily on the operating region of the maglev system. There are no safety concerns associated with the Foster-Miller approach to lightning protection which uses proven methods for mitigating these hazards. The mitigating measures for the other weather-related hazards are generic and general. More design development is required to ensure that hazards relating to specific climatic conditions are resolved.

4.15 SUMMARY OF FINDINGS - FOSTER-MILLER

Foster-Miller states that it intends to adopt an "Integrated Analytical Approach" which will aggregate the treatment of safety, reliability, and maintenance activities in subsequent design phases. However, this integrated approach is not clearly defined.

The safety analysis provided by Foster-Miller places hazards into four categories: Human Origin, Weather Related, Vehicle/Guideway Interaction, and Miscellaneous. With the exception of vehicle/guideway hazards, this approach identifies only hazards that originate outside of the maglev system rather than analyzing malfunctions and failure modes of maglev systems that impact safety. The system design descriptions provided elsewhere in the Foster-Miller SCD are more useful for understanding the safety features of the baseline design. Booz•Allen's recommended hazard severity classifications appear in the following sections.

Foster-Miller proposes composite materials for its baseline vehicle structure. The composite design approach has a limited applicable experience. Foster-Miller has not fully addressed the structural issues of composite material failure detectability, vehicle override protection during inter-car collisions (i.e., an anti-climber device), and high speed landings. The forces exerted by high speed landings may cause critical structural failures.

The Foster-Miller proposed locally commutated linear synchronous motor (LCLSM), used for propulsion and electrical power, relies on high speed power switching circuitry to switch the power inverter. This mode of operation for a power inverter as proposed by Foster Miller is unique. If the LCLSM and vehicle bogies drop out of synchronization, the magnetic forces exerted may cause the vehicle to strike the guideway. This is potentially a Category II hazard. This is potentially a Category II hazard. The LCLSM and train control systems will require a substantial amount of testing to show that all failure modes are safe.

Foster-Miller proposes a sidewall-mounted null-flux coil suspension system. A failure of the on-board super-conducting magnets (e.g., from a propagation of magnetic quenching) results in immediate loss of levitation and guidance. To mitigate the effects of such failures, Foster-Miller identifies four key design criteria. In addition to the criteria, design considerations should include applying a safety factor for the null-flux coil winding current, relative to the superconducting current, and a disciplined quality control program during the magnet manufacturing process should be implemented.

There are three potential hazards associated with installing an aircraft-type rubber tire landing gear as proposed by Foster-Miller. First, there is a potential for tire failures within the wheel well, that would damage equipment. Second, landing gear braking systems require cooling that may be limited by the closeness of the guideway sidewalls. Third, rubber tires are potentially fire hazards at high speeds.

The proposed on-board cryogenic system has potential physiological and vehicle structural hazards (e.g., asphyxiation, cold burns, and materials embrittlement) that were not addressed by Foster-Miller. These Category I hazards should be identified and mitigated during the preliminary design phase.

Although the proposed tilting mechanism provides a way to increase train speed through curves, Foster-Miller acknowledges that certain tilting mechanism failures are hazardous. While the train is negotiating a curve, tilting mechanism failures may expose passengers to excessive lateral acceleration forces. In addition, the jamming of the tilting mechanism during emergency evacuation can make vehicle egress difficult.

Foster-Miller proposes an on-board electrical system that relies on the same LCLSM system used for propulsion power. This method requires a high degree of precision timing for switching the LCLSM from the propulsion mode to the power transfer mode. Foster-Miller acknowledges that more studies are required to demonstrate the effectiveness of the power transfer system.

The Foster-Miller proposed guideway design provides limited vehicle wrap-around of the guideway. Gravity and the magnetic levitation and guidance system are the only forces preventing the vehicle from departing the guideway. The safety certification of this design will require substantial analysis and testing of the levitation and guidance system to assure that a vehicle departing the guideway is an extremely improbable event under all foreseeable conditions.

Foster-Miller proposes a very high speed vertical switch with stationary vertical side-wall levitation coils. This switching system does not rely on any moving mechanical or structural components. If there is a loss of levitation while the vehicle is in the turn-out region of the switch, the vehicle will fall to the guideway below. This is potentially a Category I hazard. A detailed safety analysis and extensive testing should be required to demonstrate that this hazard is extremely improbable.

The Foster-Miller proposed automatic train control system is similar to existing systems currently in operation. One exception is the incorporation of vital processes into the propulsion system. An approach to achieve the necessary software safety is not presented. Further study of methods for assuring software integrity should be conducted, and requirements for developing and controlling safety-critical software should be defined early in the system development.

To mitigate snow and ice on the guideway, Foster-Miller proposes to incorporate slanted surfaces into its guideway design. However, the effectiveness of slanted surfaces to eliminate snow and ice is not obvious. In addition, a review of the guideway drawings does not indicate that slanted surfaces are incorporated.

5. GRUMMAN SCD

The Grumman design is based on the electromagnetic suspension (EMS) system concept. However, the design uses the innovaton of using superconducting (SC) iron core magnets along both sides of the vehicle to generate attractive forces. The vehicle wraps around an inverted V-shaped guideway, as illustrated in Figure 5-1, and uses just one set of vehicle magnets and guideway rails with linear synchronous motor (LSM) windings for levitation, guidance, and propulsion. There are 24 levitation electromagnets distributed lengthwise on each vehicle. Each magnet consists of a horseshoe-shaped permendur-iron core with superconducting windings which provide the steady state lift force. Propulsion is provided by conventional, three-phase LSM windings embedded in the guideway rail.

The consist is a two-vehicle configuration for 100 passengers; it can be shortened to a 50-passenger, single vehicle or lengthened to a 150-passenger, three-vehicle consist. The body is made of aluminum and provides for up to nine degrees of body tilt.

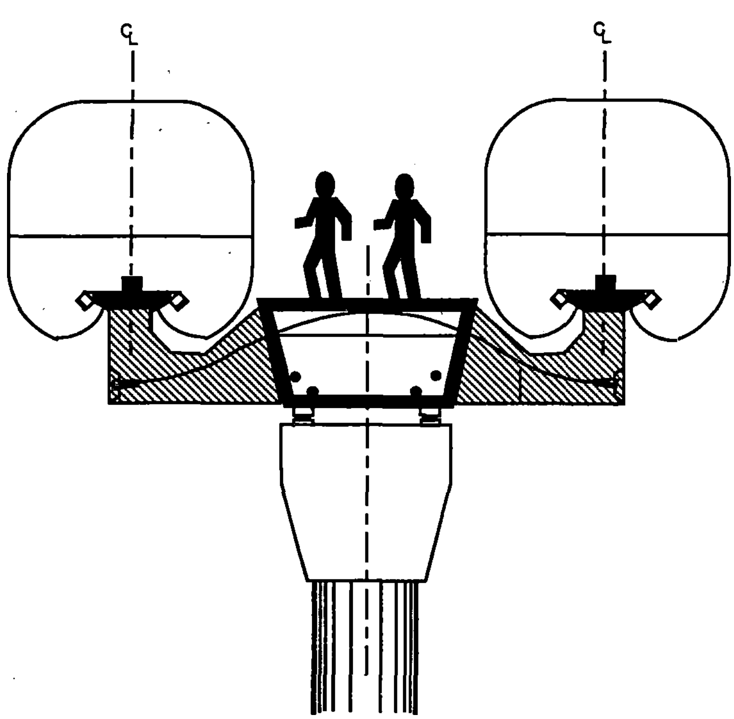


FIGURE 5-1. GRUMMAN DUAL GUIDEWAY AND VEHICLE CROSS-SECTION

The guideway consists of slender inverted V-shaped sections (one for each direction), mounted to a 27 m (88.6 ft) main beam by outriggers every 4.5 m (14.8 ft). The main beam (serving both directions) is, in turn, supported by a conventional pier on piled or spread footings. Switching is accomplished with a bending guideway beam, complemented by a sliding or rotating, elongated section that allows for a shorter length of bending guideway.

This chapter presents the results of the safety review of the Grumman system based on the approach described in Chapter 2. The design features of each major system element are described and safety-related issues are identified. The narrative discussion of safety issues within the following subsections represent the results of the detailed safety review contained in the matrices in Appendix D. Information used for this review is derived from the final Grumman SCD report [3].

5.1 GRUMMAN OVERALL SAFETY APPROACH

The Grumman SCD includes a safety assurance plan which describes the process used, and results obtained, in identifying and resolving potential safety hazards. The overall objective of this plan is to ensure that safety is a primary consideration in the process of defining the Grumman system concept. Grumman states that other specific objectives are:

- To provide guidance to the system design effort relative to safety;
- To minimize the number, severity and probability of occurrence of hazards residual to the resulting design;
- To provide an indication (evidence) that hazards associated with the system concept are controlled/mitigated to acceptable levels of risks; and
- To provide a basis for safety and hazard resolution activities in future development efforts.

Grumman conducted a Preliminary Hazard Analysis (PHA) to identify approximately 150 potential hazards and based their severity and probability on the definitions provided in MIL-STD-882B. Major system elements included in the PHA are substation/guideway power; communications, command and control; levitation/guidance; vehicle; and environment.

A control provision is recommended for each hazard, and the design feature is identified that has been or will be incorporated into the baseline design to control the hazard. The Booz•Allen review of the PHA showed that it was comprehensive and that a "resolution" or "control method" was documented for the majority of the identified hazards.

Grumman states that while the PHA identified and supported the resolution of numerous potential hazards in the design, not all hazards can be identified in a conceptual design. During the next phase of concept and design development, Grumman expects other hazards will be identified.

The interfaces between safety, human factors, reliability, and maintenance activities were handled appropriately. The reliability program plan made good use of the PHA data, recommending design approaches to reduce the probability of the occurrence of identified potential hazards. Grumman considers four approaches to achieve a high level of safe system operation:

- **Network Redundancy** - Multiple paths for accomplishing the desired function are provided. The availability of any one path permits the desired function to be executed.
- **Load-Sharing Redundancy** - The utilization of 'n' independent units/components to implement a function which requires only 'm' items for success, where n is larger than m.
- **Stand-By or Voting Redundancy** - Two or more interconnected means, dedicated to accomplishing the desired function, are provided. Decision logic and switching provisions are required. An example is 2-out-of-3 voting in which agreement is needed in at least 2 channels.
- **High Reliability Series String** - The non-redundant implementation of a function utilizing components demonstrated to be highly reliable through field use, continuous production, and based on mature technology.

5.2 VEHICLE STRUCTURE AND INTERIOR DESIGN

5.2.1 System Description

Grumman has selected an aluminum structure for its baseline design. The aluminum cabin is designed as a built-up sheet and stringer, mechanically fastened structure with internal frames and longerons at discrete locations along the length of the vehicle. The floor is constructed of bonded honeycomb sandwich panels.

The 50-passenger module undercarriage is developed with an underfloor support frame and a chassis. Connected to the primary suspension system frame are 32 structural magnet support fittings and 24 magnets.

The support frame and chassis are connected to each other by six primary tilt mechanism links and four secondary links. The magnet support fittings-chassis attachment points are located to allow the support loads to be transferred to the body. The tilt mechanism links are major load-carrying members and provide longitudinal, lateral, and vertical stability, and support the passenger cabin.

The under floor interspace is divided into eight bays that are used to locate the following systems: tilt mechanism, helium gas storage tanks, two-stage gas compressor, eddy current and friction brakes, batteries, air conditioning compressor, power conditioning equipment, "dead vehicle" wheel assembly, and skids.

Grumman will select materials that meet acceptance requirements concerning fire and toxicity resistance that comply with NFPA 130, Fixed Guideway Transit Systems. In addition, vehicle lightning protection is provided by incorporating the requirements of NFPA 130 into the design, and by bonding copper or aluminum mesh to non-metallic external surfaces to serve as a high conductivity electrical path to dissipate a lightning strike. Glazing and nose compartment materials will meet the requirements of 49 CFR, Part 223, in order to protect passengers and crew from injury as a result of objects striking the windows or leading surfaces of the vehicle.

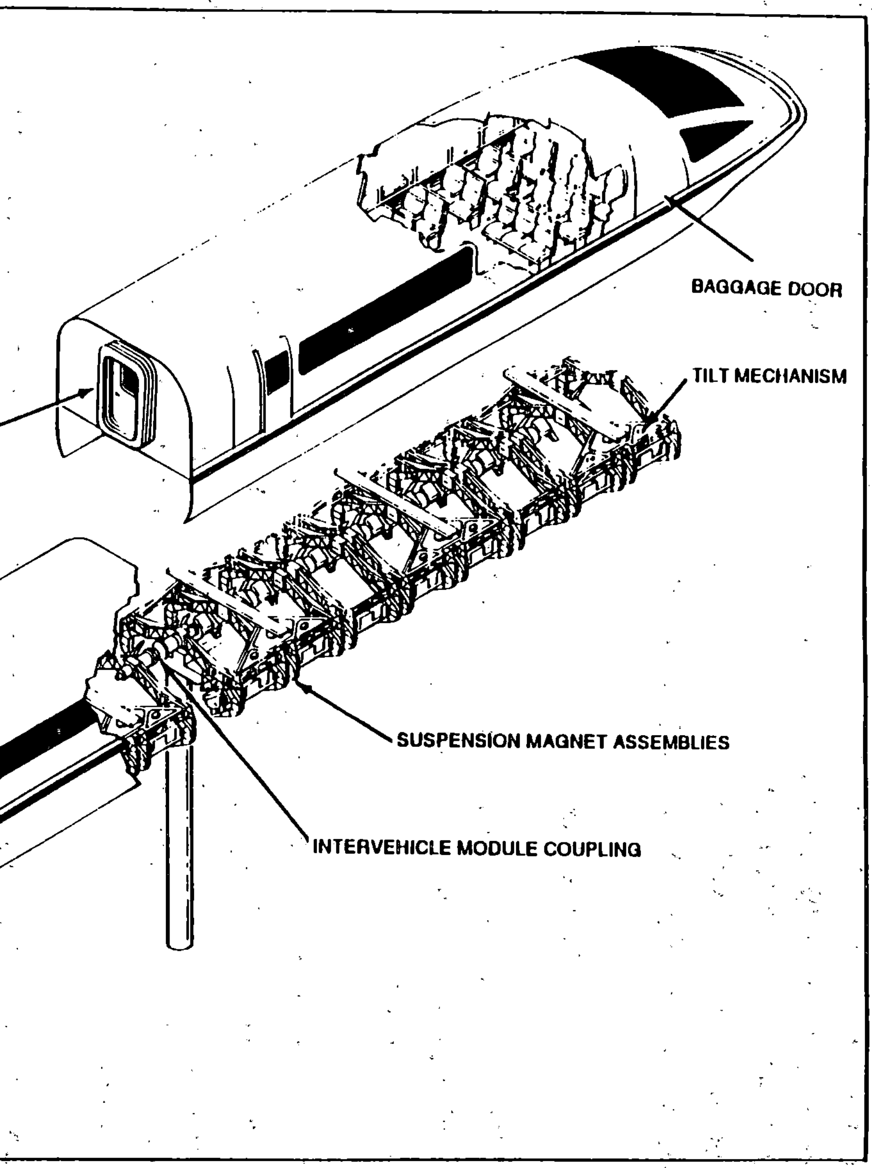
The vehicle is designed with energy-absorbing bumper assemblies fitted to the front and rear of the vehicle. In operation, the assembly absorbs the vehicle's kinetic energy during a low speed collision and limits the magnitude of deceleration.

A number of system trade-off studies (e.g., vehicle weight and power) were performed by Grumman to arrive at the two-module baseline vehicle configuration identified in Figure 5-2. The best trade-off between weight and power was identified in the range of four to five seats across. Grumman has chosen five seats across for its baseline configuration to keep the vehicle weight as low as possible with a minimum associated power penalty.

A module consists of a 12.7 m (41.7 ft.) long center section, which seats 50 passengers with two entrance doors (one on each side of the vehicle), two lavatories (one designed to accommodate handicapped passengers), multiple overhead and closet storage facilities, and a galley area. The forward and aft sections of the vehicle utilize the second module, which consists of a 4.9 m (16.0 ft.) long section that is externally identical, but internally different, depending on its forward or rear location on the vehicle.

The vehicle has side doors for passengers to enter and exit the vehicle at stations. Passengers will step directly from the vehicle onto the station platform without the need to step up or down, thereby allowing elderly and disabled passengers to easily enter and exit the vehicle. The communication, command, and control (C^3) system (see section 5.12) will control the opening and closing of the side doors. The vehicle will not move until all side doors are locked and verified in the closed position and the C^3 system gives a "proceed" signal.

FIGURE 5-2.



BASELINE CONFIGURATION

In the multi-vehicle configuration, 50-passenger cars are connected with a semi-automatic coupler assembly. The coupler assembly contains a tension/compression spring, a coupling/decoupling mechanism, two support spreaders, and a strike plate. The contact surface of the strike plate has parallel horizontal grooves that serves as an anti-climb feature that prevents one vehicle from riding up over the other vehicle during collision.

5.2.2 Safety Issues

The aluminum construction for the vehicle structure incorporates known and proven technology. There should be no significant safety issues related to the basic structure.

In order to protect passengers and crew from injury as a result of objects (e.g., birds, projectile, etc.) striking the windows or leading surfaces of the vehicle, Grumman has identified FAA aircraft glazing requirements in addition to FRA glazing requirements.

The control of the opening and closing of the doors uses "checked redundant computers" to resolve a number of door-related hazards. This method is acceptable and a common practice in the commercial aircraft and ground transit industries. However, no software requirements are given by Grumman for the different functions performed by the computers. Since the computers are performing functions that can contribute to Category I and II hazards, stringent software requirements must be defined and included in the software development process.

5.3 PROPULSION, NORMAL BRAKING, AND EMERGENCY BRAKING

5.3.1 System Description

The three-phase AC traction winding is housed in the iron rail along the guideway. The traction winding covers the whole length of the track but only small sections (~ 500 m [1650 ft] long) are energized at any given time. A wave-type winding is selected for averaging out inhomogeneities of field excitation over the length of an active section of the track.

Each LSM is individually supplied and controlled from the substation as shown in Figure 5-3. Each substation supplies 4 km (2.5 mi) length of track on each side; each 4 km length of track winding is subdivided into eight 500 m (1650 ft) sections. The track winding sections are supplied from feeder cable through bipolar thyristor switches.

Braking resistors are connected at the substation end of the feeder to provide electrodynamic braking. Three-phase ac power, supplied from the utility line, is first rectified and inverted to provide power to the motor blocks at desired frequencies. Vehicle speed variations are achieved by increasing or decreasing the frequency of the ac current.

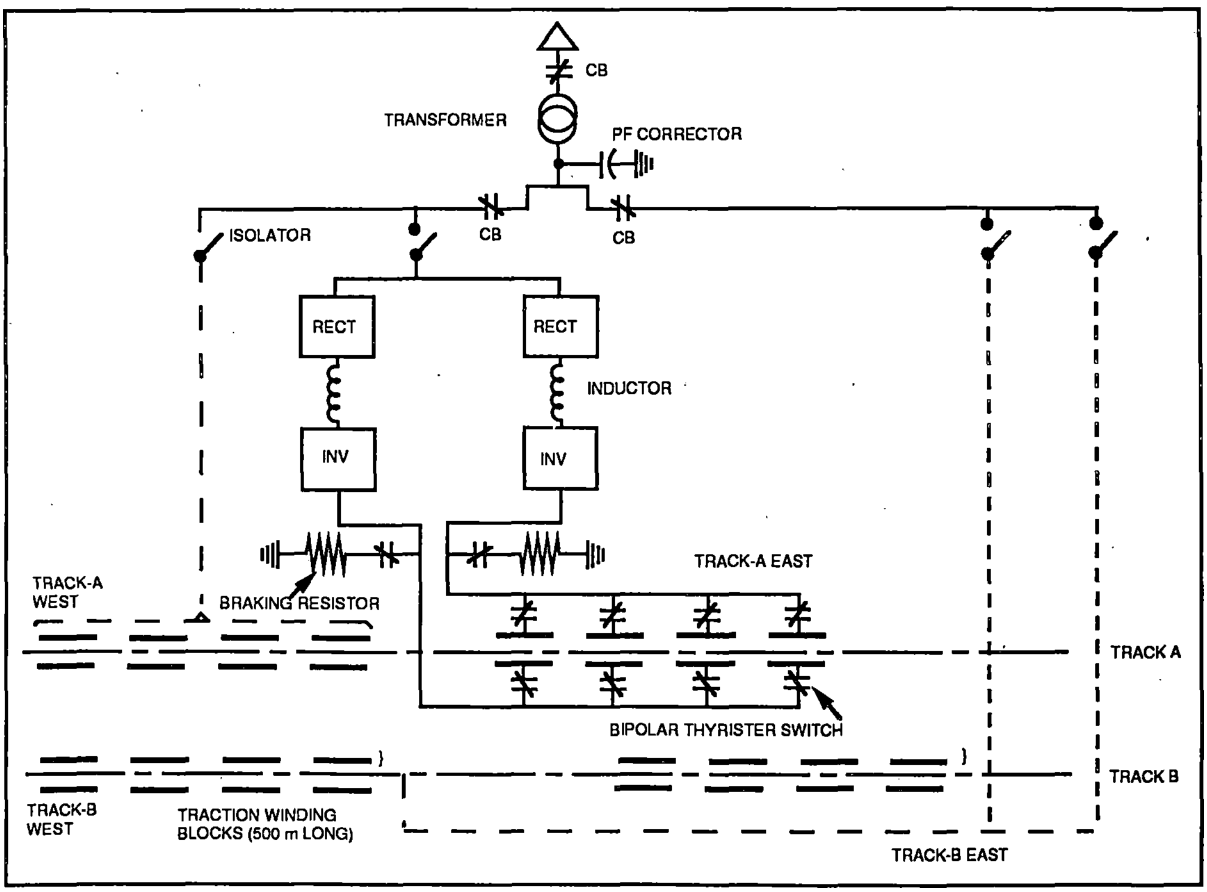


FIGURE 5-3 SUBSTATION EQUIPMENT AND ELECTRICAL SUPPLY CONCEPT

Grumman summarizes the advantages and disadvantages of the braking methods it examined in Figure 5-4. Based on the results, Grumman did not include resistive or aerodynamic brakes in its baseline configuration. The Grumman baseline braking approach is as follows:

- For normal operations, the regenerative approach will be used; and
- During emergency power loss, the eddy current brake in conjunction with a friction brake will be used for the high and low speed regions, respectively.

The friction brake system consists of two pairs of brake assemblies mounted to the chassis structure of each 50-passenger module. The brake assembly consists of a hydraulic actuator that clamps a set of floating shoes (skids) against the two sides of the guideway hat section surface. When inactive, the shoes are held in the withdrawn position by retraction springs.

TYPE OF BRAKE	ADVANTAGES	DISADVANTAGES
1. REGENERATE	CONSERVES POWER BY RETURNING IT TO UTILITY GRID	WILL NOT OPERATE WITH POWER SYSTEM FAILURE
2. RESISTIVE		REQUIRES MANY DISSIPATIVE RESISTORS ALONG FULL LENGTH OF GUIDEWAY AND MUST BE CAPABLE OF BEING ACTIVATED WITH POWER LOSS AND/OR COMMUNICATION LOSS
3. EDDY CURRENT	IS NOT DEPENDENT ON MAIN POWER SOURCE, CAN OPERATE OFF BATTERIES	NOT EFFECTIVE AT LOW SPEEDS
4. FRICTION PADS	IS NOT DEPENDENT ON MAIN POWER SOURCE, CAN OPERATE OFF BATTERIES, CAN BE USED AS PARKING BRAKE	NOT EFFECTIVE AT VERY HIGH SPEEDS
5. AERODYNAMIC	IS NOT DEPENDENT ON MAIN POWER SOURCE, CAN OPERATE OFF BATTERIES.	NOT EFFECTIVE AT LOW SPEEDS; REQUIRES LARGE SURFACE AREAS >15.25 M (>50 FT) TO BE EFFECTIVE.

FIGURE 5-4. GRUMMAN BRAKE COMPARISON

5.3.2 Safety Issues

No inherent safety problems should arise from the Grumman baseline approach to vehicle propulsion and braking. However, the normal mode of electric braking is regenerative and relies solely upon the receptivity of the electric utility power system. The unpredictability of the electric power system may affect the maglev system availability due to loss of the primary braking system. In addition, this would result in the more frequent use of the brake-up braking system.

The back-up braking system consists of the eddy current and friction brake systems which require an independent on-board power source. This power source must be extremely reliable. However, on-board batteries are only mentioned occasionally throughout the SCD; there is no detailed discussion or description of the on-board batteries by Grumman. Accordingly, the battery system will require more detailed analysis during the next phase of concept and design development.

5.4 SUSPENSION, LEVITATION, AND LATERAL GUIDANCE

5.4.1 System Description

A dynamic simulation program was developed by Grumman to show that its baseline vehicle does not require a secondary suspension system. The simulation program evaluates the wide range of maneuvers and disturbances to which the vehicle will be subjected while remaining levitated. The air gap clearance between the magnet's face and the iron rail is controlled by varying the current in the iron core magnet on the basis of gap clearance and vehicle/magnet acceleration measurements. A block diagram of this control loop with its major components is shown in Figure 5-5.

The Grumman conclusions from this gap control system study can be summarized as follows:

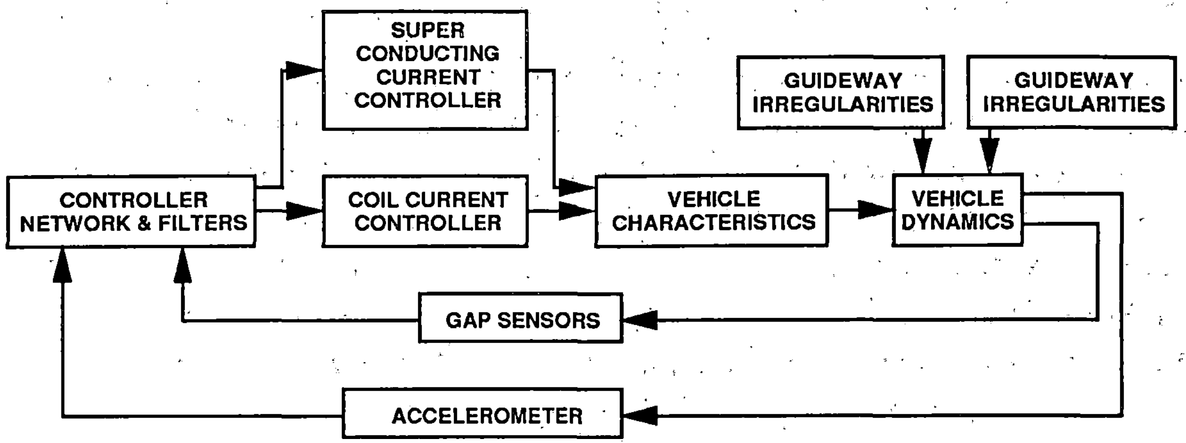


FIGURE 5-5. BLOCK DIAGRAM OF LEVITATION AND GUIDANCE CONTROL LOOP

- The control system bandwidth should be at least ~ 10 Hz to minimize gap errors during vehicle maneuvers.
- A guideway roughness profile has been identified which has a root-mean-square deviation of 0.0042 m (0.16 in) and a statistical range of +/- 0.0125 m (0.47 in) which results in vehicle cabin vibration levels seven times lower then the allowable ISO 1 hr standard.
- A secondary suspension system is not required to provide passenger comfort.
- A step rail variation of +/- 3 cm (1.2 in) can be tolerated on the levitation control system without exceeding current control capability of the normal control coils or the SC coils.

Figure 5-6 illustrates the Grumman magnet design concept. Figure 5-6 (a) shows a cross-section of the vehicle with the iron core magnets and a guideway rail identified in black. The laminated iron cored magnets and iron rail are oriented in a "V" configuration with the attractive forces (F1 and F2) between the magnets and rail acting through the vehicle's center of gravity (cg). Vertical control forces are generated by sensing the gap clearance on the left and right side of the vehicle and adjusting the currents in the control coils, shown in Figure 5-6 (b), to maintain a relatively large 4 cm (1.6 in) gap between the iron rail and the magnet face. Lateral control is achieved by differential measurements of the gap clearance between the left and right sides

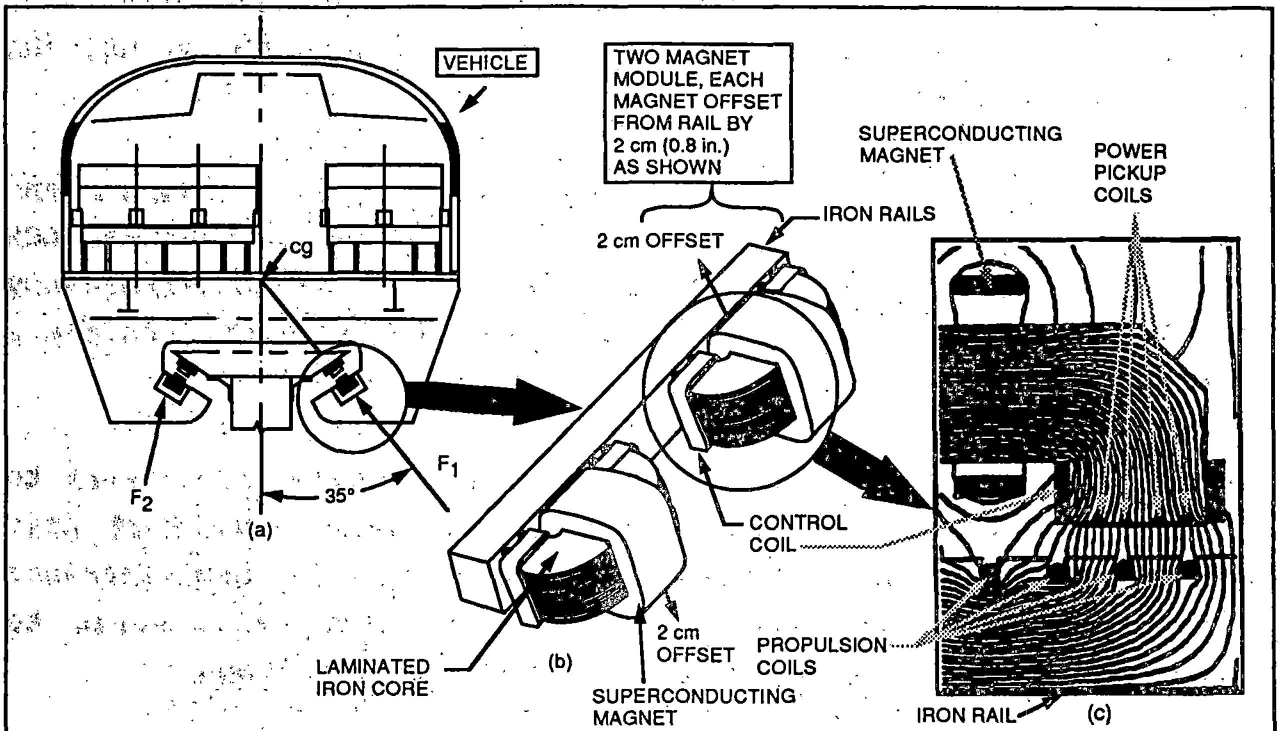


FIGURE 5-6. LEVITATION, PROPULSION AND GUIDANCE SYSTEM

of the vehicle magnets. The corresponding magnet control coil currents are differentially driven for lateral guidance control. There are 48 magnets, 24 on each side of a 100-passenger vehicle-pair. In this manner, control of the vehicle relative to the rail can be achieved in the vertical, lateral, pitch, and yaw directions. The control of vehicle roll attitude is discussed below.

Two magnets combined, as illustrated in Figure 5-6 (b), make up a magnet module (MM). Each magnet in a MM is "C" shaped, consisting of a laminated iron core with a superconducting (SC) coil wrapped around the center body of the magnet, and two copper control coils wrapped around each leg. Vehicle roll control is achieved by offsetting the magnets in an MM to the left and right side of a 20 cm (8 in) wide rail by 2 cm (0.8 in). Control is achieved by sensing the vehicle's roll position relative to the guideway and differentially driving the offset control coils to correct for roll errors. The total number of loops required for complete control of a 100-passenger vehicle-pair is 26 (one for each of the 24 MMs and two for roll control).

The iron rail shown in Figure 5-6 (b) is also laminated and contains slots for the installation of a set of three-phase LSM propulsion coils. The coils are powered with a variable frequency variable amplitude current that is synchronized to the vehicle's speed.

The Grumman magnet design uses SC iron core magnets in contrast to copper coils in existing EMS systems. Grumman states that this will allow them to operate with a large 4 cm (1.6 in) gap clearance without paying a heavy weight and power penalty that would be required if copper coils were used for the same purpose.

According to Grumman, the use of an iron core with the SC coil provides an added advantage. The magnetic flux is primarily concentrated in the iron core, not in the SC coils as in the case of an air-core system. This reduces the flux density and loads in the SC wire to relatively low values (<0.35 Tesla and ~17.5 kPa, respectively). In addition, Grumman has stated that the implementation of a constant current loop controller on the SC coil will diminish rapid current variations in the coil, minimize the potential for SC coil quenching, and allow for the use of state-of-the-art SC wire.

In summary, Grumman states that the use of SC iron-cored magnets results in a significant number of advantages:

- Large gap size - 4 cm (1.6 in)
- Low magnetic fields in superconducting coil - <0.35 T
- Low magnetic fields in passenger cabin - <1.0 gauss dc
- Low load forces in superconducting coil - ~17.5 kPa
- State-of-the-art superconducting wire - 0.65 mm (0.026 in) diameter (used in Relativistic Heavy Ion Conductor Program)

- Lower weight than copper coil system - ~80% reduction per magnet.

The "dead vehicle" handling wheels consist of two groups of wheels per 50-passenger module. Each wheel group is comprised of two sets of tires normally retracted above the chassis skid ground line. When extended, the wheels raise the vehicle to its nominal levitated height. This system can be used to maneuver and support the vehicle during maintenance and position it for initial levitation. The system can also be used to tow or push the vehicle when levitation is lost.

Grumman uses liquid helium to cool its superconducting magnets. Its design includes storing liquid nitrogen and liquid helium locally in each magnet. Reservoirs are provided under the magnets for this purpose. Each individual cryostat carries enough liquid helium and nitrogen to sustain the superconductor for at least 24 hours.

The helium system consists of the magnets interconnected in series with transfer lines for filling. Each magnet is outfitted with a fill and return line and a vent line for the helium gas. In the event of a quench, any high pressure warm helium is vented out of the system. The pressure and liquid flow regulation is accomplished automatically using feedback from liquid level sensors and pressure monitors. In addition to the liquid helium circuit, there is a separate liquid nitrogen circuit that includes foam insulated liquid nitrogen transfer lines. The nitrogen circuit feeds the magnets in series from a central reservoir. The nitrogen circuit is an open cycle system which the liquid nitrogen is allowed to vaporize and escape to the atmosphere.

Grumman provides the capability of tilting the vehicle passenger compartment by +/- 9 degrees relative to the guideway. This design allows for coordinated turns up to +/- 24 degree banking (+/- 15 degrees in the guideway and +/- 9 degrees in the vehicle). Grumman states this capability will assure that all coordinated turns can be performed at the appropriate tilt angle independent of the speed with which the vehicle is traversing the turn, as well as allowing for high-speed off-line switching. If the vehicle were to come to a stop on a horizontal curve, banked 15 degrees, the vehicle's tilt system is designed to counterbalance the guideway super elevation up to nine degrees, reducing the passenger cabin floor to a six degree tilt.

Figure 5-7 shows major components of the tilt mechanism. A sensor package located in the cabin senses lateral acceleration and provides the input to the tilt system. The package will contain several accelerometers and a sensor logic system to guarantee fail-safe operation, according to Grumman. The sensor will detect any lateral accelerations (i.e., as the vehicle enters a horizontal curve) and will generate a command to drive the tilt system in a direction that will null the signal.

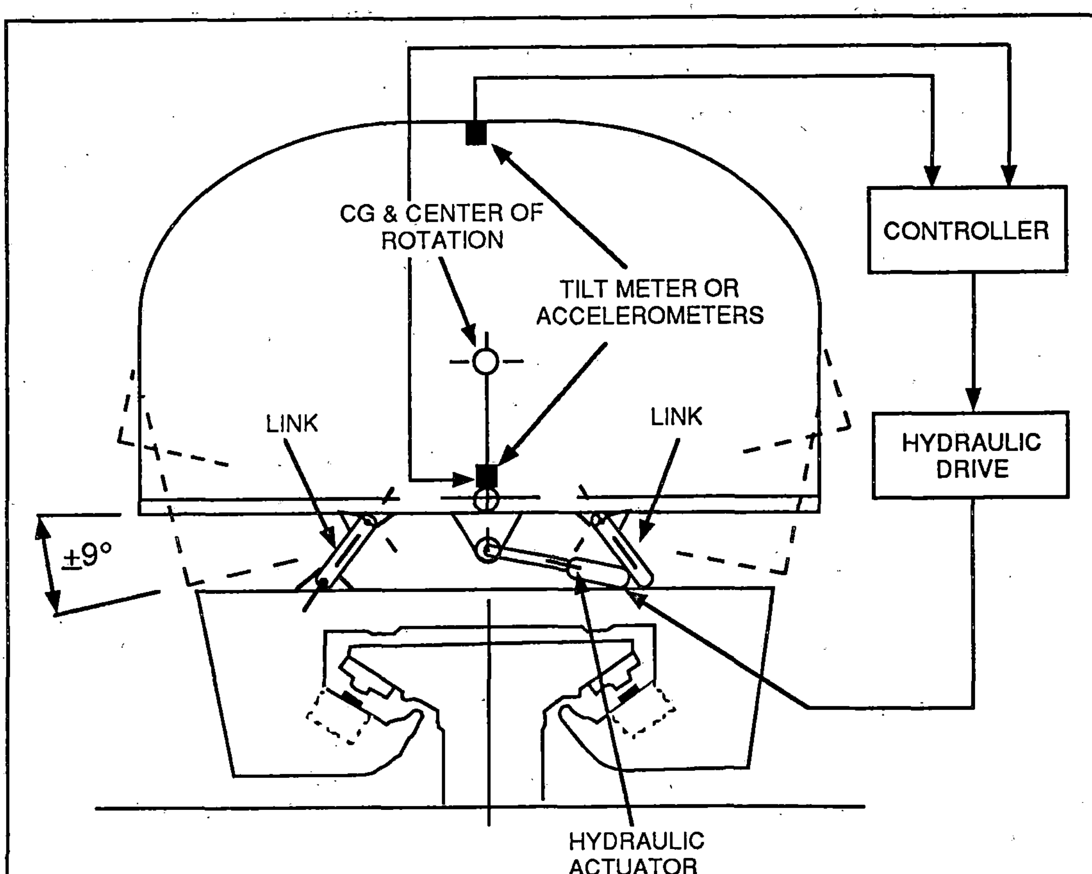


FIGURE 5-7. TILT MECHANISM APPROACH

5.4.2 Safety Issues

The lack of a secondary suspension system may lead to excessive vibration loads on the vehicle structure. This ultimately could lead to premature fatigue; therefore, the operating stress levels need to be confirmed during a prototype testing program. On-board cryogenic systems have potential Category I and II hazards that should be identified and mitigated during the preliminary design phase. They include the effects of "cold" burns, cryogenic oxygen deficiency, and materials embrittlement. These hazards are applicable for Foster-Miller as for the other SCDs and have been described in detail in Section 3.4 of this report.

A large number of hazards relating to the suspension, levitation, and tilting systems are resolved in the Grumman PHA by the use of "checked redundant computers." This approach is considered satisfactory, but, as noted previously, no software requirements are given for the different functions performed by the computers. This area will require more attention during the next phase of concept and design development.

5.5 ON-BOARD POWER SYSTEM

5.5.1 System Description

The Grumman vehicle electrical systems will require approximately 170 kw. Grumman acknowledges that supplying this power without a direct electrical contact is a challenge but has not yet established a baseline approach. One concept Grumman proposes is to use pickup coils operating on one of the larger harmonics of the traction motor pole pitch. However, the voltage and frequency generated by these coils is a linear function of the vehicle speed, resulting in a reduction of power at low speeds.

On-board batteries are mentioned occasionally by Grumman as providing emergency power for several vehicle functions. However, Grumman does not provide a detailed discussion or description of the batteries.

5.5.2 Safety Issues

Grumman states that additional study of supplying power to the vehicle is necessary and will be a major focus of future design efforts.

If all power has been lost, the vehicle must be capable of providing emergency braking. The emergency braking systems Grumman has proposed require the availability of an on-board battery system. Grumman has not sufficiently described the architecture of such a system to meet the extremely high reliability requirements.

5.6 MAGNETIC SHIELDING

5.6.1 System Description

Grumman states that the EMS type maglev system is very similar in power generation and distribution to other electrified urban transit and intercity rail transportation systems; the electromagnetic field (EMF) emissions are expected to be no greater than existing electrified systems. The Grumman system also incorporates iron core magnets and iron rails to concentrate the magnetic flux in the iron, thus minimizing the magnetic field to the passengers and the external environment.

Figure 5-8 identifies constant flux densities in the cabin and station platform that Grumman expects for its design. Flux density levels below the seat are expected to be less than 1 gauss. On the platform, magnetic levels are not anticipated to exceed 5 gauss. This data is based on a three-dimensional magnetic analysis program and assumes no shielding. Similarly, ac magnetic fields also are anticipated by Grumman to be within 0.1 mT for frequencies above 25 Hz and 0.01 mT for frequencies above 140 Hz with no shielding. With local steel shielding, both ac and dc levels could be further reduced.

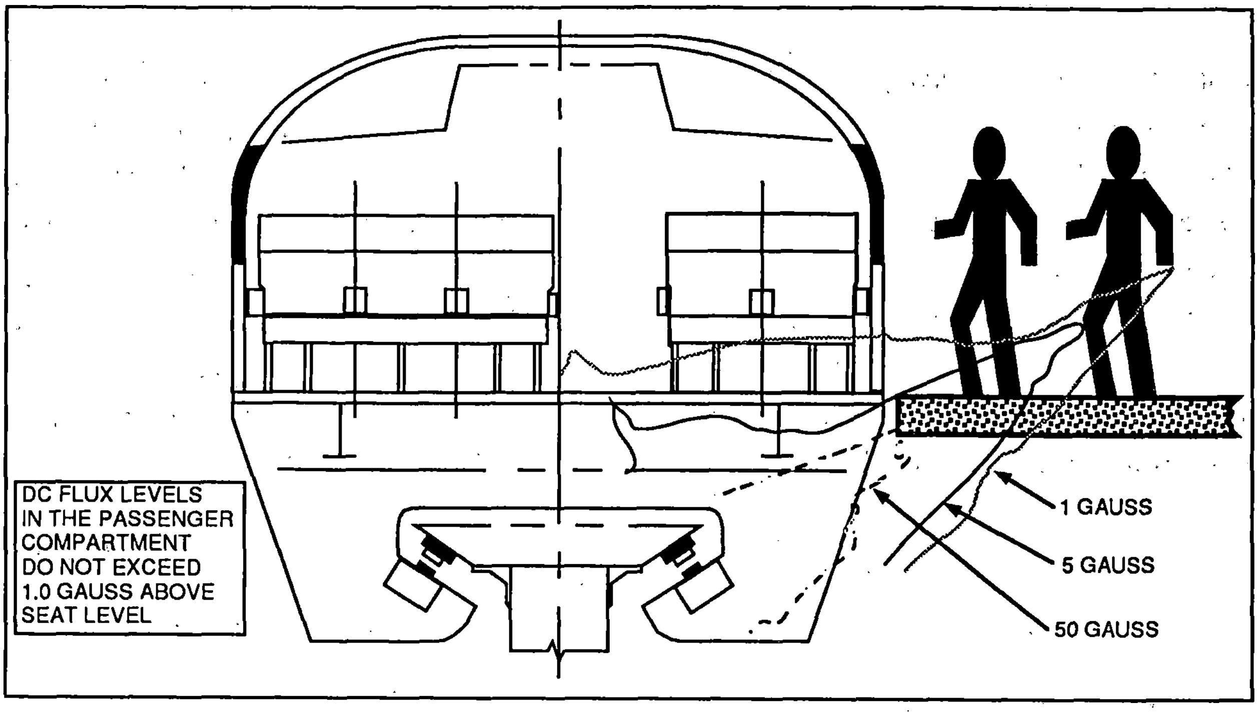


FIGURE 5-8. GRUMMAN ESTIMATED MAGNETIC FIELDS IN PASSENGER CABIN AND SURROUNDING AREAS

5.6.2 Safety Issues

Although a universal safe level for passenger exposure to ac and dc fields has not been determined, the SCD SOW set goals of 50 gauss, 5 gauss, and 1 gauss levels for dc, and 1 gauss and 0.1 gauss for ac. If the electromagnetic fields are discovered to be higher than Grumman estimates during the next phase of concept and design development, shielding may be required on and around the vehicle.

Such shielding would be required to be fail safe, and will add weight to the vehicle, affecting the trade-off analyses performed by Grumman.

5.7 FIRE PROTECTION

5.7.1 System Description

Grumman's philosophy on fire protection is that it is necessary to consider fire prevention, containment, detection, and suppression. However, the SCD does not provide any significant design discussion on specific applications. Grumman does discuss the use of fire-resistant materials and proper equipment placement as key design considerations to preclude the initiation of a fire as well as its spread; the use of fire/smoke detectors and fire extinguishers is also mentioned. Grumman listed the following items as potentially applicable sources of requirements for fire protection:

- Federal Register, Volume 54 - materials selection (for intercity and commuter trains)
- Amtrak Spec No. 352 - flammability, smoke emission, toxicity
- Amtrak Spec No. 323 - wire insulation
- NFPA 130 - vehicles
- FAA, 49 CFR, Part 25 - aircraft

5.7.2 Safety Issues

While the SCD references several fire safety-related documents, Grumman does not provide any significant design discussion on specific applications to prevent fires from occurring. The SCD text mentions fire-resistent materials. However, while the PHA identifies fire hazards, the control provisions indicated focus on fire detection and suppression; fire prevention through the use of materials is not included in the analysis. In addition, methods for monitoring, detecting, and suppressing fires in isolated, unstaffed wayside equipment are not discussed and should be evaluated.

5.8 GUIDEWAY DESIGN

5.8.1 System Description

The guideway consists of slender inverted V-shaped sections mounted to a 27 m (89 ft) main beam by outriggers every 4.5 m (15 ft). The main beam is in turn supported by a conventional pier on piled or spread footings.

A number of different guideway designs were investigated by Grumman. In each case, the Grumman design mandated that a center platform exist along the full length of the guideway to provide a safe exit for the passengers and crew, in case of an emergency, such as fire or smoke in the cabin. Escape ladders from periodic column locations are provided. The "spine girder" (outrigger) configuration shown in Figure 5-9 was chosen as the baseline. **Additional discussion of the guideway emergency evacuation-related features is presented in Section 7.3 of this report.**

5.8.2 Safety Issues

The proposed Grumman guideway incorporates a vehicle wraparound design providing additional safety to the system by inherently preventing "derailments." Also, by providing a center platform along the entire length of the guideway, it is not a requirement that the vehicle proceed to a "safe stopping zone" in the event of an emergency. This will result in faster evacuation from the vehicle if required.

5.9 GUIDEWAY SWITCH

5.9.1 System Description

Grumman states that its design provides the capability of high-speed off-line switching. Two sections of track are moved with one actuator motion 3 m (10 ft) laterally. Each section is 60 m (196.9 ft) long. Details of the Grumman track switching concept are illustrated in Figure 5-10. It identifies the two sections of the

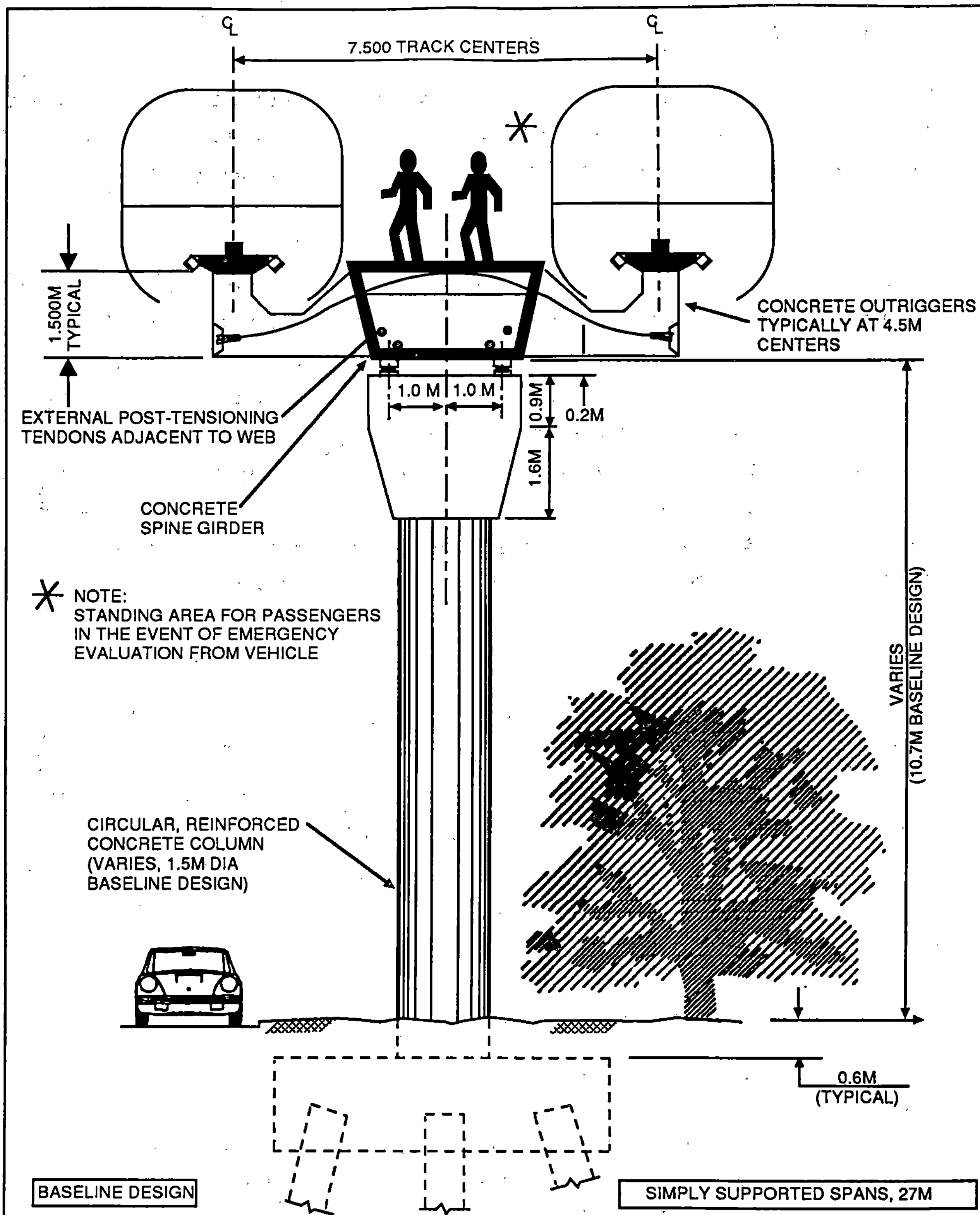


FIGURE 5-9. GRUMMAN BASELINE DESIGN TANGENT TRACK

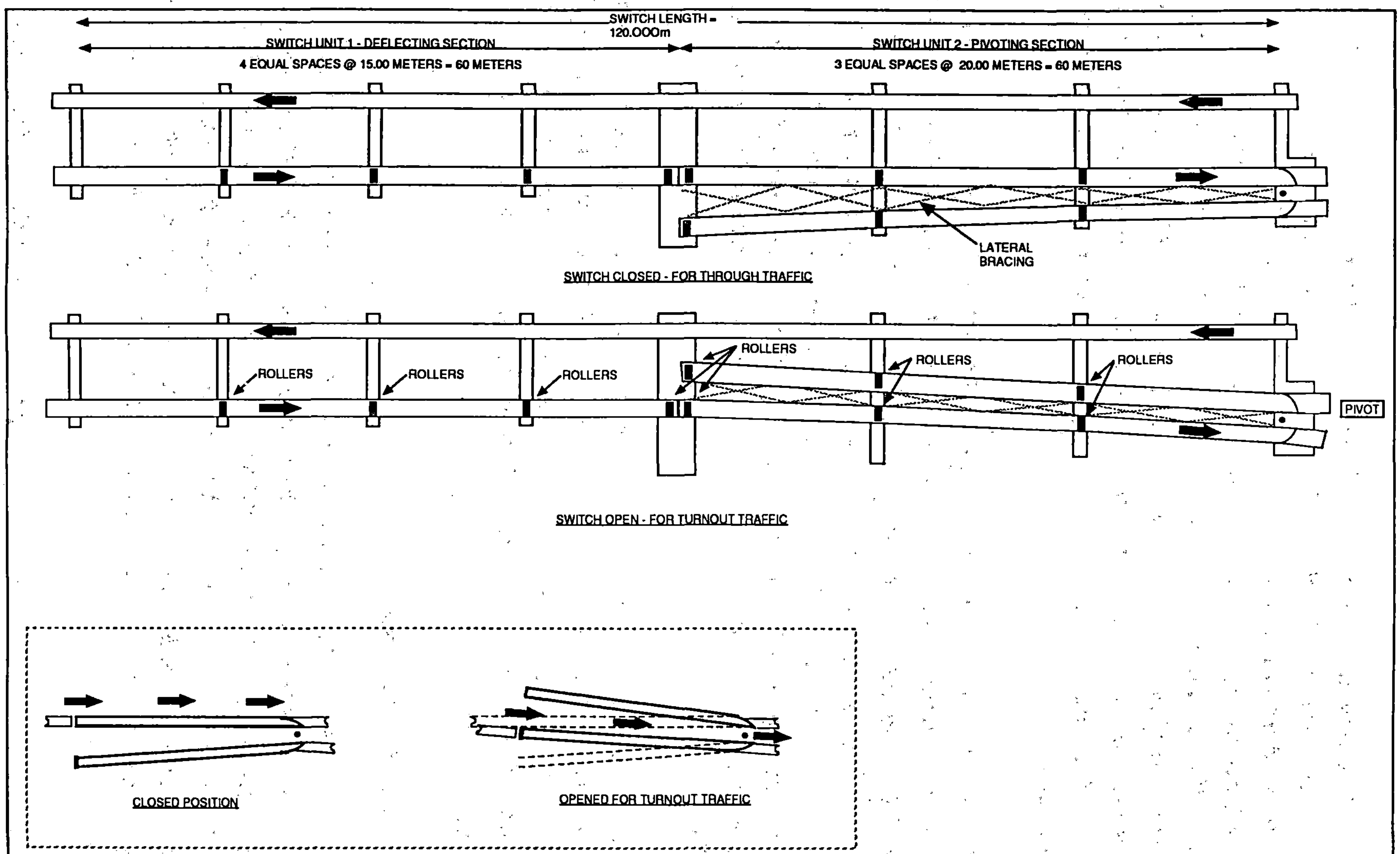


FIGURE 5-10. GRUMMAN SWITCH LAYOUT

track that are moved to accomplish this function. The upper figure shows the through traffic condition for the track switch. The lower figure identifies how the 60 m long switch, Unit 1, is flexed to a curved section, while the right hand 60 m long switch, Unit 2, is pivoted about the fixed switch points. This combined motion of the two sections (120 m [394 ft]) total length) provides a proposed turnout speed of 65 m/s (143 mph). Grumman estimates the normal operating cycle of the switch, to open or close, will be about 25 to 30 seconds.

Movement of the bending track will be controlled by a pair of hydraulic cylinders. Each cylinder will be sized so that a single cylinder will operate the section if the other cylinder is inoperable. Similar to the bending section, the pivoting section is actuated using a pair of hydraulic cylinders, each capable of completing the pivot movement alone. Both the bending and the pivoting tracks will return to their original (straight) shape when released.

The Grumman design uses mechanically operated locking bars to align the switch sections, either for the switch-open or switch-closed position. The lock bars will be driven from the ends of the bending section into the end of the pivoting section to ensure correct alignment.

5.9.2 Safety Issues

The baseline switching concept proposed by Grumman should not have any inherent safety issues that have not been recognized and addressed in similar applications. The primary difference in Grumman's proposed design is the higher operating speeds of the vehicles. The switch operating speed and the allowable vehicle speed through a switch may become factors in establishing safe headways.

The design of a closed-loop sensor system to detect proper position of the guideway switches is recommended as a control provision for several switch-related hazards. However, there is no detailed discussion or description of the switch position sensors by Grumman. The sensor systems that have the authority to cause the vehicles to stop must be designed to have a very low probability of false alarms. Frequent unnecessary disruptions to normal operations are themselves safety hazards.

5.10 GUIDEWAY MONITORING

5.10.1 System Description

Grumman has divided the guideway monitoring task into two categories: guideway integrity sensing and right-of-way sensing. Guideway integrity requires measuring misalignments of a fraction of an inch, and detecting internal cracks or other structural failures of the structure. Right-of-way sensing is looking for larger objects, particularly foreign objects, that are on or near the guideway, and range in size from a few inches to very large objects.

Grumman states that a combination of electrical and magnetic sensing approaches is the most reliable and cost effective combination to monitor guideway integrity.

The first approach uses electrical resistance measurement of the laminated rails to sense breaks in the track. This approach has the advantage of continuous monitoring of the entire length of track. Pairs of tracks are connected as arms of an electrical Wheatstone bridge to compensate for common-mode temperature differences on the rails. Breaks or cracks in the rail will show up as an increase in rail resistance. To attempt to ensure that all laminates are monitored by this technique, ac voltage excitation will be tested in an attempt to electrically connect all laminations by capacitive coupling.

A second approach to measuring joint misalignments uses magnetic principles. Using an electrical coil or the ambient earth's magnetic field, a linear magnetic field is imposed across the track joint between sections. Discontinuities due to joint misalignments will cause an angular shift in the field lines. A magneto resistive (MR) sensor chip is positioned to sense the angular shift and infer misalignment.

Grumman's baseline right-of-way sensing system is the range-gated TV system, based on its excellent poor weather performance and moderate cost. In this method, an illuminator - a diode laser array, is pulsed once per frame of image time. A fast responding image valve, such as a gated intensifier or Kerr cell, only lets a small segment of return through, in the nature of a radar or lidar system. By such "range gating," the image is collected from only a selected portion of the area illuminated by the laser pulse. The result is dramatically reduced backscatter under heavy fog, snow, and/or rain. In fact, Grumman states that most of the back scattered energy in active systems in bad weather is in the first few meters. The image is gated off while this energy is back scattered, and only energy several meters away or beyond ever is imaged in the system, the near area being monitored by the previous sensor post.

5.10.2 Safety Issues

None of the three above-mentioned systems are in existence today. The range-gated system was developed by the military to some degree but would not support the tighter range gates desirable in the maglev sensing application. A stringent development program would need to be designed and implemented on all three proposed systems to demonstrate the reliability of the guideway monitoring systems. Further study of the ability to stop a vehicle short of an identified hazard is also needed.

In addition, the Grumman PHA and the SCD text do not recommend any reliability/redundancy design approach for the guideway monitoring systems, although the hazards associated with the systems are classified as Category I events.

5.11 POWER SYSTEM AND DISTRIBUTION

5.11.1 System Description

Each substation is sized to supply power to 8 km (5 mi) of double track. Each 8 km length of track winding is subdivided into sixteen 500 m (1650 ft) sections. The track winding sections are supplied from feeder cable through bipolar thyristor switches. Three-phase ac supplied from the utility line is first rectified and inverted to provide power to the motor blocks at desired frequencies. Vehicle speed variations are achieved by increasing or decreasing the frequency of the ac current.

5.11.2 Safety Issues

Grumman recognizes that the dependence of train control and operation on the wayside power source is a safety issue. The power semiconductor devices in the wayside rectifiers, the stator switches, and the variable voltage/variable frequency power sources may be required to operate in an exposed environment and at current, voltage, and switching levels exceeding the present state-of-the-art. Again, a stringent development program should be designed and implemented on the proposed system to demonstrate the reliability of the power distribution system.

A redundancy technique for the stator switch design is recommended by Grumman as a control provision for the hazard of inability to remove guideway power. Grumman states that this is a Category I hazard and could result in a collision between trains. However, there is no detailed discussion or description of stator switches in the SCD.

5.12 COMMUNICATIONS, COMMAND, AND CONTROL

5.12.1 System Description

The communications, command and control (C^3) system provides a highly-automated means for effectively monitoring and managing the overall operation of maglev vehicles and related support systems under normal, abnormal and emergency conditions. The Grumman C^3 system is divided into five subsystems by function.

The C^3 system will be responsible for supervisory tasks, for scheduling and routing of vehicles, for managing the regional control systems, for collecting and storing necessary system data, for monitoring overall system status and for adjusting global network parameters.

The principal duty of the Regional Control Center (RCC) is reliable handling of the power distribution network that drives the vehicles. Each regional system will have primary responsibility for managing the power substations and power distribution network within its region. All power distribution functions from circuit switching and voltage regulation to switching of gate-turn-off thyristors for vehicle acceleration or braking will be managed at the regional control level. Each regional system will also have diverse communications responsibilities; it will communicate with all vehicles in its region, with Central Control, and with adjacent regional systems to coordinate hand-off of vehicles.

The Vehicle Communications (Vecom) System is the communication link between the vehicles and the rest of the network. It consists of an array of antennas, transceivers, computers, and cables fixed to the guideway and antennas and transceivers attached to the vehicle. Each individual vehicle will be capable of autonomous control of all its functions except for propulsion. Some specific examples of individual vehicle control functions: levitation electromagnets, hydraulic system, cryogenic system, interior environment, onboard communication systems, onboard braking system, onboard emergency systems.

The Integrity, Safety, and Security (ISS) System is discussed in section 5.10, Guideway Monitoring, of this report.

The Utility Communication System (UCS) supports all remaining (non-vital) communications functions. Because these functions are nonvital, Grumman elected not to include them in its SCD.

Figure 5-11 identifies the major components being monitored by the on-board Instrumentation and Control system. The primary purpose of this system is to display to the crew and the central control station the condition and status of critical onboard equipment including information that an automatic backup replacement of a component by the onboard computer was implemented. Figure 5-12 lists each of the subsystems identified in Figure 5-11. Figure 5-12 shows the function of each subsystem to be monitored and prioritizes failures into one of three basic categories:

- Category 1 - High priority failure; identifies that an automatic backup system has been implemented, will require immediate service attention upon completion of run.
- Category 2 - Moderate priority failure; an automatic backup system has been implemented and will require service attention in the near future.
- Category 3 - Low priority failure; requires no automatic backup, but will require attention in the near future.

The Grumman structure for the data links between the four vital subsystems with fault tolerance allowances is represented graphically in Figure 5-13. The Grumman baseline system uses hardware redundancy to achieve a fail-safe status; self-checking pairs are planned for use in all the data links except for the RCC x to Vecom interfaces.

5.12.2 Safety Issues

The reliability requirements of systems whose failures could result in the loss of human life are very demanding, and such failure conditions must be extremely improbable. Grumman proposes the use of checked redundant computers to control a large number of safety-critical C^3 functions. As mentioned before, this method is

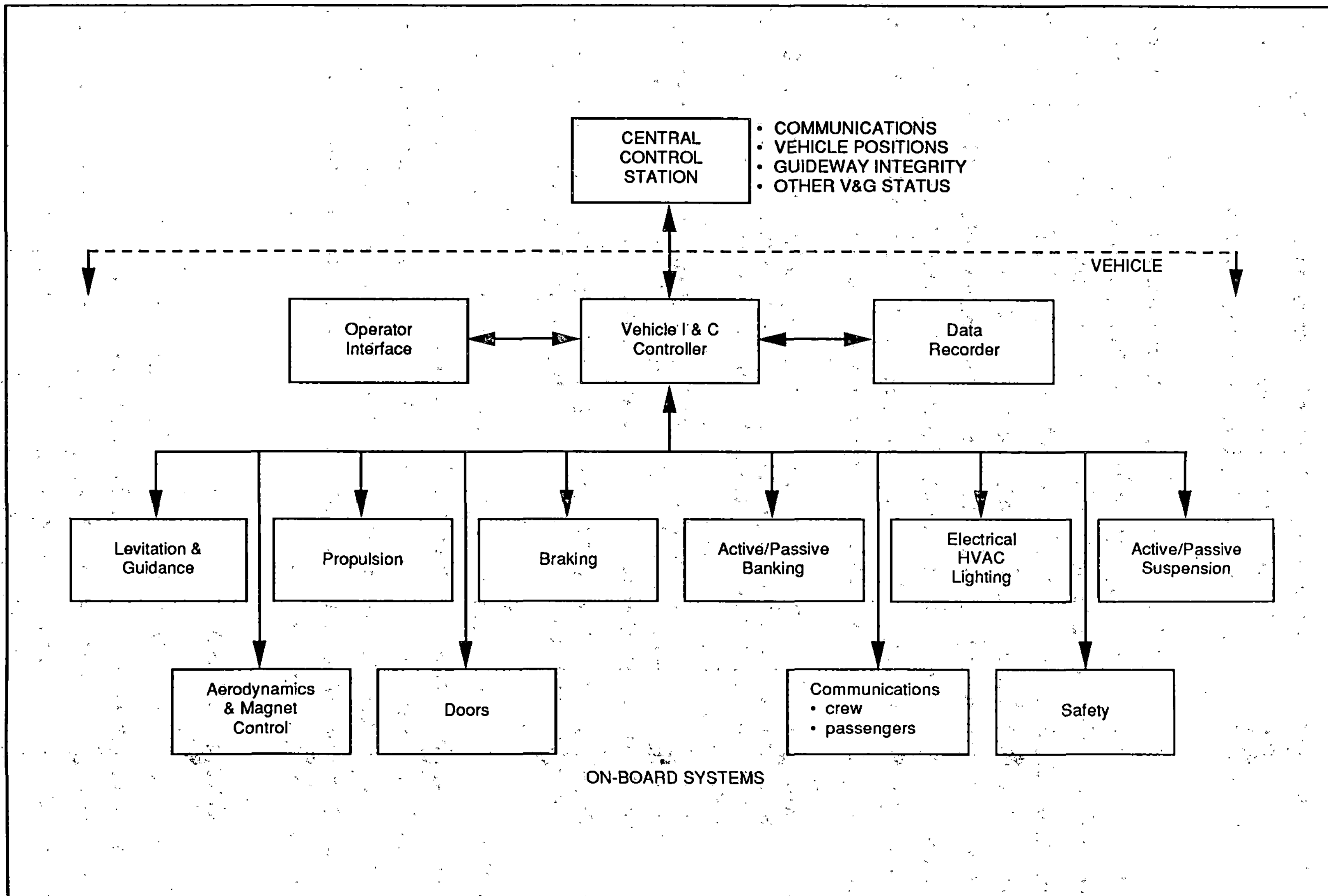


FIGURE 5-11. GRUMMAN VEHICLE INSTRUMENTATION AND CONTROL SYSTEM

SUBSYSTEM	FAILURE SENSED	PRIORITY
• LEVITATION & GUIDANCE	• LOSS OF SC COIL CURRENT • CONTROL CURRENT LOSS • HELIUM COMPRESSOR • COMPUTER • GAS SENSOR • ACCELEROMETER	1 1 2 2 2
• PROPULSION	• NOT APPLICABLE TO VEHICLE	—
• BRAKING	• HYDRAULIC PRESS. LOSS • ACTUATOR FAILURE • HYDRAULIC PRESS. • DECELERATION SENSORS • COMPUTER	1 1 2 2 2
• ACTIVE BANKING	• TILT METER • HYDRAULIC PRESS. LOSS • COMPUTER	2 1 2
• ELECTRICAL	• POWER PICKUP • A/C SYSTEM	2 2
• PASSIVE SUSP.	• NONE REQUIRED	—
• DOORS	• HYDRAULIC PRESS. LOSS • OPEN DOOR SENSOR	1 2
• SAFETY	• FIRE/SMOKE ALARM	2
• COMMUNICATION	• VOICE COMM. WITH CCC	3

FIGURE 5-12. GRUMMAN PRIORITY LEVEL

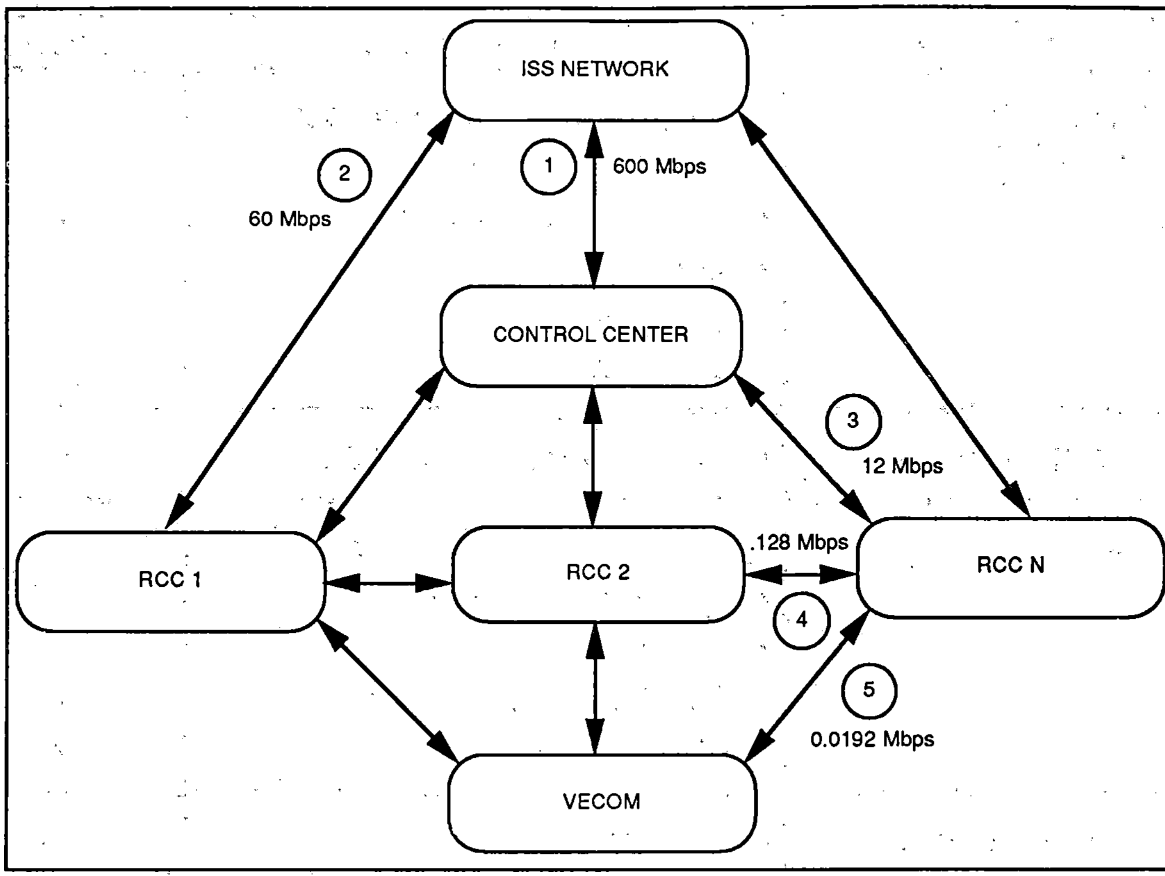


FIGURE 5-13. VITAL CHANNEL THROUGHPUT REQUIREMENTS WITH FAULT TOLERANCE

acceptable in the transportation industry, but stringent software requirements should be defined and included in the software development process.

The design of a vehicle position measurement system in the stations is recommended by Grumman as a control provision for the hazard of the train not stopping/positioning properly in the station. Grumman states that this is a Category II hazard and could result in injury to passengers while boarding or deboarding. However, there is no detailed discussion or description of this system in the SCD.

5.13 SYSTEM OPERATIONS AND MAINTENANCE ISSUES

5.13.1 System Description

Grumman analysis has shown that ninety-second headways using the 100-passenger baseline vehicle configuration are necessary to provide the minimum passenger-per-hour capacity of 4000.

The Grumman maintenance program will be divided, based on schedules and hierarchy of function, into daily, weekly, monthly, and yearly inspection and servicing activities to ensure the integrity of the infrastructure, subsystems, and structural components. Grumman has identified several subsystems requiring maintenance priority including the C^3 system, batteries, helium coolant system, superconducting magnets, and the vehicle speed verification system.

5.13.2 Safety Issues

Grumman states the importance of a structured and systematic maintenance program to the high operational integrity of the maglev system. As the design progresses, specific tasks need to be identified and categorized by applicable inspection intervals.

Grumman also recognizes that the high operating speeds and consequences of component failures will dictate a higher percentage of completed scheduled maintenance than would be experienced in rail systems. In this respect, it would be similar to the airlines, with a more stringent training requirement for maintenance crews and verification of completed tasks.

5.14 ENVIRONMENTAL EFFECTS

5.14.1 Environmental Considerations

Routes that are primary candidates for maglev systems in the United States provide a broad range of climatic conditions involving high and low temperatures, wind, rain, snow, ice, earthquakes, fog, lightning, dust, and sand.

Low temperatures should not have an operational impact on the Grumman system because it is designed to operate at -29° C(+20° F), which is considerably below the typical low temperature experienced in candidate routes.

The Grumman design has a 0.10 m (4 in) levitated clearance between the vehicle and the guideway track. Grumman asserts that this clearance will be adequate for most moderate snow falls. During frequent operations, accumulation on the track will be limited by the passing vehicle blowing the snow away. When infrequent operations allow heavy snow accumulations, a special maglev snow plow vehicle will be employed and operations restricted by requiring a reduction in vehicle speed. Also, due to the high thrust capability of the propulsion system, Grumman states that the standard front cars will be capable of plowing snow off the top of the track while operating at a slow speed.

In freezing rain conditions, icicle accumulation on the sides of the track will be prevented by providing a heavy armored leading edge on the front car that will knock off icicles. If emergency braking is needed during ice conditions, the on-board eddy current brakes will still be effective since they are non-contact in nature. The friction brakes will be somewhat effective, but with reduced braking capability. Thus, it will be necessary to reduce the operating speeds to provide for sufficient braking distance as deemed necessary.

The proposed Grumman maglev system is designed for operation in steady side winds up to 23.3 m/s (50 mph), head winds up to 13.2 m/s (30 mph), and gusting up to 33 m/s (75 mph). Grumman states its design will result in minimal impact from most wind conditions, since the levitation magnets and the associated control system is designed to adjust to these wind forces. Operations may have to be delayed or temporarily suspended during severe wind or wind gust conditions (i.e., exceeding the design limits).

The proposed Grumman guideway structure is designed to accommodate a rain rate of 5.08 cm (2 in)/hr by providing appropriate drainage and by not building in any "true" horizontal surface that could allow standing water.

The proposed Grumman guideway structure is designed to meet seismic performance category B (i.e., areas with an acceleration coefficient up to 0.19 g), applicable for potential Northeast Corridor routes.

With an elevated guideway which is not accessible to the public, operation during heavy fog should not have any major impact on maglev operations and safety, since the command and control and route integrity systems will have the capability to automatically sense and respond to any foreign obstruction on the guideway.

The Grumman design will include a metallic grid or mesh in the external surface of the vehicle and static dissipaters similar to those incorporated in aircraft. Safety-critical electronic components on the vehicle and the guideway will be protected by proper shielding and grounding techniques.

5.14.2 Safety Issues

The relative importance of environmental effects will depend primarily on the operating region of the maglev system.

If the Grumman maglev system is built in the Northeast, snow and ice will have the greatest impact. This would require a closer examination of the proposed methods of dealing with snow and ice. If the maglev system does not operate at night, the proposed snow plow vehicle must be employed each morning after a snowfall, possibly resulting in an impact on operations. However, with the Grumman guideway design, the accumulation of ice and snow is not expected to be a major problem, since it will be pushed off the guideway during normal operations.

If the Grumman maglev system is built in a high-intensity ground-shaking area such as California, category C and D design specifications (i.e., areas with an acceleration coefficient above 0.19 g) would be required. This would require some revisions in the present guideway design to accommodate these more stringent requirements.

5.15 SUMMARY OF FINDINGS - GRUMMAN

The Grumman approach to safety during system concept definition is consistent with MIL-STD-882B. The approach was systematic and extensive with the main activity being the preparation of a Preliminary Hazard Analysis (PHA).

The interfaces between safety, human factors, reliability, and maintenance activities are handled appropriately. The reliability program plan made good use of the PHA data, recommending design approaches to reduce the probability of the occurrence of identified potential hazards.

Grumman conducted a comprehensive PHA to identify approximately 150 potential hazards and rated their severity on the definitions provided in MIL-STD-882B. A control provision is recommended for each hazard, and the design feature is identified that has been or will be incorporated into the baseline design. The majority of the recommended control provisions in the PHA are discussed and described in the SCD; however, several safety-related issues remain. These are discussed in previous sections and are summarized in the rest of this chapter.

On-board batteries are mentioned occasionally throughout the SCD as providing emergency power for several vehicle functions, including emergency braking. However, there is no detailed discussion or description of the batteries in the SCD. Grumman has not sufficiently described the architecture of such a system to meet the extremely low probability requirements of a Category I event. A large number of hazards relating to the suspension, levitation, tilting, and C^3 systems are resolved in the Grumman PHA by the use of "checked redundant computers." This method is acceptable and a common practice in the commercial aircraft and ground transit industries. However, no software requirements are given by Grumman for the different functions performed by the computers. Since the computers are performing functions that can contribute to Category I and II hazards, stringent software requirements must be defined and included in the software development process.

A closed-loop sensor system to detect the proper position of the guideway switches is proposed by Grumman as a control provision for several switch-related hazards. However, there is no detailed discussion or description of the switch position sensors. The sensor systems that have the authority to cause the vehicles to stop must be designed to have a very low probability of false alarms. Frequent unnecessary disruptions to normal operations are themselves safety hazards.

Grumman provides an extensive discussion of its proposed methods for monitoring guideway integrity and right-of-way. However, none of the three proposed systems, electrical resistance measurement, magnetic sensing, or range-gated TV, are in existence today. A stringent development program should be designed and implemented on all three proposed systems to demonstrate the reliability of the guideway monitoring systems. Further study of the ability to stop a vehicle short of an identified hazard is also needed. In addition, the Grumman PHA and the SCD text do not recommend any reliability/redundancy design approach for the guideway monitoring systems although the hazards associated with the systems are classified as Category I events.

Grumman addresses fire hazards by listing some potentially applicable sources of requirements for fire protection. Grumman's philosophy on fire protection is that it is necessary to consider fire prevention, containment, detection, and suppression. However, the SCD does not provide any significant design discussion on specific applications. Methods for fire prevention, detection, and suppression in system equipment and facilities other than the vehicles should also be evaluated, particularly unstaffed wayside locations which may require automatic systems.

A redundancy technique for the stator switch design is recommended by Grumman as a control provision for the hazard of inability to remove guideway power. Grumman states that this is a Category I hazard and could result in a collision between trains. However, there is no detailed discussion or description of stator switches in the SCD.

The design of a vehicle position measurement system in the stations is recommended by Grumman as a control provision for the hazard of the train not stopping/positioning properly in the station. Grumman states that this is a Category II hazard and could result in injury to passengers while boarding or deboarding. Again, there is no detailed discussion or description of this system in the SCD.

The relative importance of environmental effects on the maglev system will depend primarily on the operating region of the maglev system. If the Grumman maglev system is built in the Northeast, snow and ice will have the greatest impact. This would require a closer examination of the proposed methods of dealing with snow and ice. If the maglev system does not operate at night, the proposed snow plow vehicle must be employed each morning after a snowfall, possibly impacting operations. If the Grumman maglev system is built in a high-intensity groundshaking area such as California, category C and D design specifications (i.e., areas with an acceleration coefficient above 0.19 g) would be required. This would require some revisions in the present guideway design to accommodate these more stringent requirements.

6. MAGNEPLANE SCD

The Magneplane concept uses single vehicle trains that operate within a semicircular trough guideway, as illustrated in Figure 6-1. Magnetic levitation is provided by an electrodynamic system, achieved by vehicle-mounted superconducting (SC) magnets inducing currents in the aluminum trough-shaped guideway, which repel the vehicle and produce lift and guidance forces. Significant vehicle velocity is required to induce the currents in the guideway. For levitation below 27 m/s (60 mph), retractable landing gear are deployed that are equipped with anti-friction air bearing pads. The Magneplane vehicles are not proposed to operate in multi-car trains. Two similar vehicles will be designed to carry 45- and 140-seated passengers. To achieve the required passenger capacity/hr, Magneplane estimates that headways of 20 seconds will be required. Guideway switching uses null-flux coils

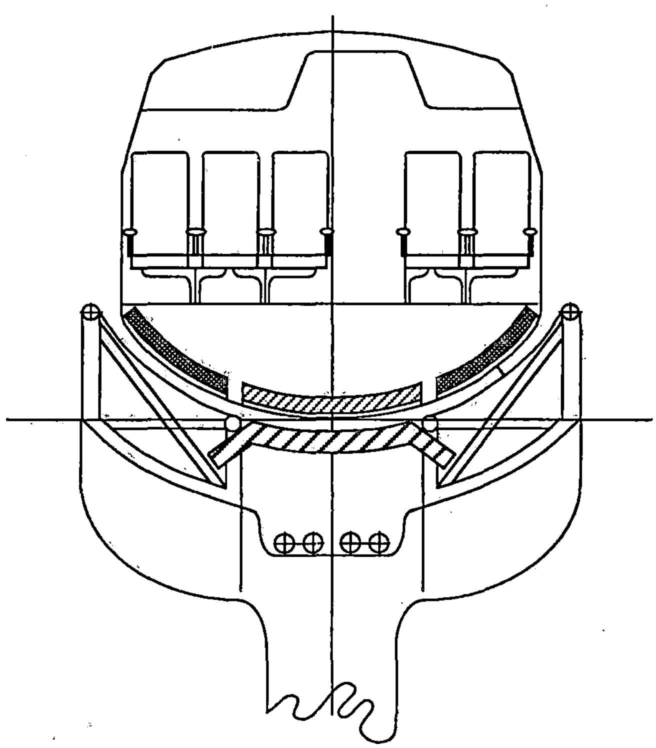


FIGURE 6-1. MAGNEPLANE GUIDEWAY AND VEHICLE CROSS-SECTION

to guide the vehicle through a fork in the guideway trough. Switching requires no moving structural members.

This chapter presents the results of the safety review of the Magneplane system based on the approach described in Chapter 2. The design features of each major system element are described and safety-related issues are identified. The narrative discussion of safety issues within the following subsections represent the results of the detailed safety review contained in the matrices in Appendix E. Information used for this review is derived from the final Magneplane SCD report.

6.1 MAGNEPLANE OVERALL SAFETY APPROACH

The stated Magneplane approach to safety is to require that no single point failure shall result in a Category I (Catastrophic) or Category II (Critical) hazard and that any single point failure that results in a Category III (Major) hazard shall be backed up by a safe mode of operation. Magneplane has defined hazard severity in terms of vehicle damage and personal injury; for each severity category, theoretical numerical hazard rates were developed for safety-related failures. Equipment maintenance classifications in terms of priority of repair are also defined. Magneplane states that system safety design requirements will be specified after "review of pertinent standards . . . and other sources of design guidance for applicability to the design," and lists several organizations.

The Magneplane SCD has adapted the remainder of its general system safety philosophy from MIL-STD 882B. The SCD report contains extensive "adapted" text from MIL-STD-882B and includes the specific requirement for a Software Requirements Hazard Analysis.

Magneplane describes two types of safety analyses that have been conducted. The first type of analysis is called "system level responses" and addresses six issues: wayside control or communication failure; global control or communication failure;

guideway integrity; guideway obstacles; weather; and earthquake. The responses described are very general.

Magneplane also provided a Preliminary Hazard Analysis (PHA) which assesses 13 subsystems: aerodynamic controls; vehicle attitude control systems; vehicle electrical system; superconducting magnets and cryogenics refrigeration; doors and door interlocks; seating, handrails and steps; landing and emergency brakes; magnetic field shielding; seats; box beam/levitation sheets; linear synchronous motor winding; and the Magswitch. Each subsystem is described and various hazards are identified; measures to resolve the hazards are also included.

Although the stated approach is appropriate, the PHA and SCD design text did not completely implement the planned approach. For example, the Magneplane PHA does not identify the hazard severity associated with each hazard under all operating conditions.

The Magneplane SCD text does not discuss the relationship between safety and reliablity. (Volpe Center note: Magneplane did discuss safety and reliability during the last In Progress Review meeting.)

6.2 VEHICLE STRUCTURE AND INTERIOR DESIGN

6.2.1 System Description

The Magneplane vehicle structure will be fabricated from composite materials. The outer shell will be made of graphite epoxy or kevlar face sheets attached on both sides of a Nomex honeycomb core. The outer body will include a fine aluminum mesh for lightning protection and a frontal design to protect against strikes by foreign objects.

In addition to normal and emergency structural load factors, a 50% safety factor was added to the design loads to determine the structural requirements. Magneplane proposes extensive testing of the structure prior to certifying the vehicle for passenger service.

The proposed vehicle design includes five-across seating, two seats on the left side and three on the right. There are two vehicle capacities proposed: a 45- and a 140-passenger configuration.

6.2.2 Safety Issues

The composite materials approach to structures has the advantage of being lightweight while meeting the specified load factors. However, existing high speed rail and maglev systems currently under development use only conventional steel or aluminum material for the carbody structural shell. Composite materials have a limited experience base and have the potential for hazardous events that have not yet been fully addressed. In particular, critical composite material failures are not always detectable. Expensive Non-Destructive Inspections (NDIs) are periodically required to ensure the integrity of the structure. Undetected failures could lead to critical structural failures resulting in potentially Category I vehicle failures.

Magneplane did not sufficiently resolve two issues related to structural design safety. In low speed impacts between the vehicle and other objects, the vehicle should be protected from damage (i.e., buff loads should be defined and integrated into the design of the vehicle). In addition, the vehicle end section should also be designed to collapse in a controlled manner so that the passenger areas are survivable zones during collisions.

6.3 PROPULSION, NORMAL BRAKING, AND EMERGENCY BRAKING

6.3.1 System Description

The Magneplane vehicle is propelled by a linear synchronous motor (LSM) located in the center of the trough-shaped guideway, as shown in Figure 6-2. The proper current, frequency, and phase angle of the LSM is maintained by wayside controllers that receive command signals from a system control center. This approach is not unique and has been adopted by the Transrapid EMS and the Japanese EDS maglev demonstration systems.

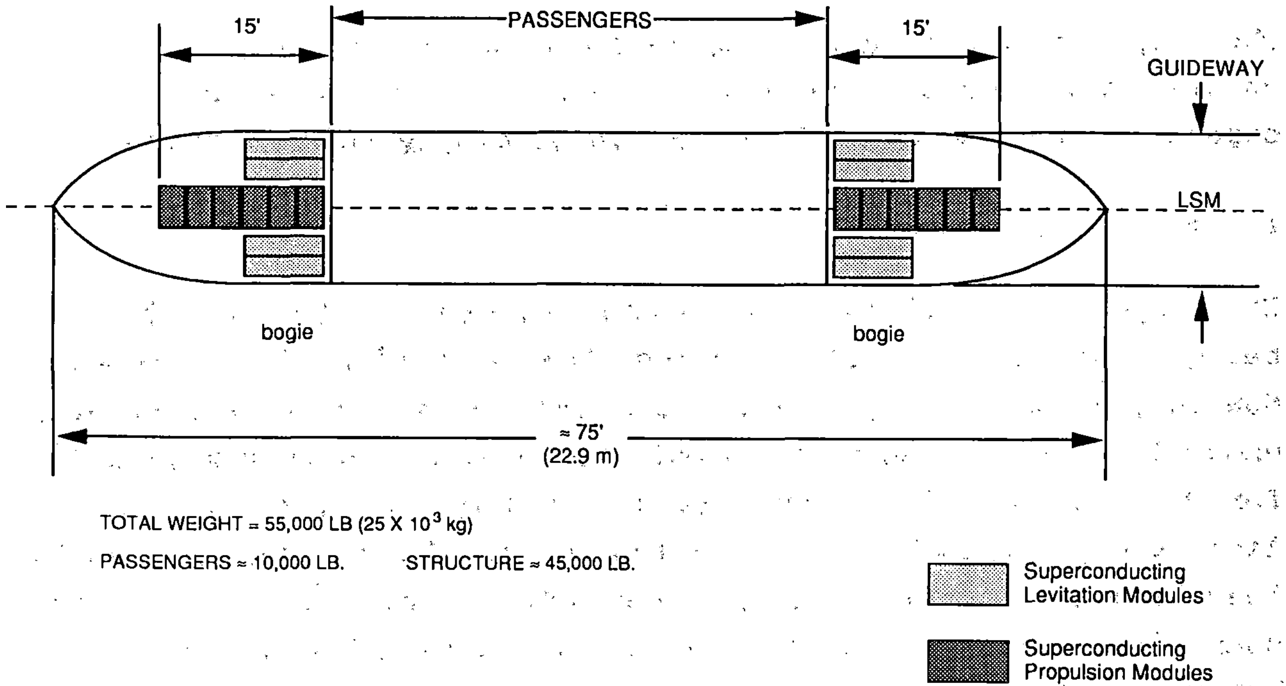


FIGURE 6-2. MAGNEPLANE BASELINE VEHICLE OUTLINE (45 PASSENGERS)

While normal propulsion and braking are provided by the LSM, high friction skid pads are provided on the underside of the vehicle for use in emergency braking situations. In the event of a failure of the levitation system, the skid pads (which have a coefficient of friction of 0.5 to 0.6) are hydraulically deployed to bring the vehicles to a stop.

6.3.2 Safety Issues

In general, LSM applications have failure modes that are potentially hazardous due to inadvertent excessive g forces. The Magneplane SCD concept uses a single LSM stator which represents a potential single point failure. A failure of one or more of the three-phase motor windings will result in an uncommanded dynamic braking action caused by the kinetic energy of the vehicle on-board magnets interacting with the LSM windings. The unknown magnitude of this force and its unexpected occurrence could result in the passenger injuries, a Category II event.

The propulsion and braking systems are mutually exclusive functions dependent upon the LSM and a complex LSM control system. The frequency synchronized LSM winding waveform interacting with the vehicle SC magnets provides normal propulsion and braking functions. The LSM receives input from the global control center via a wayside controller which governs local train movements. The wayside controller can be responsible for the operation of up to eight vehicles, eight power converters, and the associated switching. All conceivable failures, malfunctions, and inadvertent functions must be analyzed to demonstrate that Category I events caused by the controller are extremely improbable. Accordingly, this system will require more detailed analysis during the next phase of concept and design development.

Although the emergency braking system should stop the Magneplane vehicle, there are three concerns. High deceleration levels will be experienced by passengers during emergency braking. These braking levels may cause passenger injuries, particularly if passengers are allowed to move freely about the cabin as proposed by Magneplane. This is potentially a Category II hazard. In addition, no analysis has been provided to verify that during emergency braking the vehicle will remain in the guideway through switch zones, banked turns, and icing conditions. The vehicle departing the guideway is potentially a Category I hazard. Finally, loss of levitation at 300 mph may cause significant damage to the vehicle guideway and guideway-mounted equipment. The frequency and severity of emergency braking application incidents requires further investigation to assure that the risk associated with these events is sufficiently low.

6.4 SUSPENSION, LEVITATION, AND LATERAL GUIDANCE

6.4.1 System Description

The Magneplane electrodynamic levitation design uses SC magnets located at the bow and stern of the vehicle to produce strong electro-magnetic fields under the vehicle. When the magnets move, their fields induce currents in the 2 cm thick aluminum guideway sheets. These induced currents produce an opposite magnetic field to that of the vehicle magnets, and therefore repel them causing levitation. Magneplane states that the airgap between the vehicle and guideway will be large enough and sufficiently compliant so that no secondary suspension is required to ensure a good vehicle ride quality.

At high speeds, the magnetic levitation combined with the aerodynamic flight controls work to provide suspension and stability. The magnetic levitation system is designed to regulate the height of the vehicle by controlling the phase of the LSM to generate vertical forces. This action and control of the aerodynamic surfaces work together to provide a "smart" shock absorber that stabilizes the vehicle.

The Magneplane vehicle contains two bogies, each containing two levitation modules and one propulsion module, as shown in Figure 6-2. The levitation and propulsion coils contained in the modules are SC multi-filament wires enclosed in a steel conduit. The conduit provides a channel for the supercritical helium coolant.

Each levitation module contains two SC coils that are designed to be electromagnetically independent and have separate cryostats. Magneplane states that this independence, in combination with a low ratio of superconducting magnet-operating current to critical current, assures that loss of levitation in one coil does not cause a total loss of lift. Magneplane also states that one such coil is sufficient to enable the vehicle to remain levitated, but no static or transient dynamic analysis is provided in the SCD to support this statement.

The Magneplane electrodynamic suspension system levitates the vehicle only at speeds in excess of 27 m/s (60 mph). At low speeds, a retractable skid-type landing gear supported by pneumatic shock struts will be deployed as illustrated in Figure 6-3. The landing

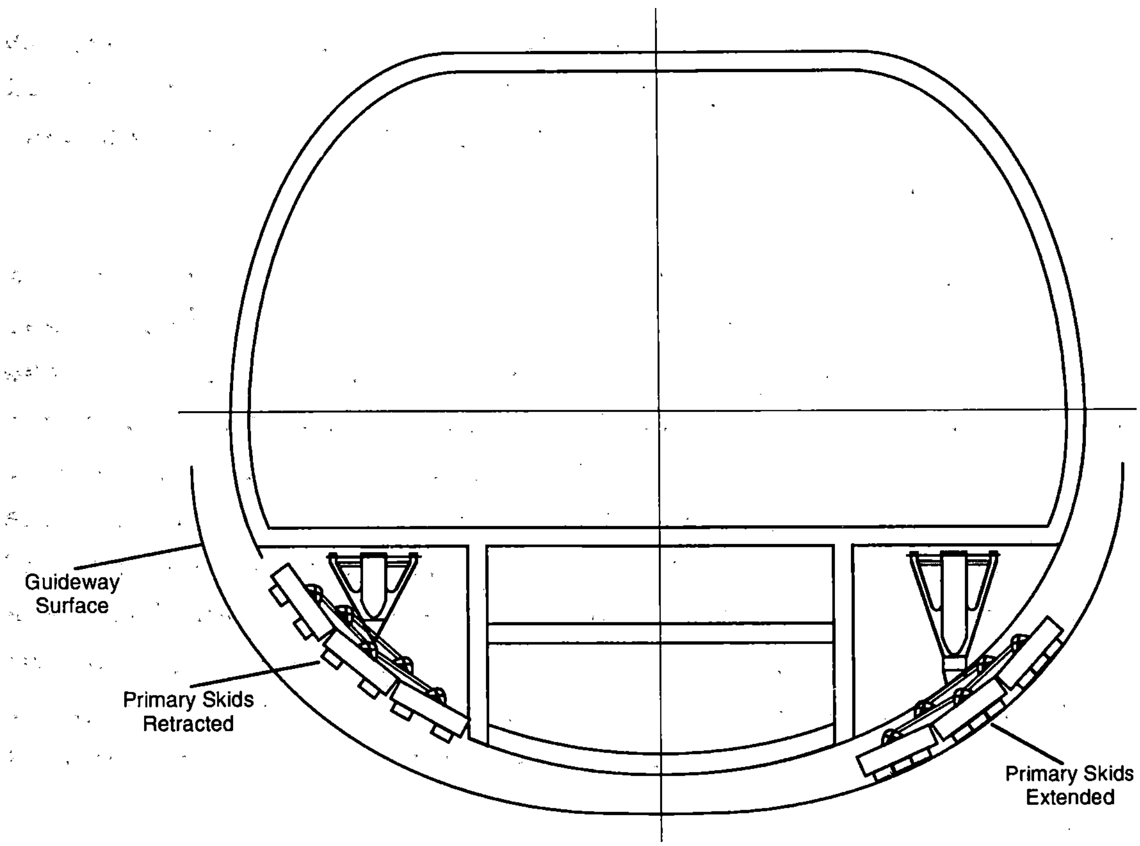


FIGURE 6-3. MAGNEPLANE SKI/SKID CONFIGURATION

gear is equipped with an air-bearing pad that creates an air cushion between the landing gear and guideway.

This air cushion is formed by forcing compressed air through a manifold system on the bottom of the pad. The landing gear can be extended to accommodate flat sections of the guideway used in switch zones.

The Magneplane vehicle is free to roll and move laterally within the curved guideway under the influence of the lateral acceleration forces. The proposed guideway is designed to ensure coordinated vehicle banking through curves to maintain all effective forces normal to the vehicle floor. With this design, a mechanical tilting mechanism is not required and is not included in the Magneplane SCD.

A liquid helium cryogenic refrigeration and storage dewar system is located at the rear end of the vehicle to provide the supercritical helium cooling fluid for the SC magnets, as shown in Figures 6-4 and 6-5.

To provide control and stability of the vehicle at high speeds, the Magneplane concept includes aerodynamic control surfaces. Magneplane asserts that the aerodynamic control surfaces and the magnetic suspension stiffness will provide a good enough vehicle ride quality so that a secondary suspension system is not needed. Two horizontal stabilizers are provided at the front of the vehicle, and two at the aft end. These surfaces are capable of generating both pitch and roll control forces. A vertical yaw canard is provided on the forward end and a conventional fin and rudder at the aft end as shown in Figure 6-6; these are capable of generating yaw stabilization and control forces as well as lateral force generation.

6.4.2 Safety Issues

The complexity of Magneplane's suspension system may prove to be a substantial challenge to designers because the aerodynamic and levitation systems operate independently, while the action of one system impacts the other. Therefore, the safety requirements placed on the suspension system must consider the dynamic interaction between the aerodynamic and magnetic levitation systems. A highly reliable design must be developed to ensure that vehicle contact with the guideway at high speed is an improbable event. It is also important to recognize that the effectiveness of the aerodynamic controls is directly dependent upon the vehicle speed. Aerodynamic controls are ineffective for controlling the vehicle at low speeds. The response rate and surface sizing of the aerodynamic controls are not discussed by Magneplane. In addition, no software requirements are specified for the functions to be performed by the suspension system. Clearly, the software requirements for control of the integrated aerodynamic and phase regulated LSM systems will be formidable. However, similar complex

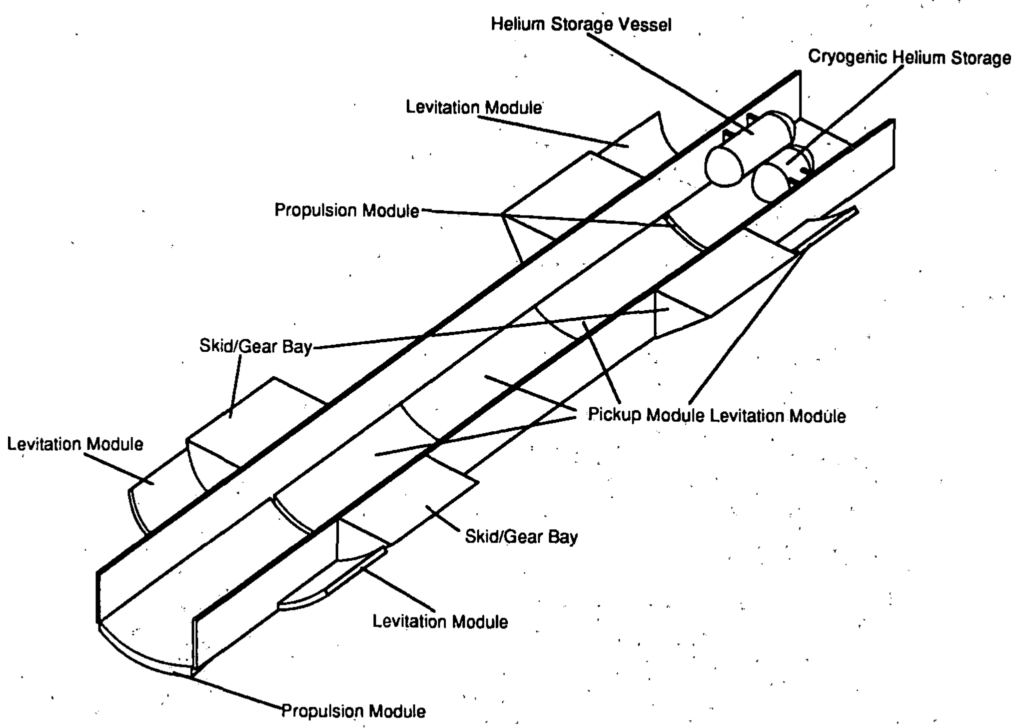


FIGURE 6-4. MAGNEPLANE CRYOGENICS AND PICKUP COILS (UNDER FLOOR)

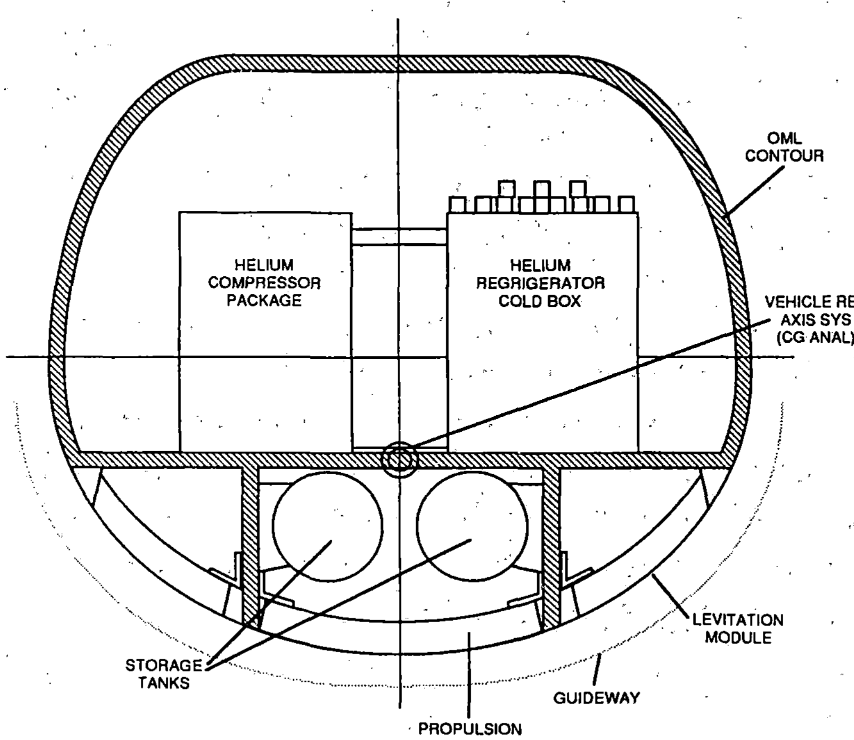


FIGURE 6-5. MAGNEPLANE CRYOGENICS (CROSS-SECTION)

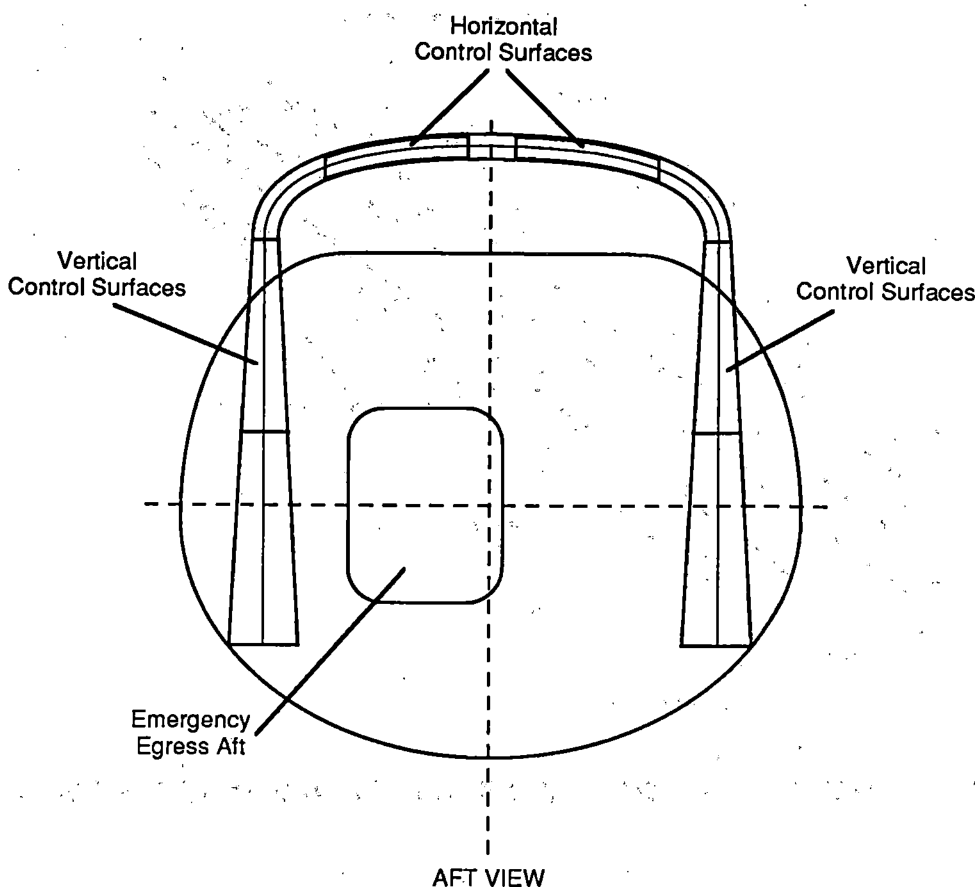


FIGURE 6-6. MAGNEPLANE AFT CONTROL SURFACE

control systems, such as aircraft automatic landing systems, are in use and exhibit high operational reliability.

A failure of the landing gear pneumatic pump or manifold would cause the air bearing pad to contact the guideway, resulting in an emergency type brake application. A more severe hazard exists when a single air pad fails. This results in a higher coefficient of friction between the failed pad and the guideway, creating a substantial yawing moment on the vehicle. Even at relatively low speed (below 27 m/s, 60 mph), this is potentially a Category I hazard.

On-board cryogenic systems have potential Category I and II hazards that should be identified and mitigated during the preliminary design phase. They include the effects of "cold" burns, cryogenic oxygen deficiency, and materials embrittlement. These hazards are similar for Magneplane as for the other SCDs and are described in detail in Section 3.4 of this report.

No aerodynamic analysis is provided by Magneplane to demonstrate the effectiveness of the control surfaces. However, the aerodynamic controls are analyzed in the PHA by Magneplane for four possible failure modes:

- Actuator failure
- Loss of vehicle power
- Bird strike
- Unexpected "hardover" condition.

Although the PHA discusses hardover control surface conditions and mitigating measures, the severity of hardover conditions at high speed was not fully investigated. A nose down pitch hardover at high speed might cause the nose of the vehicle to strike the guideway. In addition, failure conditions resulting in asymmetrical control surface settings were not addressed. Historically, the most common cause of aircraft asymmetrical control surface conditions is misrigging of the mechanical controls during maintenance. Therefore, special care would be required to ensure proper maintenance of the equipment.

6.5 ON-BOARD POWER SYSTEMS

6.5.1 System Description

Magneplane's vehicle electrical power is supplied by a linear generator inducing voltage in inductive pick-up coils located along the bottom side of the vehicle centerline, as shown in Figure 6-4. A back-up lead-acid battery power system is provided to supply vehicle electrical loads under abnormal and low speed operating modes. The available battery time ranges from 35 to 165 minutes, depending on the type of failure mode and allowable load shedding. Three modes of back-up power operation are defined as follows:

- **Mode 1:** Primary power source failure or major on-board power conversion failure. Available battery time is 35 minutes.
- **Mode 2:** Loss of guideway power. Available battery time is 54 minutes.
- **Mode 3:** Major loss of vehicle function such as loss of levitation. If magnets have been quenched, magnetic shielding and cooling functions will be reduced. Available battery time is 165 minutes.

The on-board electrical system will be used to power vehicle systems including:

- Cryogenic cooling system
- Magnetic shielding
- HVAC (Heating, ventilation and air-conditioning)
- Actuators
- Landing gear and emergency brakes
- On-board communication and control
- Lights, and
- Kitchen.

6.5.2 Safety Issues

A loss of electrical power is potentially a Category II hazard because some safety-related functions would be affected. Therefore, it is important that the electrical system and pick-up coils are reliable. Although an analysis of the pick-up coil sizing and location is presented in the SCD, Magneplane states that further experimental work is needed to finalize the design.

As a safety provision, a low voltage lead acid battery system is provided to supply power under abnormal operating modes. There are two significant safety issues associated with the use of lead-acid batteries on a maglev vehicle. First, lead-acid batteries emit potentially explosive hydrogen gas. This is potentially a Category I hazard. It is important that the battery compartment is properly ventilated to prevent the accumulation of hydrogen. Second, lead-acid batteries are prone to leakage that can cause corrosion. This is potentially a Category II hazard. A well-managed maintenance program should be implemented to control battery leakage and corrosion.

6.6 MAGNETIC SHIELDING

6.6.1 System Description

To protect passengers from magnetic field exposure, an active field cancellation system consisting of shielding coils is proposed for installation in the vicinity of the SC magnets. Magneplane states that this active system will largely cancel the fields to ensure that passengers are not exposed to magnetic fields radiating from the propulsion and levitation magnets. Near the ends of the SC shield coils, additional localized "trimming" coils may be required to limit the passenger exposure to less than 1 gauss.

6.6.2 Safety Issues

Although a universal safe level for passenger exposure to dc fields has not been determined, the SCD SOW set goals of 50 gauss, 5 gauss and 1 gauss levels to be studied with respect to cost and potential mitigating measures. Magneplane's on-board SC magnets are located very close to the passenger compartment. In fact, the distance between the magnets and the passenger cabin is less than any other SCD design. Therefore, it is recommended that failures of the shielding coils and excessive field strength be annunciated. Depending on the intensity of the magnetic field produced in the passenger compartment, it may be necessary to shutdown the on-board magnets and delevitate the vehicle if there is a failure of the shield coil system.

6.7 FIRE PROTECTION

6.7.1 System Description

To satisfy fire safety requirements, Magneplane proposes compliance with FAA requirements. Magneplane states that the vehicle will comply with Federal Aviation Requirement (FAR) 25.851 which requires a minimum of three fire extinguishers to be located conveniently in passenger compartments. A fire protection system will be installed per FAR 25.869. Electrical components will meet the applicable fire and smoke protection requirements of FAR 25.831(c) and 25.863. Electrical cables, terminals and equipment in designated fire zones will be fire retardant. Main power cables will be designed to allow a reasonable degree of deformation and stretching without failure. Main power lines will be isolated or shrouded from flammable fluid lines. Wire insulation must be self-extinguishing. Finally, Magneplane states that flammable fluids will meet FAR 25.863 to minimize the probability of ignition of the fluids and vapors.

6.7.2 Safety Issues

The Magneplane approach to fire protection is two-fold. First, Magneplane states that vehicle finish materials will meet strict combustibility and flame requirements. Second, fire suppression systems, including on-board fire extinguishers and smoke-removing ventilation equipment, will be installed. Magneplane states that vehicle fire protection will generally be in accordance with FAA aircraft requirements.

Most of the information provided by Magneplane pertains to fire prevention and suppression methods. Magneplane does not include any discussion of smoke detectors; therefore, more consideration should be given to fire detection. In addition, although materials selection is discussed with respect to flammability, smoke emission is equally important and should be addressed.

Finally, no significant fire protection discussion for stations is provided in the SCD. Limited information on detection methods for fires in isolated, unstaffed wayside locations is provided. Fire detection methods of these areas should be discussed.

6.8 GUIDEWAY DESIGN

6.8.1 System Description

The guideway consists of a trough and supporting structure as shown in Figure 6-7. The guideway is composed of two levitation box beams and an LSM winding. The vertical supports are columns or piers that have crossbeams to support the trough beam structure. The foundations for the Magneplane guideway may vary in size and type, depending on the loading dynamics and soils encountered. To monitor the guideway for safe operation, continuity straps will be installed at the joints between guideway sections to ensure integrity.

6.8.2 Safety Issues

According to Magneplane, there are no single point failures that can lead to a Category I event. However, there is little discussion about any specific guideway-related Category I hazards (i.e., misalignments, buckling, etc.). Magneplane states that ride quality monitoring will complement the continuity detectors to provide failure detection of any gradual deterioration of the guideway integrity. However, ride quality monitoring provides very little proactive protection against abrupt guideway misalignments or buckling. Therefore, this system should not be considered a viable resolution to these hazards since failures will be detected only after the vehicle passes the failed section of the guideway.

Magneplane provides no mechanical means to prevent the vehicle from departing the guideway. The shape of the guideway (semi-circular rather than up-side down "U" shape) and the fact that the vehicle does not wrap around the guideway could contribute to the occurance of this Category I hazard. Gravity and the magnetic levitation and guidance system are the only forces preventing the vehicle from departing the guideway. The safety certification of this design will require substantial analysis and testing of the levitation and guidance system to assure that a vehicle departing the guideway is an extremely improbable event under all foreseeable conditions.

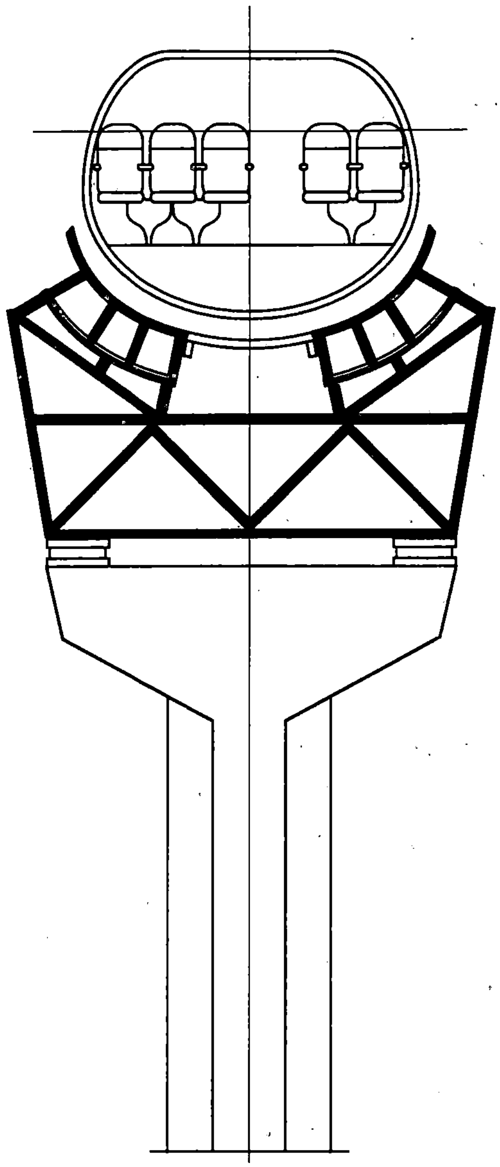


FIGURE 6-7. MAGNEPLANE CONCRETE CROSSBEAM AND COLUMNS SUPPORTING AN ALUMINUM MAGWAY

6.9 GUIDEWAY SWITCH

6.9.1 System Description

The Magneplane system guideway switching concept widens the track by increasing trough flat bottom width to form a track side branch. A vehicle traversing the switch section at speed is electro-dynamically guided along either the switch-trough branch or into the switch side branch without using moving parts. By selectively

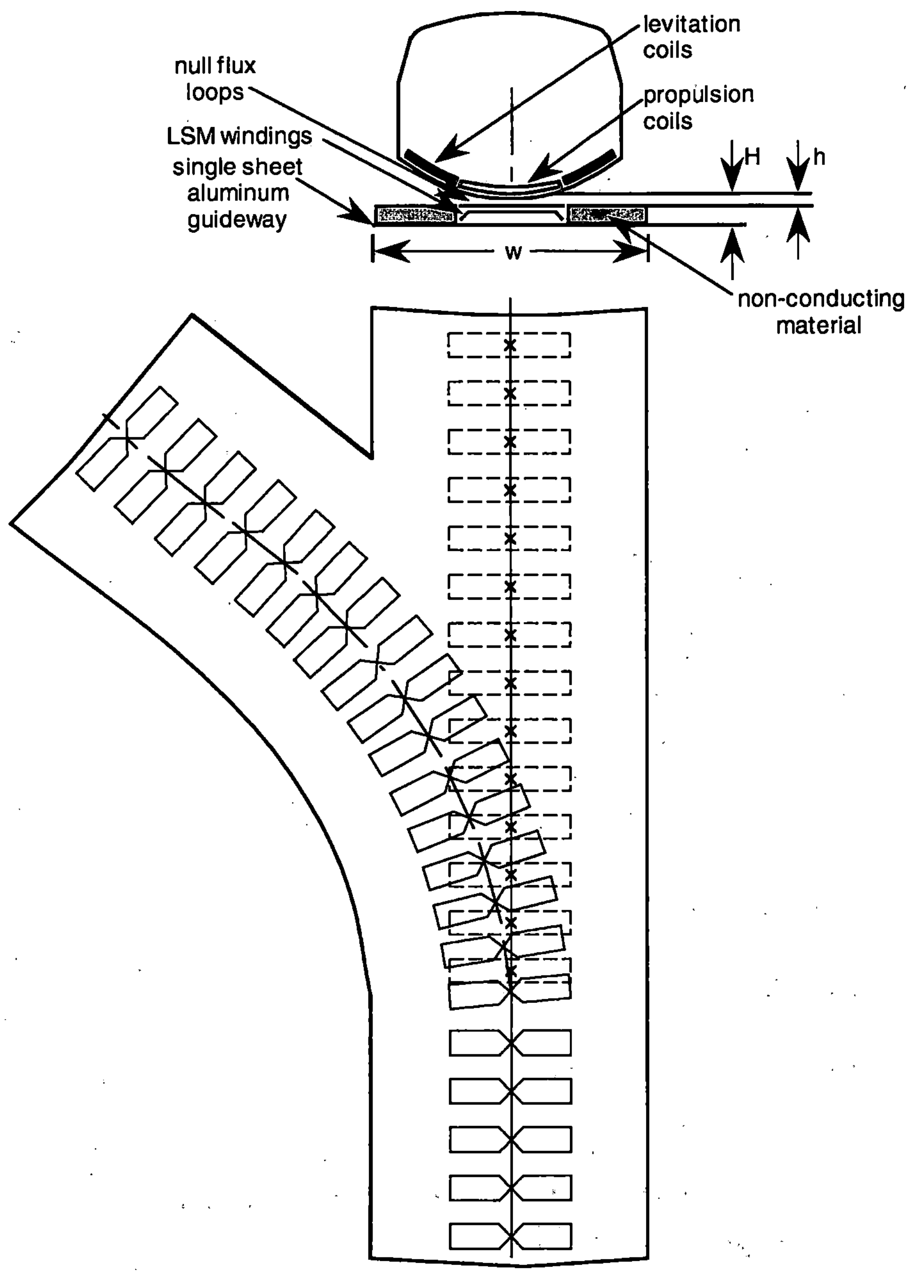


FIGURE 6-8. MAGNEPLANE SWITCH

short-circuiting one of the two sets of passive null-flux loop coils embedded in the track surface directly below the centerline paths of the switch traversing vehicles, operators can guide the vehicle as desired. Null-flux loop coils are track-embedded directly on corresponding LSM windings which are powered in accordance with the selected switch branch.

Spaces on each side of the embedded null-flux loops and LSM windings are completely filled with concrete to provide a flat running surface. This flat surface is required for the air suspension pads which extend downward from the sides of the vehicle when it is traversing through the switch at low speed (i.e., when the electrodynamic suspension is inadequate).

6.9.2 Safety Issues

The electrodynamic switching mechanism proposed by Magneplane is unique and untried. A null-flux loop coil or an SC magnet module failure that occurs while a vehicle is traversing through the switch is a potential Category I hazard. The dynamics of vehicle operation through the switch have not been analyzed in detail (only feasibility calculations are provided in the SCD report), so the ability of the vehicle to remain levitated and safely negotiate the switch at all speeds and crosswind conditions must be completely verified. The only information pertaining to low-speed switching is a drawing and description of an active mechanical switch for operation at vehicle speeds up to 100 m/s (216 mph).

6.10 GUIDEWAY MONITORING

6.10.1 System Description

Magneplane proposes four methods to provide monitoring of guideway integrity and obstacle detection. Closed Circuit Television (CCTV) will be implemented to monitor obstacles on the guideway. Block interface straps will monitor the integrity of the structure of the guideway. The vehicle will be equipped with sensors to monitor the g forces associated with poor ride quality. Finally, fences will be erected to prohibit people, animals, and debris from entering the guideway.

6.10.2 Safety Issues

The Magneplane guideway monitoring system is proposed to resolve potential Category I collision hazards. The effectiveness of the

CCTV system will be limited during night-time operations and in poor visibility conditions, and restricted to the area under surveillance. CCTV requires human monitoring, which introduces human error, further reducing system effectiveness. Vehicle ride quality monitoring is reactive and indicates an obstacle only after the vehicle strikes the object. Structural barriers are needed but do not provide a fool-proof approach to protecting the system. Power monitoring provides an indication of the guideway integrity. However, obstacles that do not interrupt the electrical continuity of the LSM windings will not be detected. Although these systems individually do provide some guideway obstacle protection, they do not adequately mitigate obstacle hazards. In addition, Magneplane vehicles should also be capable of withstanding impacts with small objects that cannot be detected in a timely manner, such as birds and debris.

6.11 POWER SYSTEM AND DISTRIBUTION

6.11.1 System Description

Power substations will be located every 21.2 km (13.25 miles) along the guideway feeding converter stations that stepdown the power from 115kv to 34.5kv for distribution. Power will be delivered from power stations to converter stations via a double overhead aluminum line along the right-of-way. An overhead ground wire will be included for lightning protection. The converter station will be designed and connected to the guideway such that loss of one 34.5kV distribution circuit will cause a normally open relay to close and allow the guideway to be powered from the remaining distribution circuit as shown in Figure 6-9.

6.11.2 Safety Issues

The Magneplane distribution concept includes dual 115kv and 34.5kv power lines for redundancy. Magneplane states that a loss of any one single power line will not cause a disruption of power to the system. However, a loss of power from the utility will result in loss of power to the affected block, resulting in a loss of

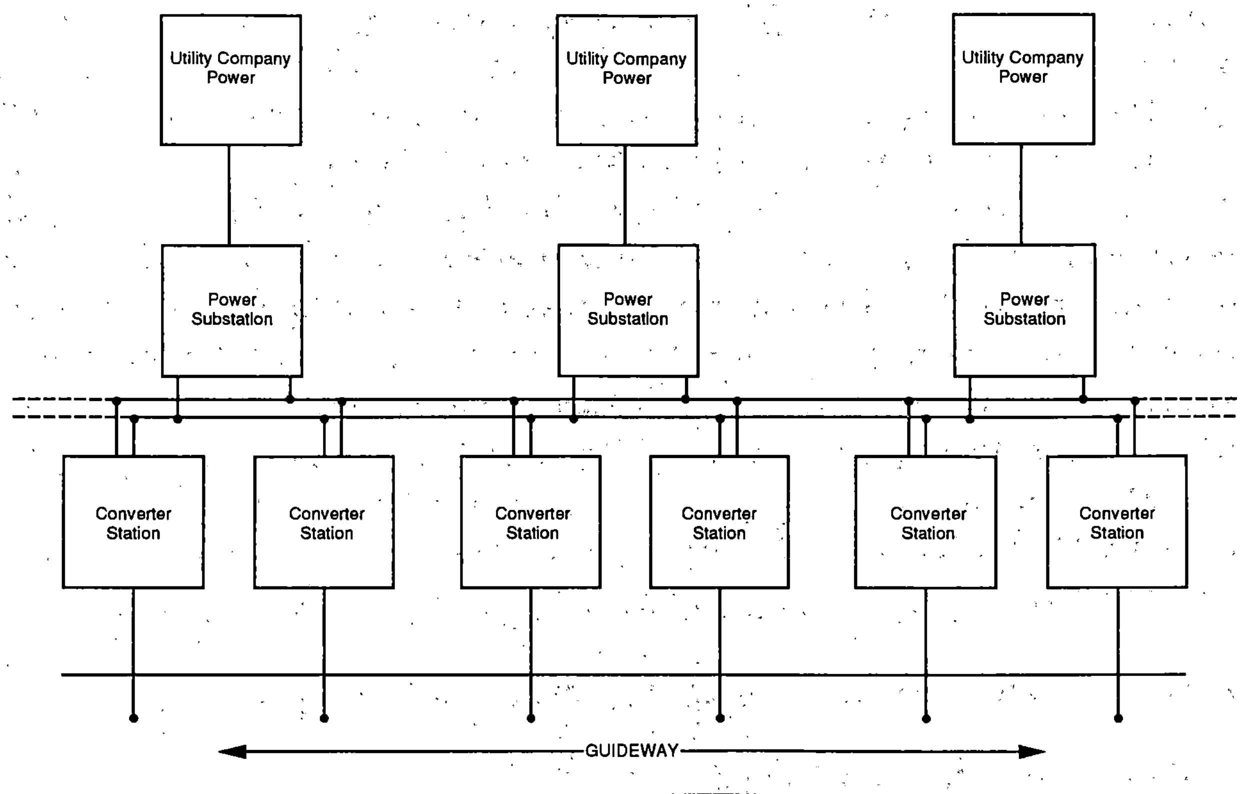


FIGURE 6-9. MAGNEPLANE POWER SYSTEM DISTRIBUTION

levitation, a Category II hazard. In addition to power feeder failures, a failure of any converter will also result in loss of power to the affected block. To mitigate this hazard, a failure management plan should be developed to define the procedures that will be initiated in case of a power system failure.

6.12 COMMUNICATIONS, COMMAND, AND CONTROL

6.12.1 System Description

There are three levels of the communications system used to control the Magneplane system: On-board control, wayside control, and global control.

The on-board controller receives input from vehicle sensors and the wayside controller. The on-board communications system is responsible for processing the information related to: aerodynamic control surface position, landing gear deployment, emergency braking, and door operation.

Information that is used to control the LSM and on-board controllers is received by the wayside controller from the global control center. The wayside controller receives velocity, position and other status data from the vehicle. The wayside controller then transmits the information to the global control center. The wayside controller is responsible for processing information and/or providing commands to the following systems:

- LSM power frequency, phase and current magnitude
- Vehicle position and velocity commands
- Vehicle status
- Guideway block continuity and position markers
- Power converter commands
- Power switch control
- Velocity commands.

The global controller (i.e., Central Control Facility) continuously manages the overall traffic. The global controller is responsible for maintaining headways and vehicle speeds, monitoring ticket purchases and scheduling, and assigning passengers to vehicles.

6.12.2 Safety Issues

Measures will be needed to ensure very high levels of reliability and availability in the wayside controller, vehicle-borne equipment and communications link. A high level of system reliability will be necessary as the control system is inherently vital to safe operation of the Magneplane system. This will require checked redundant architecture to insure proper operation of microprocessors. The possibility of a wayside controller failure must be recognized and a rapid recovery strategy built into the design. This is essential at the proposed close headways because without such a recovery strategy, many vehicles could be stranded on the guideway for a prolonged time period.

The global communications concept design demonstrates the need for setting up software reliability requirements early in the design process. Performing safety-critical and non-essential functions within the same system requires partitioning of software elements into safety-critical and non-essential modules. Software that monitors ticket purchases should be partitioned from software performing critical train control functions. Magneplane does not provide any discussion of an approach to achieve the required safety levels in software. Further study of methods for assuring software integrity should be conducted, and requirements for developing and controlling safety-critical software should be defined early in the system development.

6.13 SYSTEM OPERATIONS AND MAINTENANCE ISSUES

6.13.1 System Description

To provide an insight into Operations and Maintenance (O&M) issues, Magneplane provides a section of the SCD describing O&M procedures. These procedures include:

- Initial Activation of the LSM
- Re-synchronization of Vehicle Movement
- Traversing Horizontal Curves
- Magport-Guideway Transition
- Network Traffic Management, Safe Headway Definition
- Passenger and Freight Scheduling
- Daily, Weekly and Longer-Term Maintenance Procedures.

In addition to these procedures, Magneplane provides calculations used to determine the safe headway distances. As mentioned in the previous section, the headways are controlled by the global controller. The safe headway is calculated based on the distance between and speeds of two successive vehicles on the guideway.

Based on the information in Table 6-1, headways as low as 19.9 seconds and as high as 126 seconds may be used to meet the 4,000 passenger/hour criteria.

TABLE 6-1. MAGNEPLANE BASIS OF SAFE HEADWAY CALCULATION

Communications and decision time	0.25 s
Brake deployment time	3.75 s
Running velocity	134 m/s
Deceleration	4.9 m/s^2

6.13.2 Safety Issues

The safe headway definition does not provide a safety margin for overall system control failure conditions. In particular, the conventions of Automatic Train Control (ATC) interlocking must be observed in the control of guideway switches. Before a train is cleared to proceed through a switch, the route must be established and held by the controller to prevent the switch operating in the approach of a train. The 19.9 second headway appears to make no allowance for this. Transit system minimum headways are usually determined, not only by the capability of the system, but by the ability to minimize station dwell times. To achieve 20-second headways, a considerable number of platforms will be needed at each station with complex switching configurations to direct vehicles into vacant platforms.

At 20-second headways, the calculated guideway levitation sheet and LSM winding temperature may rise 72° C (161° F) above ambient air temperature. Since Magneplane proposes using the guideway for emergency evacuations, guideway heating is a significant safety issue and is discussed in more detail in Chapter 7 of this report.

Switching in maintenance and storage yards is very important to an effective system. Because the Magneplane switching scheme requires levitation, which requires speeds above 27 m/s (60 mph), another switch scheme for yards is needed. These issues require further work in any future analysis.

6.14 ENVIRONMENTAL EFFECTS

6.14.1 Environmental Considerations

To address environmental conditions, Magneplane provides a System Level Response analysis. Magneplane states that, based on 20-second headways, the normal operation of the system is expected to generate enough heat to eliminate snow and ice from the guideway. In addition, the Magneplane guideway design is expected to protect the vehicles from crosswinds. If winds become excessive, global control will slow the vehicles and keep them in the magports. Magneplane states that the vehicles and guideway will be designed such that rain and fog will not affect operation. Finally, Magneplane states that the vehicles, like airplanes, will be able to withstand moderate lightning strikes.

To mitigate the earthquake hazard, the Magneplane Global Control will be connected to local earthquake networks. Operationally, vehicles will be slowed and the guideway integrity will be evaluated by passing vehicles. After the guideway has been patrolled and judged safe, the vehicles may proceed at full velocity.

6.14.2 Safety Issues

Based on the thermal heating of the guideway during normal operations, Magneplane claims snow and ice will not accumulate. However, Magneplane's heating calculations are based on 20-second headways, which may not always be applicable. A more conservative heating calculation would use maximum headways. Furthermore, Magneplane does not address accumulation of snow and ice during any hours when the system is not operational. Vehicles would have to be continuously run for the duration of any storm, even if there are periods of low passenger traffic.

Magneplane states that the guideway design shelters the vehicle from crosswinds. This is a critical assumption because flight controls, suspension and levitation systems will be directly affected by wind conditions. In particular, the aerodynamic control system is vulnerable to wind gusts. The inherent protection provided by the guideway must be demonstrated in analysis and/or wind-tunnel testing.

The Magneplane vehicle will be made of composite materials. The ability of the vehicle to transfer a lightning strike to the guideway with no equipment damage will depend on the composite material and construction.

6.15 SUMMARY OF FINDINGS - MAGNEPLANE

The Magneplane system safety approach as defined in the SCD is based on MIL-STD-882. To resolve hazards, the approach classifies hazards into one of four severity categories. Two types of safety analyses were performed in the SCD: a System Level Response analysis to provide methods for mitigating system level hazards such as weather, braking obstacles and control system failures, and a Preliminary Hazard Analysis (PHA) performed on 13 subsystems. To resolve the identified hazards, a design precedence was created: first, design for minimum risk; second, incorporate safety devices; third, provide warning devices; and fourth, develop procedures and training.

Although the stated approach is appropriate, the PHA and SCD did not completely implement the planned approach. For example, the Magneplane PHA does not identify the hazard severity associated with each hazard under all operating conditions.

The Magneplane SCD design text does not discuss the relationship between safety and reliablity. (Volpe Center note: Magneplane did discuss safety and reliability during the last In Progress Review meeting.)

Probability rate goals are assigned to each of the four hazard severity categories as targets for the design and operation of the system. The probability rate goals are defined with no discussion of their source or derivation. There are no data or analyses provided to indicate whether the baseline design can meet the safety criteria established for each hazard.

Magneplane proposes composite materials for its vehicle structure. The composite design approach has limited applicable experience. Magneplane has not fully addressed the issues of material failure detectability, low speed impacts between vehicles, and provisions for a survivable collision zone at the ends of the vehicle carbody.

Magneplane proposes a single linear synchronous motor (LSM) to provide both propulsion and braking for the vehicle. The A failure of one more of the three-phase motor windings will result in uncommanded braking caused by the kinetic energy of the vehicle on board magnets interacting with the LSM windings. Therefore more analysis is necessary to quantify the frequency and barking forces casued LSM failires. In addition, the emergency skid braking system could cause high deceleration rates causing standing passengers or passengers not wearing seat belts to fall and be injured. Further analysis is needed to quantify the braking rate and frequency of occurrence of emergency brake applications.

The complexity of Magneplane's suspension system may prove to be a substantial challenge for designers. The aerodynamic and levitation suspension systems will operate independently while the action of one of these systems will affect the other. This relationship as well as the response rates and aerodynamic control surface sizing are not discussed by Magneplane and should be addressed.

For low speed operations less than the 27 m/s (60 mph), air-bearing pads are required for levitation. Certain air-bearing pad failure modes are potential Category I hazards. In particular, a failure of one pad will result in a yawing force exerted on the vehicle, causing the vehicle to turn within and possibly depart the guideway.

To provide cooling for on-board superconducting magnets, Magneplane proposes an on-board cryogenic system. These systems have physiological and structural integrity hazards associated with them. A systematic approach to resolving these hazards must be incorporated into the engineering design process.

Magneplane addresses fire hazards by discussing approaches for selecting materials that meet strict combustibility requirements, providing on-board fire extinguishers, and installing ventilation equipment. More consideration should be given to smoke emission requirements for materials and fire detection systems. Methods for fire prevention, detection, and suppression in system equipment and facilities other than the vehicles should also be evaluated, particularly in unstaffed wayside locations which may require automatic systems.

The guideway and vehicle interface does not contain any mechanical or structural means to prevent the vehicle from departing the guideway. A substantial amount of analysis and testing will be required to show that the vehicle leaving the guideway is extremely improbable under all conditions.

The Magneplane electrodynamic switching design does not include any mechanical or structural moving members. A failure of the superconducting magnet module while the vehicle is traversing through the switch is a potential Category I hazard. The dynamics of vehicle operation through switches has not been analyzed in detail (only feasibility calculations are provided).

The Magneplane communications system uses software to perform safety critical and non-safety critical functions. However, Magneplane does not provide any discussion of an approach to achieve the required safety levels in software. Methods for assuring software integrity should be developed prior to system development.

Operationally, Magneplane proposes using headways as low as 20 seconds in order to meet the passenger capacity requirements. This proposed headway does not appear to consider the conventions of automatic train control systems with respect to switching times and station platform operations. In addition, at 20-second headways, the calculated amount of guideway heating is substantial and may impede the proposed emergency egress onto the guideway. However, these calculations are based on 20-second headways. Magneplane does not address snow build-up during longer headways and periods of non-operation. Also, Magneplane states that the guideway design will shelter the vehicle from crosswind gusts. This assumption is critical since the suspension system relies on aerodynamic controls. Therefore, the capability of the guideway to protect the vehicle from crosswind gusts should be demonstrated by analysis and wind-tunnel testing.

7. EMERGENCY RESPONSE SYSTEMS

This chapter reviews the emergency response systems for each maglev SCD including the evacuation of passengers from each proposed transportation system. The review pays particular attention to the facilities, equipment, procedures, and training associated with each SCD and to the needs of elderly and disabled passengers. Based on information and drawings provided within each SCD report, several illustrations were created and are included in this chapter to support the text.

7.1 BECHTEL

7.1.1 Communication During an Emergency

Bechtel states that during emergency situations, communication between vehicles and system central control occurs using vehicle-to-wayside radio communication/data transfer links. Back-up communication is provided for by a back-up link transmitted on the propulsion motor windings. All ground communication/data transfer between system wayside controllers and central control is via a fault tolerant fiber optic cable network.

A number of vehicle-to-guideway communication and/or data links are specified in the SCD. The primary vehicle-to-wayside link is a leaky coaxial cable antenna transceiver system for wide frequency band communication/data transmission over a 20 km (12 mi) range. Transmissions will be networked for direct radio links with central control and other vehicles. A secondary vehicle-to-wayside radio link will be provided using vehicle beacon readers and transponders spaced at relatively close intervals along the guideway to ensure reliable line-of-sight transmission. A third vehicle-to-wayside link uses low frequency signals modulated onto the guideway LSM-powered propulsion windings. Voice communication services will also be provided to the on-board passengers via standard cellular telephones.

The SCD specifies using three on-board attendants for the baseline 100-passenger vehicle to provide passenger assistance in emergency situations and during vehicle emergency evacuation. This exceeds current commercial aircraft federal regulations which require one on-board attendant for every 50 passengers. Any emergency response-related information will be transmitted to the vehicle attendants who, in turn, will inform the passengers with an on-board public address system. Attendants will also assist passengers during any subsequent evacuation.

The least reliable part of the emergency response communications for the proposed system design is the vehicle-to-wayside link. Emergency response vital links may be susceptible to electromagnetic interference effects and may malfunction or fail due to transmitter and/or receiver equipment faults. However, the SCD specification for three independent vehicle-to-guideway transmission systems provides for very significant emergency response communications redundancy. Additionally, each of the three specified transmission links is based on different implementation technology and thus offers different trade-offs between sensitivity to electromagnetic interference effects, transmission bandwidth capability, and inherent reliability of the required communications hardware/software. Accordingly, the proposed communication methods available for emergency response information transfer purposes (emergency control of the vehicle and evacuation announcements) is considered to be adequate.

7.1.2 Emergency On-Board Power Supply

The SCD specifies an on-board NiCad battery emergency power system which is completely independent of the on-board dual fuel cell normal power supply. The emergency power supply is capacity-rated to supply power for emergency ventilation fans, lighting and communications for approximately one hour.

The vehicle hydraulic supply system is required to operate the cabin-tilting actuators and incorporates three accumulators. The energy stored in these accumulators must be sufficient to operate the cabin-tilting system actuators after failure of the normal (i.e. non-emergency) electrical power system which drives the hydraulic system pump motors. The hydraulic system accumulators will be sized to maintain at least several seconds of normal operation of the vehicle secondary suspension and aerodynamic control surface actuators with the hydraulic system pump inoperative. Secondary suspension conventional mechanical springs will be connected in parallel with the hydraulic actuators so the suspension will remain functional under emergency conditions with the hydraulic suspension inoperative. Under these conditions, the vehicle will exhibit degraded performance to the extent that the ride at higher speeds will be uncomfortable but not dangerous.

The vehicle on-board compressed air system for air bladder deployment and operation of the air-bearing landing pads at speeds below 10 km/hr (6.2 mi/hr) uses air tanks sized to power these pads for at least one landing or take-off with the system air compressor inoperative. Additionally, a back-up airstart cartridge will be provided for emergency operation of the air-bearing landing pads for one landing or take-off.

Thus, back-up emergency power will be provided for each of the on-board electrical, hydraulic, and air systems and will have sufficient power capacity to operate all of the vehicle essential functions for emergency situations which require a vehicle landing and subsequent emergency evacuations.

7.1.3 Vehicle Emergency Evacuation Strategy

The emergency evacuation strategy presented in the Bechtel SCD requires that passengers remain on-board the vehicle at all times, except for the potentially life-endangering situations identified as Category I hazards. This strategy requires continued operation of the system with degraded or restricted performance without endangering passengers and crew.

Two alternative vehicle emergency evacuation means are provided over the full length of the guideway:

- A preferred vehicle controlled-coasting to a "safe stopping" site, and
- A back-up inflatable chute or slide.

The Bechtel-proposed preferred means of vehicle emergency evacuation (Figure 7-1) utilizes the kinetic energy of the vehicle and controlled vehicle braking to "coast" the vehicle to a safe stopping site located approximately every 4 km (2.4 mi) along the guideway length. Emergency platforms will be provided at sites for emergency egress through the vehicle side doors and, if necessary, through aircraft-type side window panel emergency exits, onto the site platform, shown in Figure 7-2. The SCD specifies aircraft doors (Type-A) 1.05 m x 1.85 m (3.5 ft x 6 ft) for the maglev vehicles; up to 104 passengers-per-minute can evacuate through these doors.

The emergency platform can be used to transfer passengers/crew to a "rescue vehicle" on either track of the dual-track guideway, shown in Figure 7-2. Additionally, a stairway will be provided for alternative evacuation from the emergency platform to a safe location on the ground.

Vehicles will coast to a stop on the guideway using a controlled application of LSM dynamic braking, and braking provided by the vehicle's aerodynamic and magnetic drag. The proposed LSM propulsion system will be able to stop a vehicle on any given guideway LSM winding block length, even with power loss from the supply utility. Vehicle dynamic braking will be controlled by selectively switching the electrical resistance of the wayside resistor banks located near the wayside power substations. This will dissipate the LSM energy generated by the decelerating vehicle.

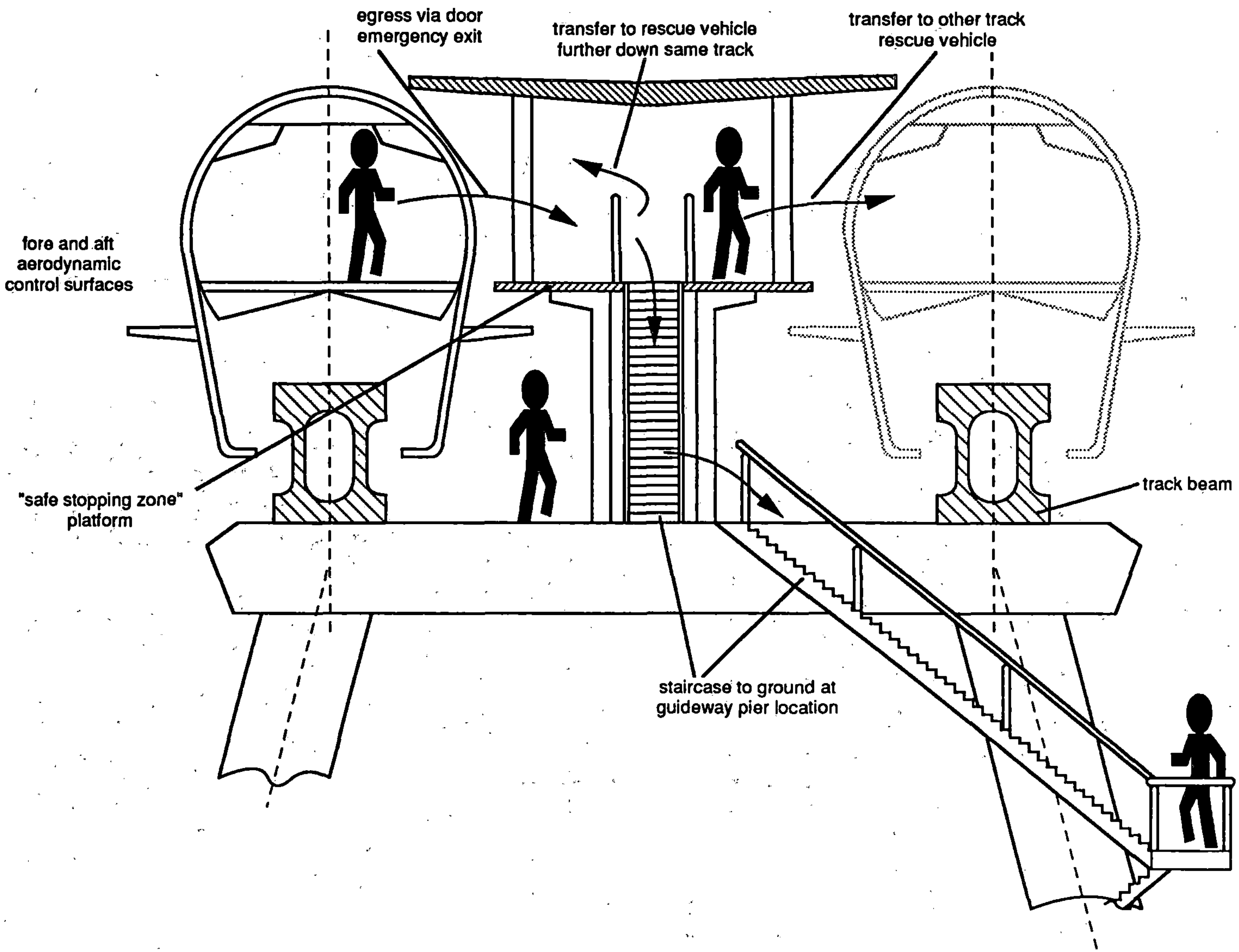


FIGURE 7-1. BECHTEL PROPOSED VEHICLE EMERGENCY EGRESS MEANS
OPTION A: PREFERRED "SAFE STOPPING ZONE" EGRESS OPTION

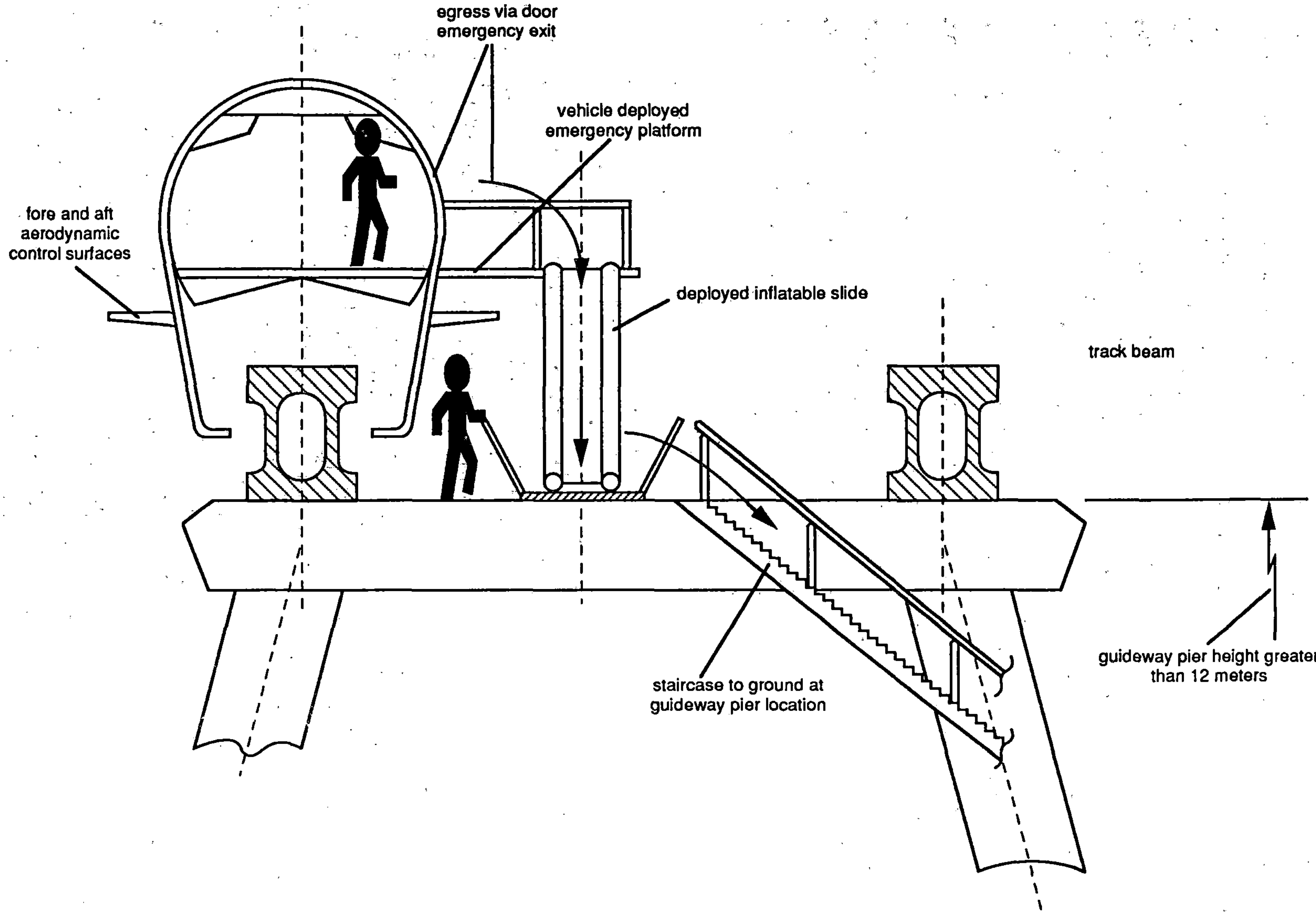


FIGURE 7-2. BECHTEL PROPOSED VEHICLE EMERGENCY EGRESS MEANS
OPTION B1: VEHICLE DOORWAY INFLATABLE SLIDE/GUIDEWAY WALKWAY

An independent source of standby power at each substation resistor bank will provide the power necessary to regulate the resistor bank switching in the event of a total power outage from the supply utility. The vehicle plug-type flat-plate aerodynamic and drag chute emergency braking will not be used for coasting to a safe stopping site because of their relative uncontrollability.

The spacing between safe stopping sites will depend on the difference in the coasting distance for a vehicle decelerating from a given speed with and without maximum LSM dynamic braking coasting effort. The SCD suggests placing the safe stopping sites together with the guideway power conditioning substations spaced at 4 km (2.4 mi) intervals. By doing so, road access for substation maintenance can be used additionally for ground transport of evacuated passengers and crew.

Vehicles decelerating to a stop from speeds down to approximately 80 m/s (180 mph) can coast to a safe stopping site spaced every 4 km (2.4 mi). Bechtel states that a vehicle will coast to a stop in about 6 km (3.6 mi) from an initial speed of 80 m/s (180 mph) without dynamic braking and can be stopped in about 2 km (1.2 mi) with maximum dynamic braking. Dynamic braking energy recovery, using converters to feed the LSM-generated ac power output back into the dc power lines, is advocated by Bechtel for economic reasons and will be available for thrust augmentation purposes to extend the coasting distance for vehicles initially traveling below the threshold speed of 80 m/s (180 mph).

This strategy will allow all system vehicles to reach a safe stopping site in emergency conditions independent of the utility power supply, provided there is sufficient dynamic braking taking place within the system by other vehicles to maintain the needed thrust to extend the coasting range of vehicles stopping from initial speeds less than 80 m/s. While these conditions may not always be met, exceptional cases will be handled by the vehicle back-up emergency evacuation plan.

The concept of safe stopping sites for emergency evacuation purposes was first conceived for the German Transrapid maglev system and requires maintaining a vehicle "safe hover" condition while decelerating the vehicle to a safe stopping site. Safe hover requires the vehicle's electrodynamic primary suspension and air-bearing landing pad system to remain functional during the decelerating coast to a safe stopping site. Safe hovering during controlled coasting depends on realizing a low probability of primary magnetic suspension system loss relative to other emergencies which require safe stopping and vehicle evacuation.

The safe hover condition for the Bechtel SCD is comparable to that of the Transrapid system. Thus, acceptance of the safe stopping site concept for the Transrapid maglev system can be considered a precedent for acceptance of the concept for the Bechtel maglev system. Loss of the Transrapid vehicle active feedback controlled electro-magnetic primary suspension system can result from electrical or mechanical component failure in the suspension system or from failure of the on-board power supply system. Numerous electrical components, sensors, and electrical units comprise each of the separate suspension electromagnets and associated feedback loop. This complexity compromises the overall suspension system reliability to the extent that it is is no longer acceptable for public transportation. The Transrapid maglev system now relies upon suspension magnet loop redundancy to realize acceptable predicted revenue system vehicle availability (i.e., use of a substantial number of distributed suspension magnet loops per vehicle such that only certain location combinations of multiple magnet loop failures would jeopardize safe hovering).

Compared with the Transrapid system, loss of the Bechtel vehicle passive electrodynamic primary suspension system can result from superconducting magnet quenching or from magnet winding/dewar component failure but not from failure of the on-board power supply system. The magnets are persistent current-mode operated and require only infrequent charging. Also, these superconducting magnets do not require on-board refrigeration power for their cryogenic cooling system because the magnet winding cryocooling is based on an on-board supply of helium to absorb the generated heat load.

The probability of superconducting magnet quenching can be made extremely low by appropriate magnet design practice such as the practice reflected by the Bechtel SCD baseline magnet design having a winding current density of only 24% of the critical current so as to provide for a conservative operational quenching safety margin of four. State-of-the-art lightweight magnet dewars can be designed to exhibit exceptionally high reliability, being structural rather than power active components. Further, the proposed utilization of 96 separate superconducting magnet windings contained within 12 separate dewar modules for the primary suspension of the Bechtel proposed vehicle would provide for a high degree of operational redundancy in the same manner as for the Transrapid primary suspension system. Such redundancy would, however, be conditional upon the proximity of the Bechtel proposed magnet windings not allowing for the inductive coupling propagation of any magnet quench from one winding to another.

The Bechtel proposed additional "back-up" means for vehicle emergency evacuation uses aircraft-type inflatable emergency escape chutes/slides deployed immediately below each of the four vehicle doors (see Figure 7-3). Passengers and crew egress directly to ground level when the elevated guideway height does not exceed 12 m (40 ft) is shown in Figure 7-2.

In emergency evacuation situations where the guideway height exceeds 12 m (40 ft) or where the local ground is not readily accessible by the slides, a walkway between the tracks of a dual guideway will be provided. Emergency egress onto walkways will be via a short platform extended from the vehicle below each of the four vehicle doors and a relatively short, inflatable chute/slide as shown in Figure 7-2. A stairway to ground will be provided at intervals along the walkway as shown in Figure 7-3.

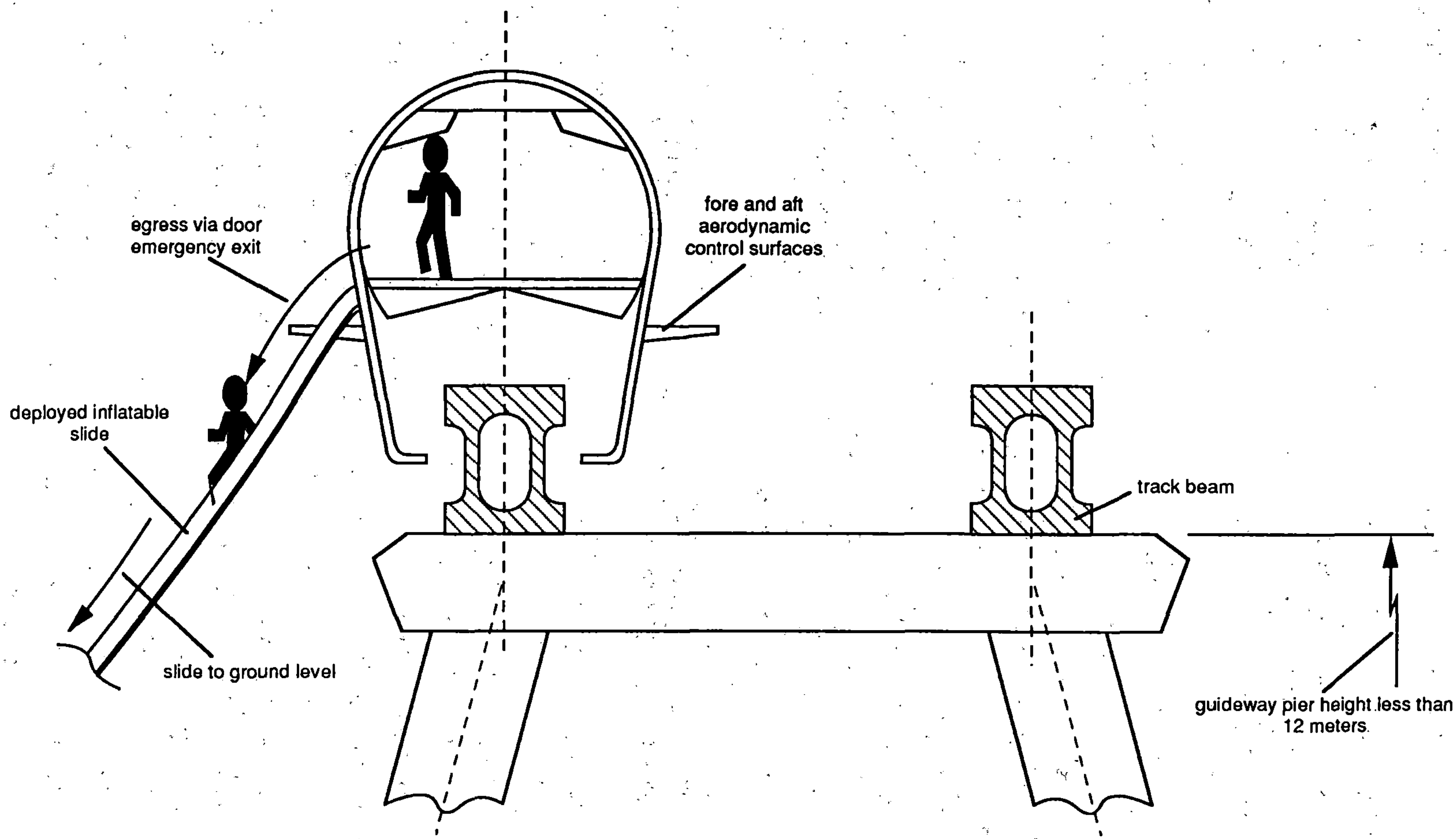


FIGURE 7-3. BECHTEL PROPOSED VEHICLE EMERGENCY EGRESS MEANS OPTION B2: VEHICLE DOORWAY INFLATABLE SLIDE TO GROUND

7.1.4 Vehicle Emergency Evacuation Within Guideway Switch Zones

The proposed system baseline guideway switch is composed of a flexible fiber reinforced plastic beam which can be laterally deformed by suitable actuators to line up with the turn-out branch from an undeflected straight-through track setting.

The baseline switch concept will be compatible with the inflatable slide emergency evacuation options shown in Figures 7-2 and 7-3, if a widened walkway floor is placed beneath the switch flexible beam. This will allow access to the ground from the vehicle inflatable slide for switch elevations higher than 12 m (40 ft). For straight-through and turn-out branch switch beam settings, switch elevations less than 12 m require adequate structure clearance to deploy inflatable slides on one side of the vehicle. Neighboring track for opposite direction travel should not be located so close to the switch track that it would prevent slide use.

7.1.5 Vehicle Emergency Evacuation Within Superelevated Guideway Zones

For the proposed vehicle, the hydraulically actuated active cabin tilting and the guideway beam superelevation angles can each be up to 15 degrees. Accordingly, any vehicle which is stopped on a superelevated track in an emergency should be leveled using the active tilting system to ease emergency egress. A vehicle stopped on a superelevated track with an inoperative cabin tilt mechanism could be tilted at an angle up to 30 degrees from horizontal. Emergency egress should still be possible using deployable slides, but it will be more difficult from a tilted vehicle and will be only marginally possible for disabled and elderly passengers. Emergency egress via vehicle deployable slides onto a guideway-attached walkway, shown for a level vehicle in Figure 7-3, cannot be considered because the slide may be misaligned with the walkway enough to jeopardize safe egress.

The Bechtel tilt design is such that only an inner vehicle structure containing the passenger cabin is tilted. The exterior structure remains fixed relative to the vehicle's magnet bogies. This design simplifies the tilting mechanism, allows for advantages in external aerodynamics and insulates cabin acoustical noise. It is not apparent, however, how the vehicle doors are designed to accommodate the 15 degree relative tilt between the cabin inner shell and the exterior vehicle shell which could exist if stopped on a superelevated track. Another difficulty is with the stowage location for the deployable slide below each door; there is no mention of this design issue in the SCD.

7.1.6 Vehicle Cabin/Crew Compartment Layout and Exits for Emergency Evacuation

The aisle width, seating pitch, overhead baggage stowage bin facilities, emergency lighting, emergency exit sizes, and emergency exit arrangements proposed for the vehicles appear to be consistent with commercial aircraft practice (3 x 3 coach class seating at 74 cm (31 in) pitch with 59 cm (23.4 in) aisle width). Such practice should allow compliance with emergency evacuation standards which call for evacuation of a vehicle within 90 seconds of an emergency stop.

Bechtel considers that this emergency evacuation duration is more than adequate for a maglev vehicle where the risk of rapid fire spreading and/or explosion in vehicles is lower than the risks for aircraft where large quantities of liquid fuel are typically on-board.

The SCD proposes using only single vehicles with 100-passenger capacity for revenue service. To meet specified system capacity, vehicles will operate at very low headways relative to current public guided ground transport system operating practices.

Headways of 30 and 90 seconds minimum are specified for maximum system capacity of 12,000 and 4,000 passengers-per-hour, respectively.

Four 1 m (3.3 ft) wide entrance/exit doors, two-per-vehicle side, are provided in the vehicle cabin layout. In the event of an emergency, each door will be required to evacuate up to 50 passengers. The doors on only one side of the vehicle will be available for emergency egress for safe stopping site platform access or for escape slide deployment, as shown in Figures 7-1, 7-2, and 7-3. For an evacuation duration of 90 seconds, this corresponds to an evacuation rate of 1 passenger every 1.8 seconds. The requirement to evacuate up to 50 passengers per available door for the proposed vehicle design is conservative compared with aircraft practices where, for example, a Boeing 747 aircraft may evacuate 100 passengers per available door.

The FAA proposed commercial aircraft requirements for maximum distance between any seat row and the nearest exit to be less than 9 m (30 ft) are easily satisfied by the proposed maglev vehicle cabin layout. Adherence to this requirement minimizes the distance to exits for all passengers and thereby improves the chances of safe egress during an emergency.

7.1.7 Advantages of Bechtel Emergency Response System

Emergency evacuation after using LSM dynamic braking controlled coasting of vehicles to safe stopping site platforms along the guideway will almost be comparable to station egress.

Emergency evacuation, after using vehicle controlled coasting to safe stopping site platforms, will be available to vehicles beginning their coast anywhere over the entire length of the guideway, including through track switches and superelevated curves.

Additional back-up means for emergency evacuation using deployable slides will be available over the entire guideway length except through one branch setting of the switch design and on curves with the vehicle tilting system inoperative.

Two options for emergency egress from the track walkway to a safe location will be provided, either by using a staircase to ground level or from the walkway into a maglev rescue vehicle.

7.1.8 Safety Concerns for Bechtel Emergency Response System

Passengers may be subjected to significant longitudinal g forces during controlled coasting deceleration to a safe stopping site, particularly for minimal vehicle braking distances within the constraints of safe stopping site spacing.

Emergency evacuation by means of vehicle controlled coasting to safe stopping site platforms will not be available to vehicles beginning their coast from speeds below about 80 m/s (180 mph) during a power outage if too few other vehicles are decelerating. Under these conditions, there are insufficient regenerative power, and coast-extending thrust will be available to the slow vehicle.

Evacuation by means of vehicle deployable slides will not be available over the entire length of the non-baseline mechanically passive alternate switch design which relies on laterally displacing the vehicle magnet pods.

When the vehicle cabin tilting system is inoperative, evacuation using vehicle deployable slides over guideways exceeding 12 m (40 ft) in height will be difficult on highly superelevated curves. Emergency evacuation from vehicle deployable slides has a higher risk of injury than emergency egress directly onto a walkway or site platform and may be particularly difficult for disabled and elderly passengers.

For the high guideway slide egress option, the close proximity of the emergency walkway to adjacent tracks of a dual track guideway will require drastic speed reduction or the complete stoppage of all vehicle traffic on adjacent tracks to minimize or eliminate vehicle-induced wind and acoustical noise impact on walkway occupants.

7.2 FOSTER-MILLER

7.2.1 Communication During an Emergency

During emergency situations, communication between vehicles and system central control occurs using vehicle-to-wayside radio communication/data transfer links in the 933 MHz frequency range. All ground communication/data transfer between system wayside controllers and central control utilize redundant fiber optic cable networks. Provision will be made on this ultra-high-frequency radio link for the trainset crew to request initiation of voice communication via a separate vehicle-to-wayside line-of-sight radio frequency link and to indicate unusual on-board situations.

Measures to ensure optimal reliability of the system-vital vehicle-to-wayside ultra-high-frequency radio link are not specifically addressed in the SCD; the SCD mentions only the need for system redundancy. Because of the uncertainty regarding system reliability, a proper assessment of the communication system cannot be made. Properly designed for high-reliability operation, the communication system can fulfill its role to provide communication of information between vehicle and station central control.

The SCD requires one on-board attendant for each train vehicle unit to provide for passenger comfort needs and also to assist in emergency situations and evacuations. Only the attendant/ passenger ratio in the first class seating vehicle unit conforms to current commercial aircraft federal regulations which require one on-board attendant for every 50 passengers. With 74 seats in business class seating vehicle units, this ratio fails to conform to stated airline standards. Further analysis is needed to determine if one on-board attendant for every 50 passengers is appropriate for maglev operations.

Emergency response-related information is relayed to the passengers via the on-board public address system accessible from the crew positions for each vehicle unit. Additionally, an on-board intercom system is provided between all crew positions in each trainset providing a vital communication link when information must be transferred between crew members during an emergency.

7.2.2 Emergency On-Board Power Supply

Vehicle on-board power is supplied by a battery back-up subsystem which is constantly charged by the inductive coupling wayside-to-vehicle power transfer system. The type of emergency battery power is not identified in the SCD, but the battery subsystem energy density, power capacity, weight and volume are estimated for typical on-board emergency power requirements.

This on-board power battery subsystem is for on-board emergency use only; the inductive power transfer system is designed to directly provide all on-board power needs over the entire speed range of the vehicle, including trains at a standstill.

The vehicle hydraulic power supply system powers the landing/guidance wheels and the vehicle tilting system. Hydraulic system accumulators could provide sufficient power to operate the vehicle tilting system and to deploy the wheels during an emergency stop with the wayside-to-vehicle power transfer system inoperative. However, hydraulic system accumulators are not specifically addressed in the SCD.

Back-up emergency power could be provided within the design boundaries of the SCD-proposed system for each of the on-board electrical and hydraulic systems; the backup emergency power supply could provide sufficient power to operate all of the essential vehicle functions, e.g., lights, communications, etc., in an emergency which requires vehicle landing and subsequent emergency evacuation. However, discussion and details have not been provided in the SCD.

7.2.3 Vehicle Emergency Evacuation Strategy

The Foster-Miller SCD indicates vehicle passengers must remain on-board for all but severe cases of emergency, such as out-of-control fire, structural failure, or long-term stoppage.

Three options for emergency egress from stopped vehicles are presented:

- Sidewall level egress via the normal vehicle doors onto a guideway supported emergency walkway, shown in Figures 7-4 and 7-5 for single and for dual track guideways, respectively.
- Fore/aft egress via an emergency exit hatch at the nose and the tail of each train set onto a guideway track floor walkway, shown in Figure 7-6. In addition, the vehicle design provides for emergency egress from one vehicle to another in a train set, through an articulation unit above the magnet bogies.
- Downward egress via vehicle floor emergency hatch doors and deployable staircases or ladders (not indicated in the SCD) onto a guideway emergency walkway suspended below the track, shown in Figure 7-7.

All three vehicle emergency egress options can accommodate passenger/crew egress from the guideway walkways to ground level via emergency staircases, shown in Figures 7-4, 7-5, 7-6, and 7-7. These staircases will be located periodically along the length of the track. The distance between staircases along the guideway was not specified in the SCD.

Both the lateral and the fore/aft vehicle emergency egress options can also accommodate egress from guideway walkways to rescue vehicles, shown in Figures 7-4, 7-5, and 7-6. In the downwards egress option shown in Figure 7-7, movement from the suspended walkway up into a rescue vehicle on the same guideway is not practical because of safety risks associated with deploying the rescue vehicle floor hatch staircases or ladders onto the suspended walkway.

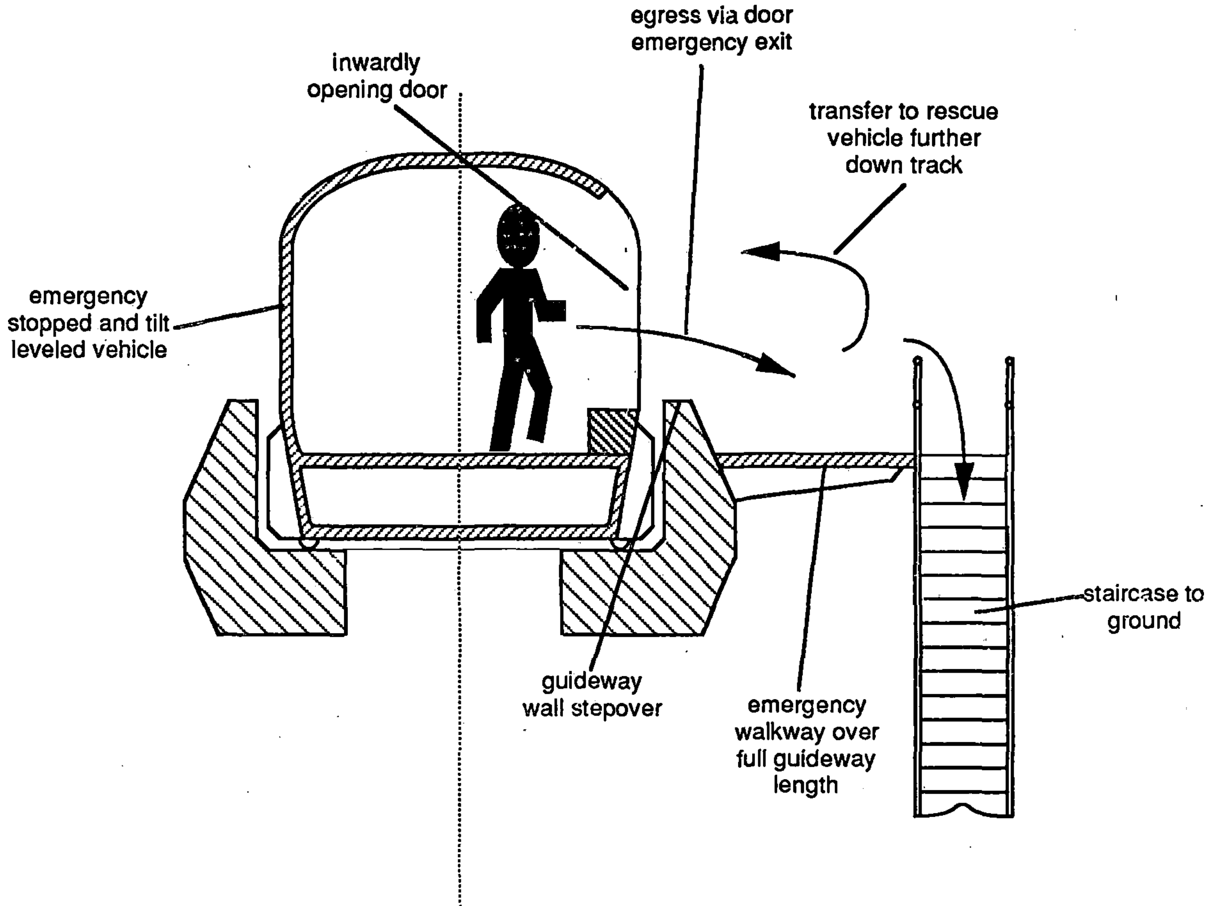


**FIGURE 7-4. FOSTER-MILLER PROPOSED VEHICLE EMERGENCY EGRESS MEANS
OPTION A: PREFERRED VEHICLE SIDE EGRESS OPTION - SINGLE GUIDEWAY**

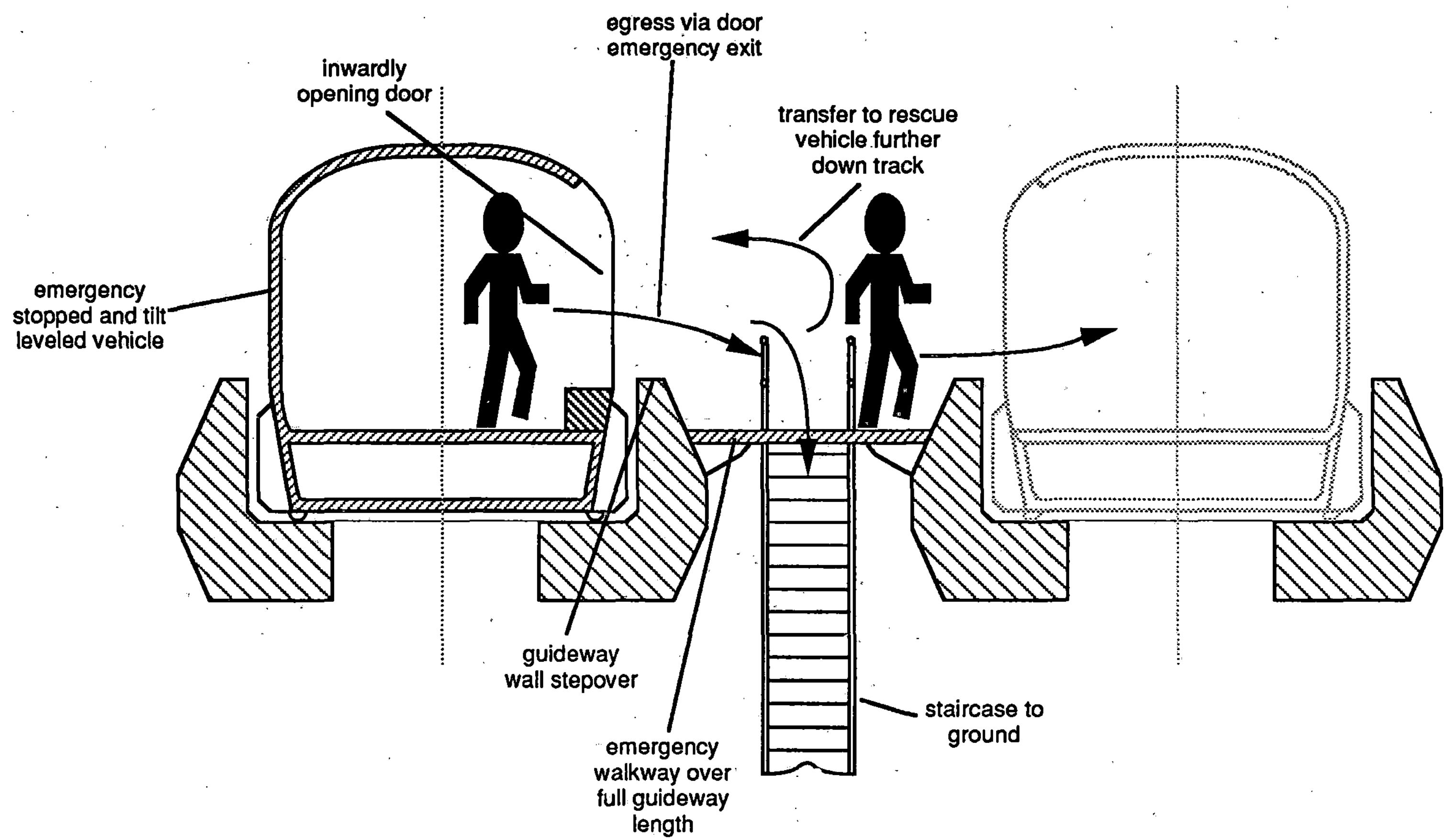


FIGURE 7-5. FOSTER-MILLER PROPOSED VEHICLE EMERGENCY EGRESS MEANS OPTION A: PREFERRED VEHICLE SIDE EGRESS OPTION - DUAL GUIDEWAY

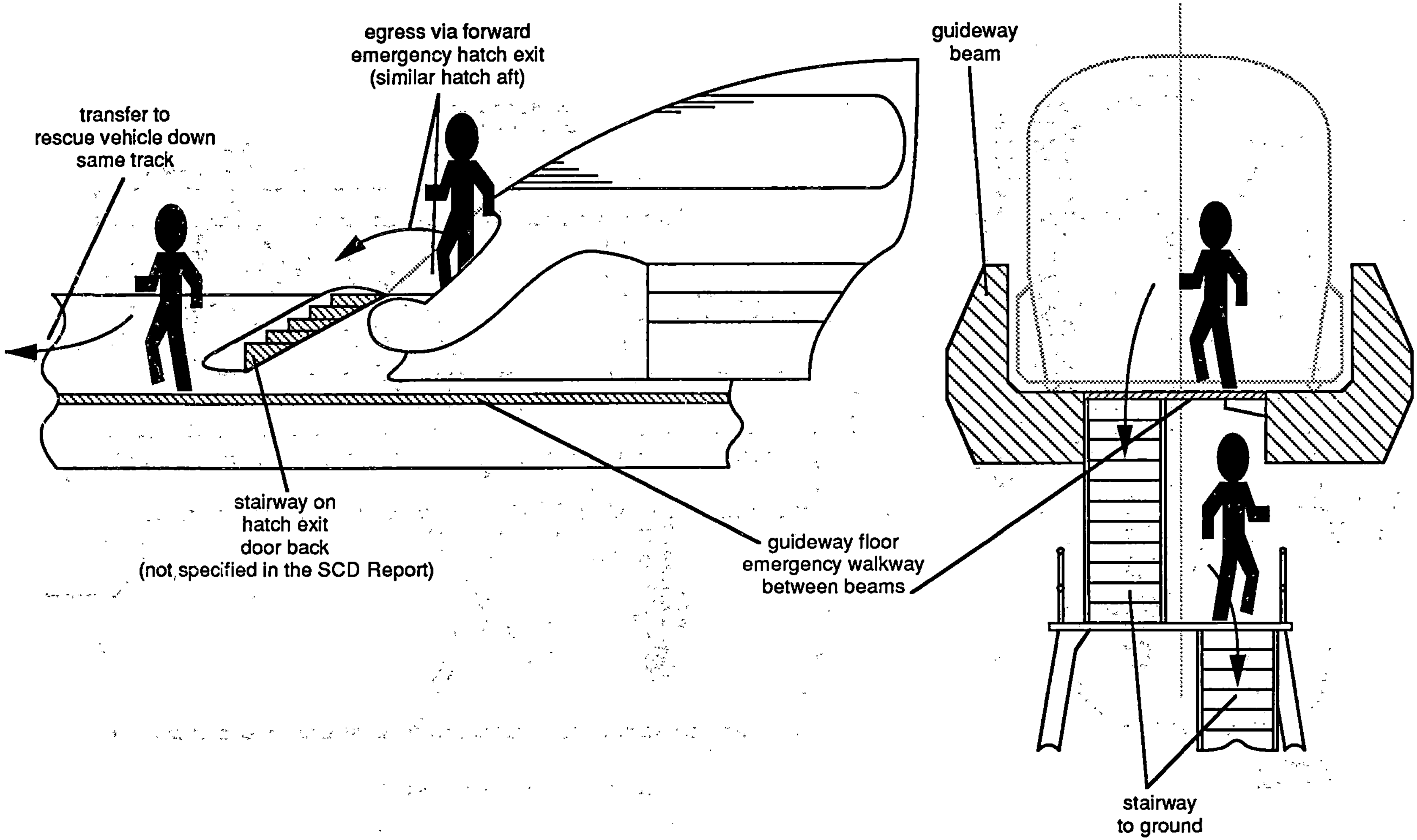


FIGURE 7-6. FOSTER-MILLER PROPOSED VEHICLE EMERGENCY EGRESS MEANS OPTION B: VEHICLE ALTERNATIVE END EGRESS OPTION

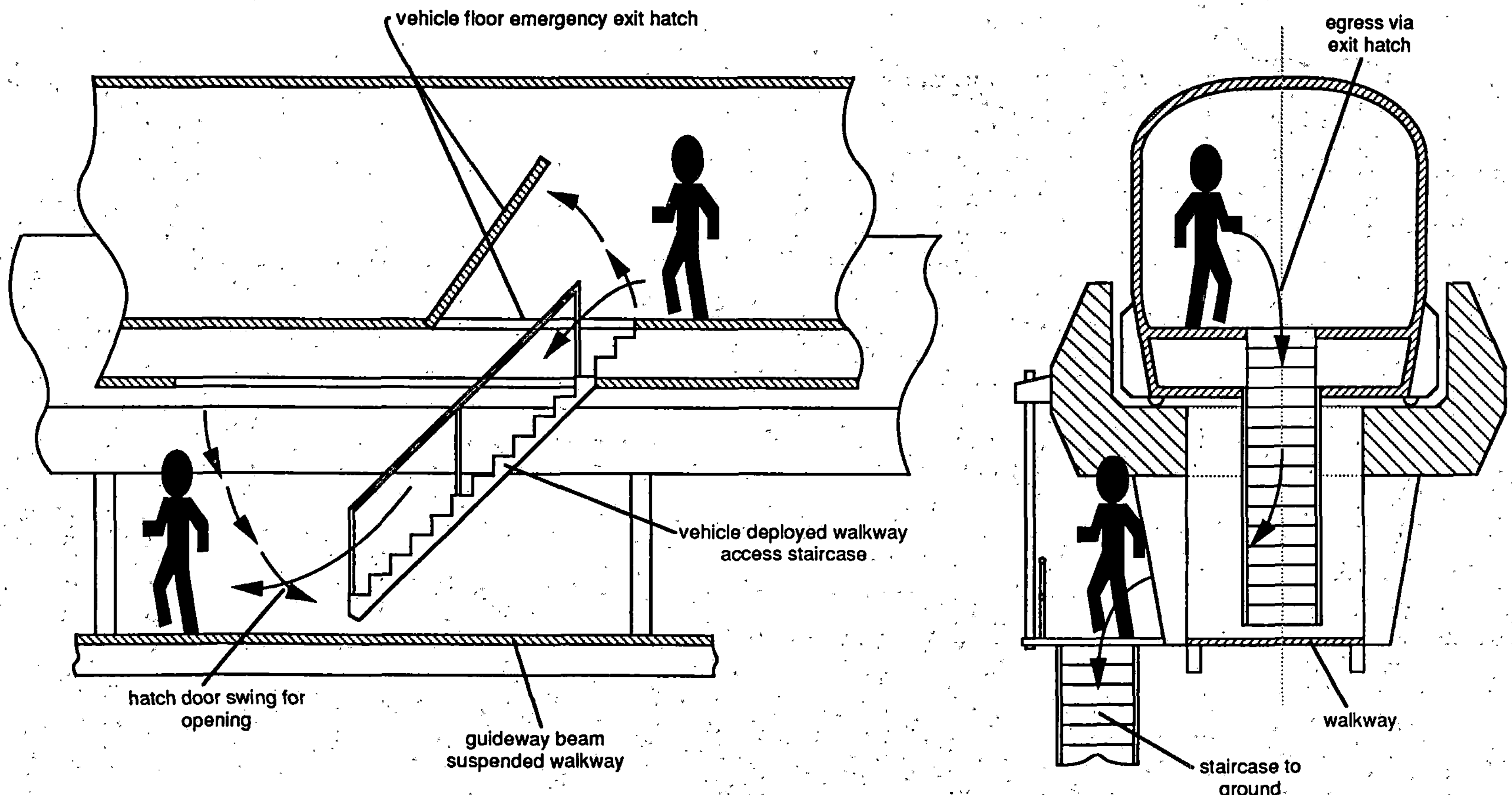


FIGURE 7-7. FOSTER-MILLER PROPOSED VEHICLE EMERGENCY EGRESS MEANS OPTION C: VEHICLE ALTERNATIVE DOWNWARD EGRESS OPTION

Another issue not addressed by the SCD is the interference between the vehicle floor door staircase/ladder in egress option "C" and the guideway connection diaphragm members which are spaced at 5-6 m (16.5-19.8 ft) intervals between the track structural beam sidewalls. Currently, the 1.4 m (4.6 ft) square vehicle floor exit only allows for steep ladder access onto the suspended walkway. The steepness dramatically lowers the emergency egress rate and presents difficulties for disabled or elderly passengers. Additionally, the SCD does not explain how the suspended walkway will negotiate the obstruction caused by guideway pylons.

The SCD proposes standardized 24.7 m (81.5 ft) long maglev vehicle units which could be interconnected between nose and tail units to form revenue system trainsets. The vehicle units, with added identically shaped nose and tail extensions to allow for bi-directional operation, are interconnected to form a baseline two-car 146 passenger trainset.

Four inward-sliding side doors are provided for each vehicle unit, with two doors on each side (front and rear) of the vehicle passenger cabin. The vehicle doors are 1.37 m (54 in) wide allowing for two-abreast emergency egress, if necessary, for lateral egress option "A". As shown in Figures 7-4 and 7-5, the guideway sidewall constitutes a 0.46 m (18 in) high obstacle to lateral egress from the vehicle doors to the emergency walkway. Deployable steps with folding handrails will be required to assist elderly and disabled passengers from the vehicle to the emergency walkway.

7.2.4 Vehicle Emergency Evacuation Within Guideway Switch Zones

Three different system guideway switch design concepts are proposed in the Foster-Miller SCD:

- A vertical switch design, shown in Figure 7-8, used for high speed mainline application; designated as switch Type I.

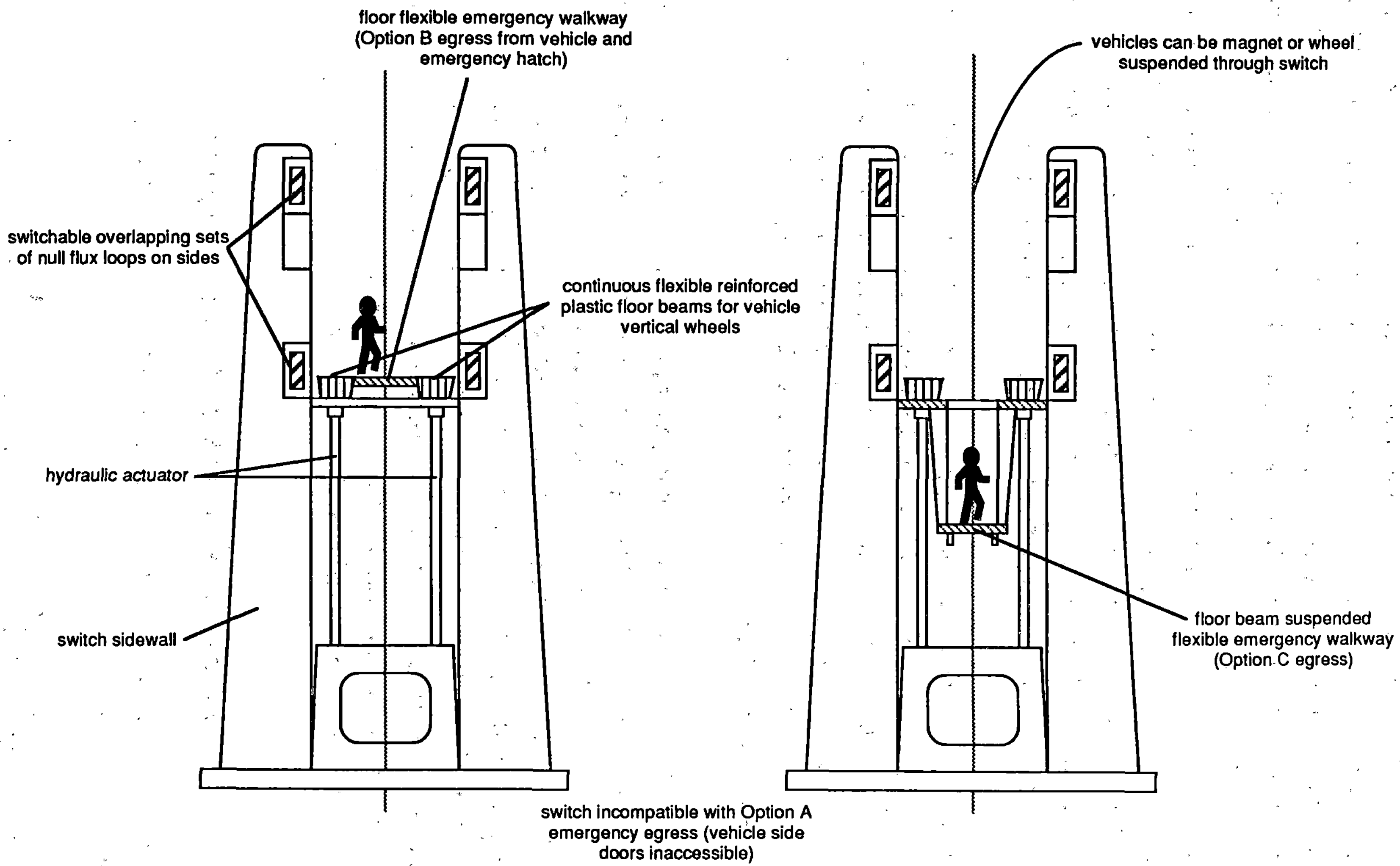


FIGURE 7-8. POSSIBLE APPLICATION OF FOSTER-MILLER EMERGENCY EGRESS MEANS TO PROPOSED TYPE 1 - HIGH SPEED VERTICAL SWITCH DESIGN CONCEPT (SWITCH EMERGENCY EGRESS NOT SCD ADDRESSED IN SCD REPORT)

- A lateral switch design, shown in Figure 7-9, used primarily for intermediate speed off-mainline application (e.g., in the vicinity of stations); designated as switch Type I.
- A lateral switch design used primarily for very low speed application (e.g., within terminals or maintenance yards); designated as switch Type III.

Proposed high-speed switch Type I, shown in cross-section in Figure 7-8, incorporates two overlapping sets of null-flux levitation coils in the vertically extending sidewalls of the switch structure. Electrically opening one and closing the other set of null-flux coil sets will vertically divert a switch traversing trainset into either an upper or lower track branch. If installed, continuous flexible and reinforced plastic floor members will be hydraulically actuated to be vertically positioned for the upper or lower track branch in conjunction with the electrical opening or closing of the null-flux coil sets. These Type I switch moveable floor members will provide the vehicle with wheel landing surfaces in the event of a magnetic suspension system failure while traversing the switch.

This Type I vertical switch design precludes placing emergency walkways along the sides of the guideway as required for emergency egress option "A" and shown in Figures 7-4 and 7-5. This switch design could, however, incorporate an emergency walkway between or suspended below the landing wheel floor members, as shown in Figure 7-8; this walkway is required for the fore/aft or the downward emergency egress options shown in Figures 7-6 and 7-7, respectively. Switch walkways should be designed to be flexible enough to accommodate vertical movement of the floor members.

The intermediate speed switch, Type II, shown in cross-section in Figure 7-9, incorporates the hydraulically actuated lateral displacement of multiple segmented length track sections supported by wheels running on laterally oriented rails.

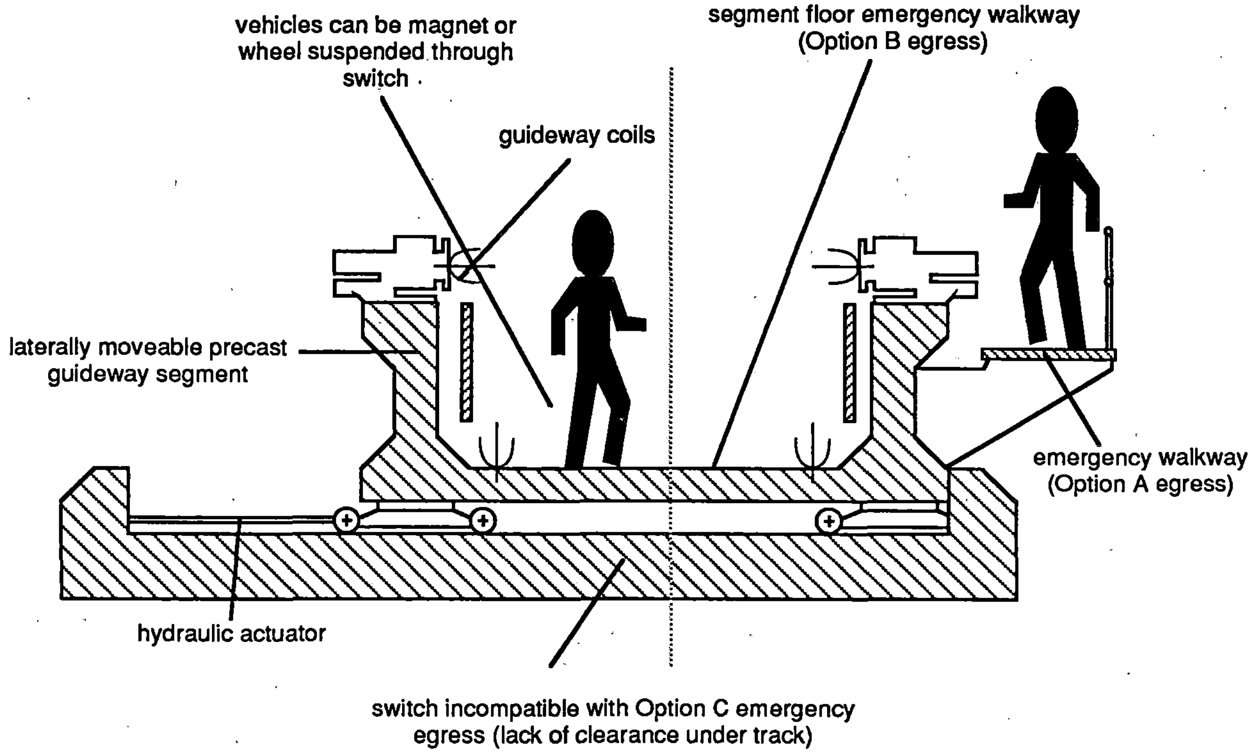


FIGURE 7-9. POSSIBLE APPLICATION OF FOSTER-MILLER EMERGENCY EGRESS MEANS TO PROPOSED TYPE II - LOW SPEED LATERAL SWITCH DESIGN CONCEPT (SWITCH EMERGENCY EGRESS NOT ADDRESSED IN SCD REPORT)

The Type II lateral switch design will allow for the location of an emergency walkway along either side of the moveable track segments, as required for the proposed lateral emergency egress option, shown in Figures 7-4 and 7-5. These walkways will be designed to have sliding, overlapped joints to allow for the small rotational movements of the segmented length track sections. This switch design inherently provides for the track floor emergency walkway, shown in Figure 7-9, required for the fore/aft emergency egress option. This lateral switch design precludes constructing the suspended emergency walkway required for the downward emergency egress option, shown in Figure 7-7. Table 7-1 below summarizes the feasibility of switch types with emergency egress options.

TABLE 7-1. COMPATIBILITY OF PROPOSED SWITCH CONFIGURATION TYPE WITH VEHICLE EMERGENCY EGRESS OPTIONS

Switch Type	Vehicle Emergency Egress Options		
	Lateral Option "A"	Fore/Aft Option "B"	Downward Option "C"
I	No	Yes	Yes
II	Yes	Yes	No

7.2.5 Vehicle Emergency Evacuation Within Superelevated Guideway Zones

The proposed vehicle's hydraulic active tilting system can tilt the vehicle up to 12 degrees from horizontal, and the guideway beam superelevation may be angled up to 12 degrees from horizontal. Thus, vehicles with operative tilting systems stopped on a superelevated segment, under emergency conditions, can be leveled to ease emergency egress from the train. While the first egress option can be implemented without complication, possible differences in angles between the vehicle floor and superelevated segments present fore/aft door egress difficulties for elderly and disabled passengers on walkways without handrails. Egress onto a suspended walkway is also difficult; downward egress is only possible for vehicles stopped on a superelevated curve that are tilted to match the superelevation angle. This tilting provides clearance for deployment of the vehicle floor door staircase or ladder to the suspended walkway. Possible differences between the vehicle and walkway angles also present difficulties for elderly and disabled passengers on walkways without handrails.

If the tilting system fails, the vehicle may experience tilting angles up to 24 degrees relative to the walkway; emergency egress onto guideway walkway from vehicle side doors becomes difficult for elderly and disabled passengers. Downward egress becomes virtually impossible because of stairway/ladder clearance requirements.

7.2.6 Vehicle Cabin/Crew Compartment Layout and Exits for Emergency Evacuation

Foster-Miller states that cabin aisle width, seating pitch, overhead baggage stowage bin facilities, emergency lighting, emergency exit sizes and emergency exit arrangements are consistent with commercial aircraft practices. The cabin layout is based on 2 x 3 business class seating at 1.0 m (39.4 in) pitch, 2 x 2 first class seating at 1.1 m (43.3 in) pitch, and 0.54 m (21.3 in) aisle width. This cabin layout is compatible with the commercial aircraft arrangements used to meet requirement for emergency evacuation of vehicle passengers and crew within 90 seconds of an emergency stop.

Four 1.37 m (54 in) wide entrance/exit doors, two per vehicle unit side, are provided in each vehicle unit. Each unit also has one wheelchair station. Each door, in the event of an emergency, will thus be required to evacuate only up to 37 passengers for the lateral egress option on the basis that only doors on one side of the vehicle will be available for emergency access, as shown in Figures 7-4 and 7-5. The corresponding evacuation rate for 37 passengers in a 90-second duration is one passenger every 2.4 seconds. The requirement to evacuate up to 50 passengers per available door for the Foster-Miller proposed vehicle design is consistent with aircraft practice. This emergency evacuation duration is considered more than adequate for a maglev vehicle where the risk of rapid fire spreading and/or explosion in vehicles is lower than the risks for aircraft where large quantities of liquid fuel are typically on-board.

Two 1.4 m (55 in) square emergency floor hatch doors are provided in each of the proposed vehicle units. Each floor hatch, in the event of an emergency, will thus be required to evacuate up to 37 passengers for the downward egress option, shown in Figure 7-7. The evacuation rate is identical to the previous rate; one passenger every 2.4 seconds.

Based on vehicle passenger capacity designs, nose and tail vehicle unit hatch-type exits will be required to evacuate up to 74 passengers for business class seating per vehicle unit to achieve a 90-second evacuation duration (i.e., a maximum of one passenger every 1.2 seconds per consist trainset). The awkwardness of egress, especially for elderly and disabled passengers, from the vehicle fore and aft emergency hatches (Figure 7-6) makes the realization of complete evacuation within the specified 90-second duration unlikely, even for the baseline two-vehicle unit trainset configuration.

The Foster-Miller proposed vehicle cabin layout satisfies the FAA commercial aircraft requirement that the maximum distance between any seat row and the nearest exit be less than 9 m (30 ft) by the to normal entry/exit doors for the lateral egress option "A" and the floor emergency hatch doors for the downwards egress option "C", but not when nose and tail-unit emergency hatch exits are used; evacuation through up to one half of the trainset overall length would be required in this latter case.

7.2.7 Advantages of Foster-Miller Emergency Response System

Emergency evacuation from a stopped vehicle onto a guideway-supported walkway, using either the lateral or the fore/aft egress option, will be possible over the entire guideway length, except as noted in Section 7.2.8.

Emergency evacuation from a stopped vehicle onto the guideway-supported emergency walkway for the lateral emergency egress option will be relatively easy to accomplish if deployable steps are available.

Two options for emergency egress from the guideway-supported emergency walkway to a "safe location" will be available for the lateral and fore/aft egress options, either via a staircase to ground level or via maglev rescue vehicle.

7.2.8 Safety Concerns for Foster-Miller Emergency Response System

The Foster-Miller SCD describes several emergency evacuation scenarios. In any emergency situation, there is always a tendency toward passenger panic. Under those circumstances, it is preferable to have a few consistently reliable options available for passengers to exit the vehicle. The Foster-Miller SCD describes several combinations, some of which will work in some circumstances and some of which will not work in others. Emergency evacuation from a stopped vehicle onto a guideway-supported walkway is not available for two of the six combinations of switch design and emergency egress options.

None of the three emergency egress options for superelevated curves are available when the vehicle tilting system is inoperative.

The downward vehicle emergency egress option appears to be limited by guideway track cross-member diaphragm and guideway pylon interference considerations, by design incompatibility with both lower speed switch designs and by implementation difficulties in highly superelevated track curves.

For trains with more than two vehicle units, the proposed fore/aft vehicle emergency egress option requires significantly longer vehicle evacuation times when compared to the other two Foster-Miller egress options.

Emergency evacuation through the nose and tail hatch exits for the fore/aft emergency egress option is hampered by the extra time needed to navigate through the hatch; passage through these hatches is slow because of the hatch size and orientation imposed by the aerodynamic nose and tail section design.

Emergency evacuation through the vehicle floor hatch-type exits down descending ladders or staircases to the emergency walkway suspended below the track for the proposed downwards vehicle emergency egress option will be difficult, particularly for disabled and/or elderly passengers.

The guideway sidewall constitutes an obstacle to lateral egress from the vehicle side doors to the emergency walkway. Deployable steps will be required to assist elderly and disabled passengers.

The close proximity of the emergency walkway (for the lateral egress option vehicle evacuation) to the adjacent track of a dual track guideway will require drastic speed reductions or complete stoppage of all vehicle traffic on the adjacent track to minimize or eliminate vehicle-induced wind and acoustical noise impact on walkway occupants.

There is no way of knowing exactly where evacuated passengers and crew are located along the track at any given time or when the track is completely cleared of all passengers and crew, unless the proposed closed-circuit TV camera surveillance coverage is extended to the entire guideway length.

Further study is required to determine appropriate evacuation rates for maglev vehicles. Because maglev vehicles do not carry large amounts of fuel on-board, as do airplanes, the 90-second evacuation goal may be too stringent.

7.3 GRUMMAN

7.3.1 Communication During an Emergency

During emergency situations, communication between vehicles and system central control occurs using vehicle-to-wayside ultra-high-frequency (UHF) radio communication/data transfer links. All ground communication/data transfer between system wayside controllers and central control is via a fault-tolerant fiber optic cable network.

The SCD identifies the need for extremely high reliability of the communications link between the vehicles and the wayside regional centers. The SCD states that loss or significant deterioration of this communication link will invoke a system-wide emergency stop.

Potential sources of unreliability for the proposed communications system and techniques to optimize radio link reliability are extensively addressed in the SCD.

A potentially serious problem is the baseline system UHF radio transmission multipath interference problem. This results from the radio waves being reflected off terrain or other ground objects. Grumman plans to minimize this problem by continually comparing signal quality among a number of wayside transceivers distributed along the guideway length at nominal 2 km (1.2 mi) intervals. This wayside transceiver spacing allows for nearly continuous geometric line-of-sight transmission, ideal for optimal UHF radio link reliability. Grumman plans to use an array of fixed antennas at wayside-located receiving sites and multiple antenna/receiver combinations on the vehicle, combined with directional polarization transmission multiplicity. The strongest signal is automatically selected from each wayside antenna array. Two vehicle antennas are proposed, separated by as great a distance as possible, with redundant transceivers for each antenna.

A "leaky" transmission line or waveguide vehicle-to-guideway communication link, based on or near field-coupling between the vehicle antenna and guideway transmission line located in close proximity, is suggested as an alternative to the baseline radio link if an insufficient number of radio frequency channels are available because of system frequency allocation limitations.

The proposed baseline UHF radio link vehicle-to-guideway communication system has a high degree of redundancy and the inherently high reliability of a line-of-sight transmission system. The fiber optic cable networks proposed for the system ground communications can be designed to be exceptionally reliable by using state-of-the-art availability enhancement techniques.

Accordingly, the proposed communication system reliability and availability appear adequate for use in emergency conditions to control the train and to provide subsequent evacuation instructions to passengers.

Grumman recommends one on-board attendant on the baseline 100-passenger vehicle to provide for passenger needs and supervision and to assist in emergency situations, especially evacuation. This attendant/passenger ratio does not meet the current commercial aircraft federal regulations which require one on-board attendant for every 50 passengers. Any emergency response-related information will be transmitted to the vehicle attendant, who will then communicate vital information to the passengers via the on-board public address system.

7.3.2 Emergency On-Board Power Supply

The predicted vehicle electrical power demand of about 170 kw requires an on-board battery power supply. The proposed lead-acid battery weighs approximately 6000 lbs (i.e., about 4.5% of the estimated loaded baseline vehicle weight). This power supply will provide power for up to 30 minutes for vehicle operations when power transfer from wayside via vehicle induction coil pickup of the linear propulsion motor harmonics is unavailable because the train is traveling at speeds less than 161/241 km/hr (100/150 mph).

An emergency electrical power supply independent of the on-board normal electrical power supply is not specifically addressed in the SCD. The issue of providing a highly reliable on-board emergency power supply with the required capacity to provide all needed suspension, braking, lighting, and communication functions during any emergency stop and vehicle evacuation should be addressed.

7.3.3 Vehicle Emergency Evacuation Strategy

The Grumman evacuation strategy requires passengers to remain on-board except at scheduled station stops and in life-endangering emergency situations. This strategy allows for continued operation of the system after detecting faults; the vehicle operates with degraded performance or restricted operation which either prevents life-endangering hazardous situations or minimizes their probability.

Vehicle emergency evacuation over the length of the guideway will be via the normal entry/exit doors and/or emergency exit windows on either side of the vehicle. Passengers will egress onto the top slab of the dual guideway center spine girder which forms a horizontal platform surface 3 to 4 m (10 - 13 ft) wide, shown in Figure 7-10. Passengers and crew then transfer to a rescue vehicle or egress to ground level via emergency staircases. These staircases will be located every 10 to 20 girder span-lengths along the guideway.

The SCD proposes standardized 50-passenger vehicle modules which can be fitted with nose and tail sections; these end sections will contain a crew compartment and a storage bay. This modularized design approach allows for a single 50-passenger vehicle, a double-module 100-passenger trainset which is designated the baseline configuration, or longer multiple module trainsets, depending on system capacity requirements. Each vehicle module is provided with

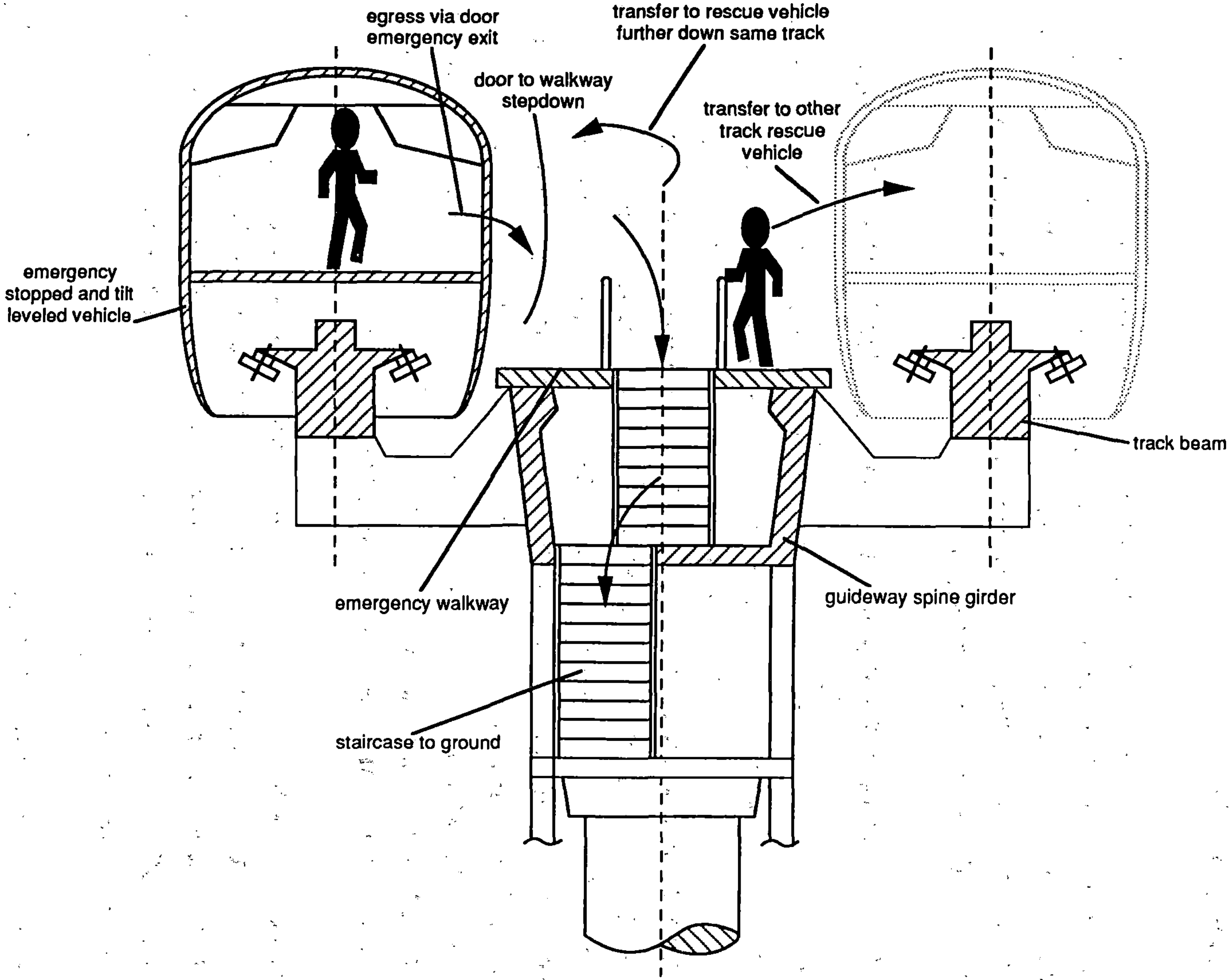


FIGURE 7-10. GRUMMAN PROPOSED VEHICLE EMERGENCY EGRESS MEANS

two power-operated sliding doors 0.81 m (32 in) wide, one on each side of the module, for normal entry/exit and emergency egress. Module 4/5 m x 9/5 m (0.8 ft x 1.8 ft) windows are provided, some of which are intended to be "popped out" for use as additional emergency exits.

There is a 1 m (3.3 ft) vertical separation between the vehicle floor and the emergency egress platform, which is evident in Figure 7-10. A deployable short ladder or folding staircase will be required to assist elderly and disabled passengers during egress. This is not addressed in the SCD.

7.3.4 Vehicle Emergency Evacuation Within Guideway Switch Zones

The proposed guideway switch design does not incorporate the center structural spine girder with the vehicle track beams cantilevered on both sides of the girder suggested in the baseline guideway configuration shown in Figure 7-11. Instead, the individual track beams of the switch are supported on pier cross-beam members located at 15 m (49.5 ft) intervals along the length of the switch. A front section of the switch length incorporates a bending track beam while the rear section has a rotating and laterally translating switch dual beam. These switch moveable beams have steel rollers running on steel rails mounted on the pier cross-beam members, shown in the switch cross-section in Figure 7-11.

Although not addressed in the SCD report, emergency egress walkways could be cantilevered to the fixed outside beam and to the moveable outside beam of the switch, but vehicle clearance requirements preclude adding such a walkway to the center moveable beam of the switch as indicated in Figure 7-11.

Thus, emergency egress onto a narrow walkway will be possible only over the length of the switch design on the switch turn-out branch, but not over the length of the rotating/laterally translating rear section of the straight-through branch.

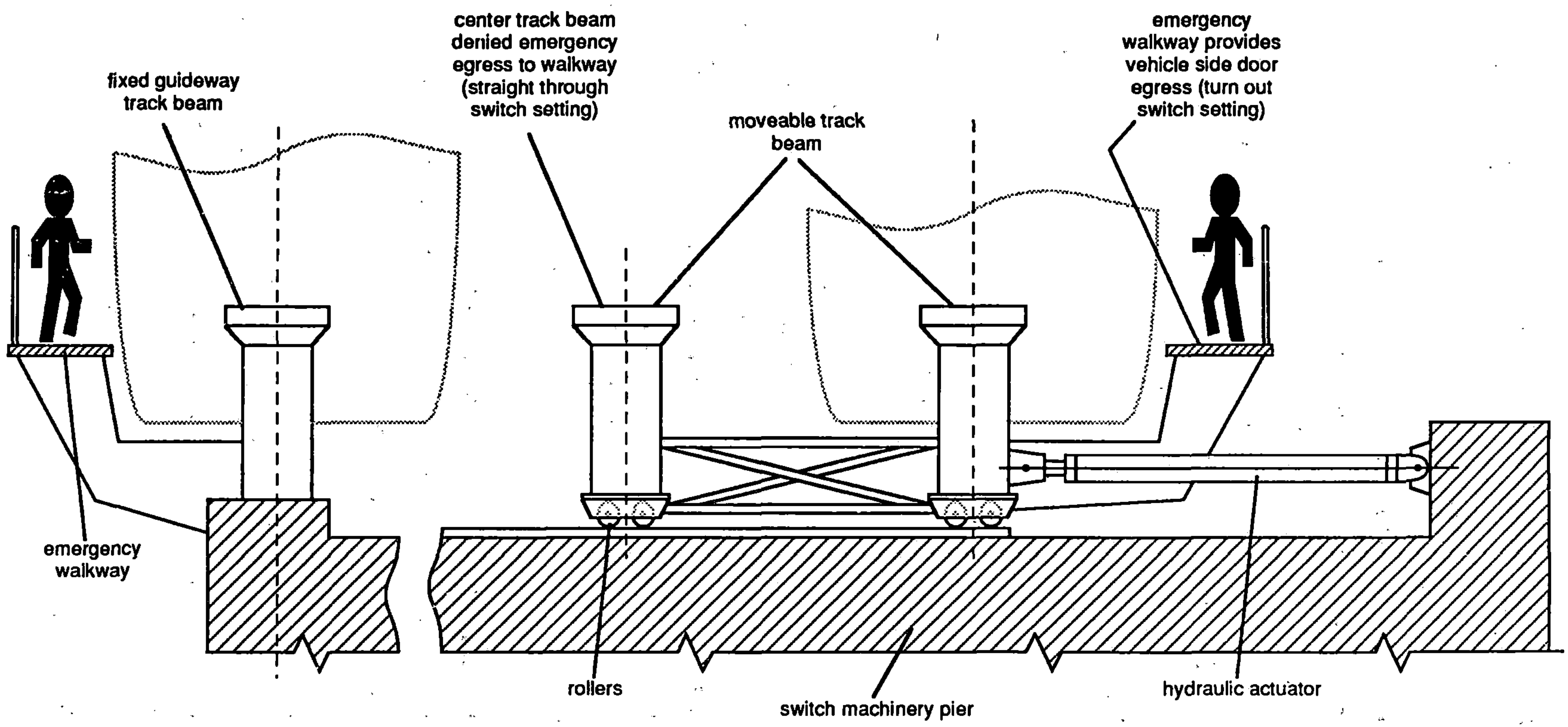


FIGURE 7-11. POSSIBLE APPLICATION OF GRUMMAN EMERGENCY EGRESS MEANS TO PROPOSED LATERAL SWITCH DESIGN CONCEPT (SWITCH EMERGENCY EGRESS NOT ADDRESSED IN SCD REPORT)

7.3.5 Vehicle Emergency Evacuation Within Superelevated Guideway Zones

The proposed vehicle's hydraulic active tilting system can tilt the vehicle up to nine degrees from horizontal; and, the guideway track beam superelevation angle may be up to 15 degrees from horizontal. Thus, vehicles with operative tilting systems thatare stopped on a superelevated track segment can be leveled to within six degrees of horizontal to ease emergency egress from the train. If the tilting system fails, however, the vehicle may experience tilting angles up to 24 degrees from the walkway and emergency egress onto the guideway walkway from vehicle side doors will be difficult.

7.3.6 Vehicle Cabin/Crew Compartment Layout and Exits for Emergency Evacuation

The aisle width, seating pitch, overhead baggage stowage bin facilities, emergency lighting, emergency exit sizes, and emergency exit arrangements are consistent with commercial aircraft regulations (2 x 3 business class seating at 96.5 cm (38 in) pitch with 56 cm (22 in) aisle width specified). The cabin layout is compatible with the requirements for emergency passenger and crew evacuation within 90 seconds of an emergency stop.

This 90-second duration is considered by Booz•Allen to be more than adequate for a maglev vehicle where the risk of rapid fire spreading and/or explosion is lower than the risks associated with aircraft.

Four 0.8 m (32 in) wide entrance/exit doors, two per train side (one per module set), are provided for the baseline dual module 100-passenger trainset configuration. Accordingly, each door will be required, in the event of an emergency, to evacuate up to 50 passengers. Only doors on one side of the vehicle will be available for guideway spine girder platform emergency egress, as shown in Figure 7-11. This evacuation rate corresponds to one passenger every 1.8 seconds to achieve an evacuation time of 90 seconds. The requirement to evacuate up to 50 passengers per door for the Grumman proposed vehicle design is consistent with aircraft practice.

7.3.7 Advantages of Grumman Emergency Response System

Emergency evacuation from a stopped vehicle onto the guideway walkway will be available over the entire guideway length, except for some portions of a switch, and through superelevated curves for a vehicle with an inoperative tilting system. Emergency evacuation from a stopped vehicle onto the guideway walkway will be relatively easy with vehicle-deployable short ladders or stairs.

Two options for emergency egress from the guideway walkway to a point of safety will be available:

- Via a staircase to ground level and
- From the walkway onto a rescue vehicle.

The system guideway capital costs associated with providing emergency evacuation means from a stopped vehicle to an emergency walkway is minimal because the top of the spine girder of the dual-track guideway structure will function as a walkway. Therefore, the costs of providing for emergency evacuation are limited to constructing egress staircases from the walkway to ground at spaced intervals.

Further study is required to determine appropriate evacuation rates for maglev vehicles. Because maglev vehicles do not carry large amounts of fuel on-board, as do airplanes, the 90-second evacuation goal may be too stringent.

7.3.8 Safety Concerns for Grumman Emergency Response System

With an inoperative vehicle cabin tilting system, emergency evacuation from a stopped vehicle onto the guideway spine girder top walkway will be difficult through highly superelevated guideway curves. These conditions will make evacuation difficult for disabled and elderly passengers.

The close proximity of the emergency walkway to the adjacent track of the dual-track guideway requires drastic speed reductions or complete stoppage of all vehicle traffic on the adjacent track to minimize or eliminate vehicle-induced wind and acoustical noise impact on walkway occupants.

The 1 m (3.3 ft) vertical separation between the vehicle floor and the emergency egress platform requires a deployable short ladder or folding staircase to assist elderly and disabled passengers during egress. This is not addressed in the SCD.

7.4 MAGNEPLANE

7.4.1 Communication During an Emergency

During emergency situations, communication between vehicles and system central control occurs using vehicle-to-wayside radio and fiber optic communication/data transfer links. All ground communication/data transfer between system wayside controllers and central control is via a fault-tolerant fiber optic cable network.

The SCD specifies the need for at least one attendant to be on-board each Magneplane vehicle in operation. Attendants have access to a display unit which provides a summary status of the vehicle operations and any data/messages received across the radio frequency link from the "global" control center. Both keyboard and voice communication will be available across the radio frequency link. Any emergency response related information can be transmitted to the vehicle attendant both aurally and textually, thus reducing the likelihood of communication errors. The attendant will notify the passengers via the on-board public address system or a provided megaphone and assist passengers during subsequent emergency evacuations.

The least reliable element of the emergency response communications system is the vehicle-to-wayside radio frequency link. This link may be susceptible to electromagnetic interference effects or to atmospheric-induced propagation uncertainties, and could malfunction or fail because of transmitter and/or receiver equipment faults. Radio frequency link reliability factors, such as line-of-sight transmission, ultra-high-frequency highly-directional beam transmission and on-board plus wayside transmitter/receiver redundancy should be addressed in subsequent program phases.

7.4.2 Emergency On-Board Power Supply

A sealed conventional lead-acid battery on-board power supply subsystem is specified in the SCD (25 and 33 kwh for the 45- and 140-passenger vehicles, respectively); the battery array is divided into left and right-hand sections for fault tolerance purposes. An otherwise separate on-board emergency electrical power supply, used primarily for emergency lighting and communications purposes, is not specifically identified in the SCD, although either section of the on-board battery power system may power the vehicle during emergencies because of the redundant configuration.

With respect to vehicle emergency power loads, any emergency situation requiring the rapid stopping of the vehicle, followed by an urgent evacuation of passengers and crew, can be expected to only require a small supply of emergency power. There should be sufficient thermal capacity in the superconducting magnet dewars to provide for electrodynamic suspension during a vehicle emergency deceleration to a stop without reliance on cryocooler operation.

Proposed hydraulic actuator deployment of the on-board emergency braking skids for rapid deceleration (estimated to be about 0.45 g's at high speed and increasing to about 0.6 g's at the low speed magnetic drag peak) is independent of any on-board electrical power supply; these brakes are actuated by firing an air/hydraulic accumulator. Although not specifically stated in the SCD report, it is conceivable that low speed landing air pads could be similarly deployed without reliance on an on-board emergency electrical power supply in cases where a reduced deceleration emergency stop is necessary. Furthermore, cabin air conditioning and heating loads should be minimal during a vehicle emergency stop and urgent evacuation.

7.4.3 Vehicle Emergency Evacuation Strategy

The overall strategy for emergency evacuation recognizes that different circumstances will require significantly different means to allow passengers to move to a safe location following an incident.

For stations and maintenance areas which have platforms, four side doors are provided for both the 45- and 140-passenger vehicle designs, with two doors on each side near both the front and rear of the vehicle passenger cabin. The sliding doors open and close by compressed-air-driven actuators. The vehicle doors are approximately 1.2 m (4 ft) inches wide allowing for two-abreast emergency egress, if necessary.

Four window panel emergency exits are provided for both the 45- and 140-passenger vehicle designs, with two exits on each side between the front and rear doors of the vehicle passenger cabin. These emergency exits are specified as aircraft Type I which must have rectangular openings sized no smaller than 0.6 m x 1.2 m (2 ft x 4 ft). These exits may be used in the event that the vehicle does not come to rest in an upright position.

Emergency evacuation along the guideway outside of stations and maintenance areas is provided via hatch-type exits at each end of the vehicle which permit passengers to egress onto the guideway track semicircular trough shown in Figure 7-12. The staircase shown in Figure 7-12 integrated with the hatch door to assist in emergency egress, is not included in the SCD design.

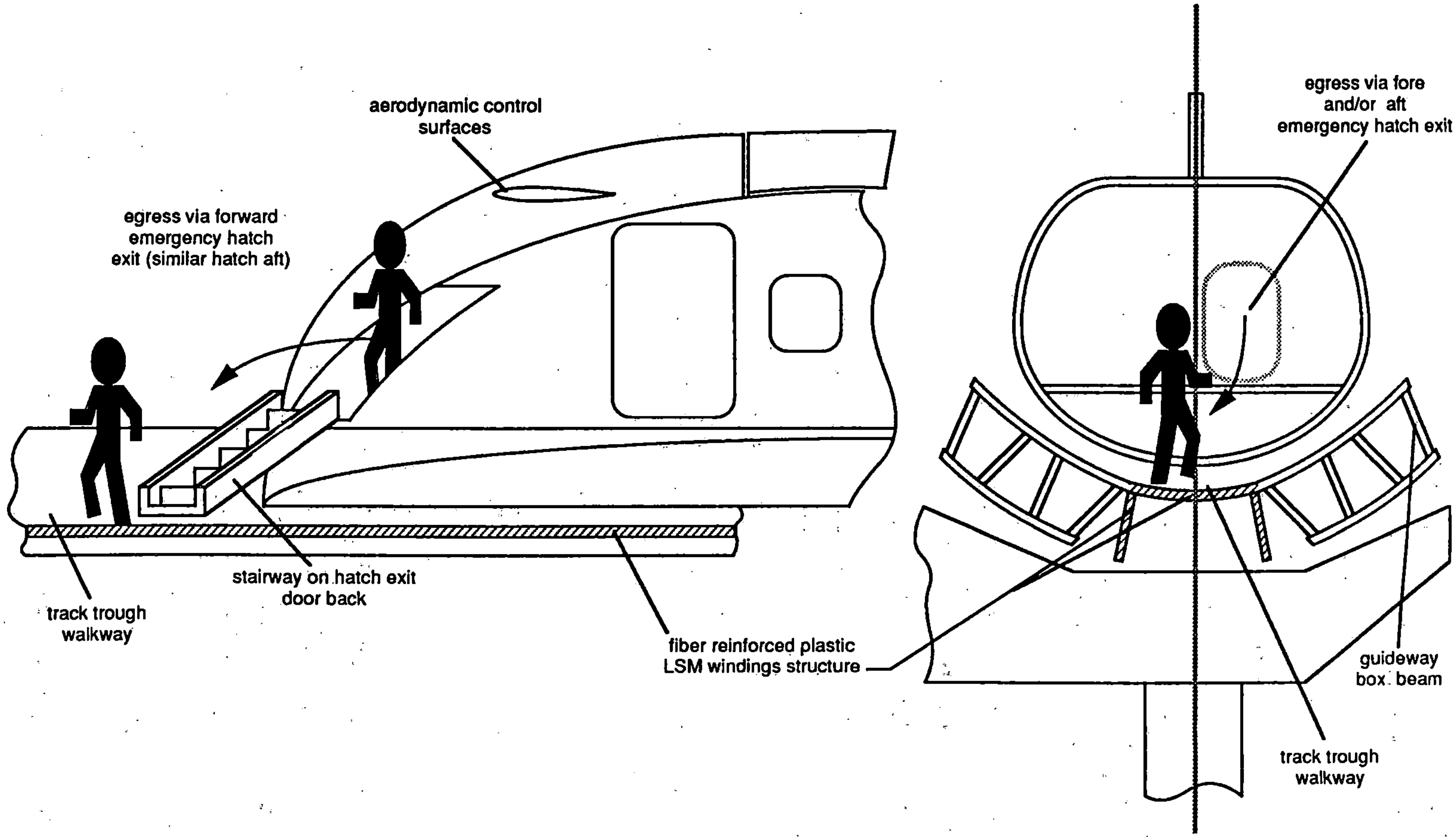


FIGURE 7-12. MAGNEPLANE PROPOSED VEHICLE EMERGENCY EGRESS MEANS - VEHICLE TO GUIDEWAY PATH

The guideway surface, where the evacuated passengers/crew will walk, consists of a fiber-reinforced plastic curved support structure for propulsion system LSM windings. This LSM winding support structure is designed to withstand considerable linear motor-induced loading, and thus will not be compromised by the additional loading of egressing passengers. The radius of the guideway cross section is 2.1 m (7 ft). Accordingly, the local curvature of the walkway, shown in Figure 7-12, should not impede safe movement. The walkway height increase, from the trough center to the edge of a nominally 0.5 m (1.6 ft) wide "single-file walking right-of-way," is about 1.4 cm (.55 in).

The temperature of the guideway can be anticipated to be higher than the surrounding ambient air temperature. This heating is caused by sunlight radiating heat and the ohmic resistance heating of the LSM windings and aluminum sheets. Although guideway heating is discussed for eliminating ice and snow, emergency egress concerns were not addressed by Magneplane.

A thermal analysis is provided that indicates the guideway temperature may rise 72° C (161° F) above ambient air temperature during minimum headway operations at a speed of 30 m/s (67 mph).

High frequency vehicle operation may increase the temperature of the metal guideway to that of boiling water. Clearly, if this condition prevails at the location of an emergency evacuation, passengers may be burned by contact with the metal portions of the guideway. If the fiber-reinforced plastic structure is insulated from the metal portions of the guideway, then the risk of such exposure may be reduced. However, in the panic of an emergency evacuation, there can be no assurance that passengers will remain on the plastic structure.

Evacuated passengers egress from the guideway trough to a point of safety using a small hinged stairway; this stairway may be deployed from a storage location on a guideway local, platform-mounted between the side box beams of a dual guideway. This hinged stairway will swing over the trough, shown in Figure 7-13, to allow the passengers/crew to climb out of the track trough and over the side box beams. Such hinged stairways and associated local emergency platforms will be provided at intervals along the guideway length. The suggested maximum spacing between these egress locations and an emergency platform is specified by the SCD to be approximately 0.76 km (0.5 mi).

The local emergency platform allows for transferring passengers/crew to a standard revenue system maglev rescue vehicle, either on the same or an adjacent track, shown in Figure 7-13.

Alternatively, passengers/crew may walk along the guideway track trough to the nearest station where a small hinged stairway, similar to that described above and shown in Figure 7-13, will provide access to the station platform.

A wider stairway may be provided from the local emergency platforms to ground level, as shown in Figure 7-13. These stairways will be counterbalanced for self-stowing and will be normally inaccessible from the ground.

The SCD does not address the issue of system reactivation activities; there is no mention of checking if guideway segments are clear of evacuated passengers and crew. Continuous monitoring of the guideway tracks with closed circuit TV camera surveillance, presumably capable of providing for clear track assurance, is proposed for critical locations, but this surveillance system will only cover about 10% of guideway length.

7.4.4 Vehicle Emergency Evacuation Within Guideway Switch Zones

The Magneplane system guideway switching concept widens the guideway by increasing trough flat bottom width to form a guideway side branch. A vehicle traversing the switch section at speed is electrodynamically guided along either the switch-trough branch

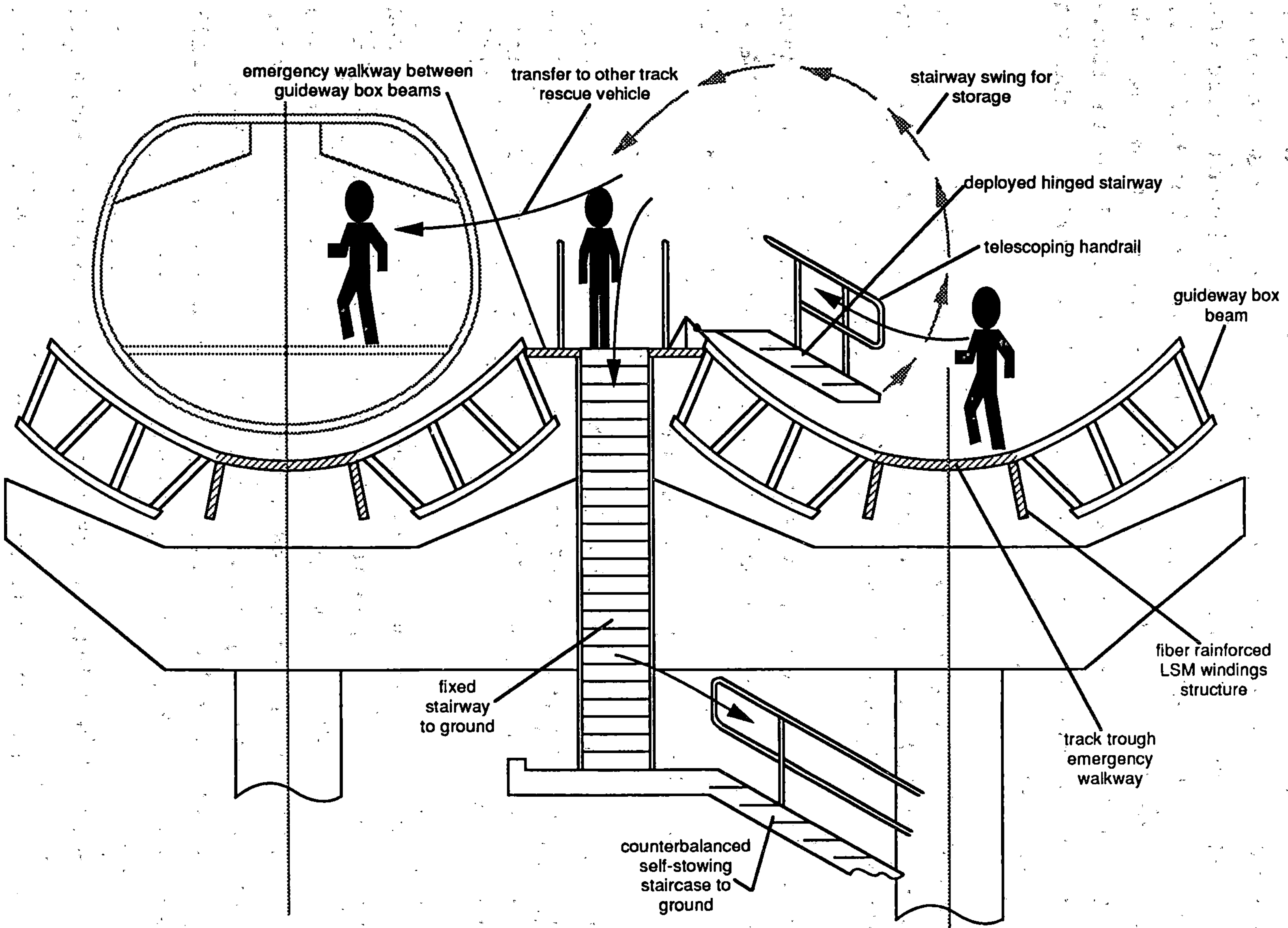


FIGURE 7-13. MAGNEPLANE PROPOSED VEHICLE EMERGENCY EGRESS MEANS GUIDEWAY TO GROUND OR TO RESCUE VEHICLE EGRESS

or into the switch side branch without using moving parts. By selectively short-circuiting one of the two sets of passive null-flux loop coils embedded in the guideway surface directly below the centerline paths of the switch traversing vehicles, operators can guide the vehicle as desired. Null-flux loop coils are guideway-embedded directly on corresponding LSM windings which are powered in accordance with the selected switch branch.

Spaces on each side of the embedded null-flux loops and LSM windings are completely filled with concrete to provide a flat running surface, shown in Figure 7-14. This flat surface is required for the air suspension pads which extend downward from the sides of the vehicle when it is traversing through the switch at low speed (i.e., when the electrodynamic suspension is inadequate). These flat surfaces through the guideway switches also allow for evacuation through the hatch-type emergency exits at both ends of each maglev vehicle onto the section within guideway switch zones in a manner similar to the emergency egress procedure onto standard dual track guideways. These switch flat surfaces provide a walkway through the switch to the nearest hinged stairway which provides access over the track structural box frame to a guideway local emergency platform.

7.4.5 Vehicle Emergency Evacuation Within Superelevated Guideway Zones

The Magneplane vehicle is physically free to roll within the guideway semi-circular trough when traversing curves, but is limited by electrodynamic side forces which tend to act about the vehicle roll axis to keep the vehicle propulsion magnets almost directly over the LSM (known as vehicle "keel effect"). The guideway section troughs are effectively "superelevated" because the guideway banking results in essentially zero lateral forces relative to the vehicle's fixed axis for trains traversing the curve at the designed speed. The "superelevation" through curves is implemented by means of the appropriate angular displacement of the LSM windings and the associated side levitation plate box

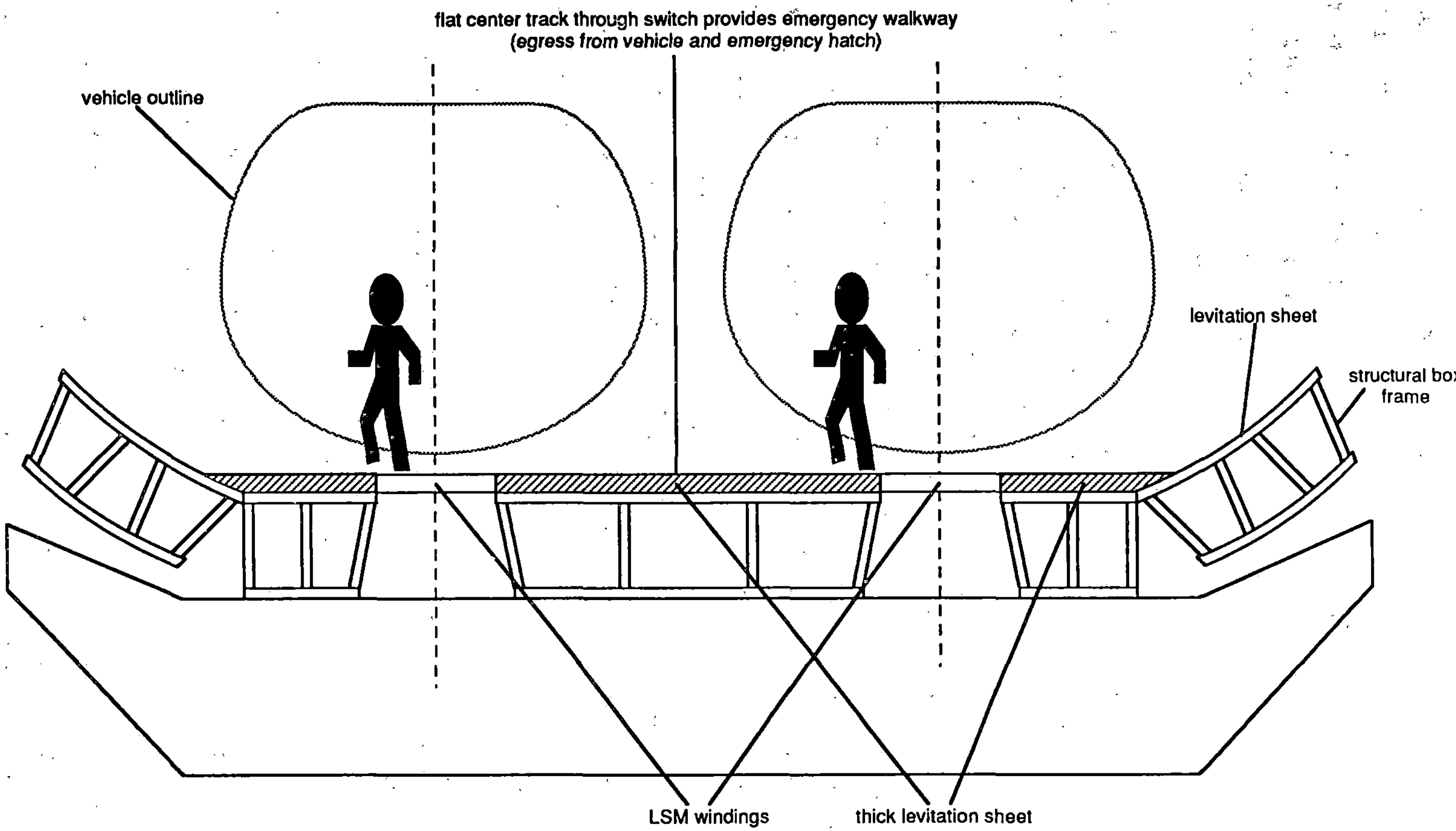


FIGURE 7-14. POSSIBLE APPLICATION OF MAGNEPLANE EMERGENCY EGRESS MEANS TO PASSIVE LATERAL SWITCH DESIGN CONCEPT

structures about the center of the trough cross-sectional curvature.

During emergency stopping on a guideway section curve, the vehicle "keel effect" roll stiffness should progressively diminish as the speed decreases towards zero, provided that each emergency braking skid produces the same friction forces. This would allow the vehicle to roll in toward a horizontal position using the pendulous action caused by gravity. The pendulous action occurs because the vehicle's center of gravity is vertically below the center of the track trough cross-sectional curvature.

Therefore, provided that the emergency braking skids function correctly, any vehicle stopped on a guideway curve will be level. The guideway trough walkway is available through curves for passenger/crew movement away from the stopped vehicle to a rescue vehicle, a station platform, or a ground level location. If the superelevation induced "bank angle" is high, such as the bank angle of a curve designed for high speed, the guideway walkway may be located on the levitation sheet portion of the trough, and not on the LSM winding support structure. However, this levitation sheet walkway would likely not be perceived by evacuating passengers/crew to be any different from a tangent LSM winding support structure walkway.

7.4.6 <u>Vehicle Cabin/Crew Compartment Layout and Exits for Emergency Evacuation</u>

The aisle width, seat pitch, overhead baggage stowage bin facilities, emergency lighting, emergency exit sizes and opening/ identification/accessing of emergency exit arrangements are consistent with commercial aircraft requirements.

The maglev vehicle fire protection requirements are specified to be in accordance with FAA aircraft requirements. Therefore, Magneplane considered a 90-second emergency evacuation more than adequate for a maglev vehicle where the risk of rapid fire spreading and/or explosion is lower than with aircraft, due to the lack of large quantities of liquid fuel on-board.

If current aircraft design standards are applied to Magneplane vehicles, then fore and aft hatch-type exits must be capable of evacuating 23 or 70 passengers, respectively for 45- and 140-passenger vehicles, within 90 seconds in the event of an emergency (i.e., a maximum of one passenger every 1.3 seconds). Egress from the hatch-type exits would be awkward, as illustrated in Figure 7-13. Therefore, realization of a 90-second evacuation seems unlikely for a 140-passenger vehicle under conditions of passenger panic.

The FAA requires that for commercial aircraft, the maximum distance from any seat row to the nearest exit be 9 m (30 ft) to ensure ease of egress in an emergency. This requirement is easily satisfied by the proposed maglev vehicle cabin layout for normal entry/exit doors, but not for the emergency hatch exits. Adherence to this requirement minimizes the distance to exits for all passengers and thereby improves the chances of safe egress during an emergency.

7.4.7 Advantages of Magneplane Emergency Response System

Emergency information can be transmitted both aurally and textually from the global control center to the vehicle attendant. This redundant presentation of vital information can reduce communication errors during an emergency.

Emergency evacuation from a stopped vehicle onto the guideway trough will be available over the entire guideway length, including switches and superelevated curves.

The system capital costs associated with providing emergency evacuation from a stopped vehicle to a safe location will be minimal because the guideway track trough functions as the emergency walkway. Passengers and crew travel along the walkway to a deployable staircase transfer point where a track-attached local emergency platform will be provided.

Two options for emergency egress from the guideway walkway to a safe location will be provided. A hinged staircase is available for egress over the box beam onto a guideway-attached local emergency platform. Passengers can then egress via a staircase to ground level or from the platform into a rescue vehicle. Two egress options will be of considerable value in the event that one egress path is blocked or unsafe due to the specific emergency conditions.

7.4.8 Safety Concerns For Magneplane Emergency Response System

In emergencies requiring evacuation (e.g., during an on-board fire or major guideway damage), passengers and crew will egress onto the guideway, not on to a dedicated walkway physically separated from the operational troughs. There is no way of knowing exactly where evacuated passengers and crew are located along the track at any given time or when the track is completely cleared of all passengers and crew, unless the proposed closed-circuit TV camera surveillance coverage is extended to the entire guideway length.

The least reliable element of the emergency response communications system is the vehicle-to-wayside radio frequency link. Therefore, radio frequency link reliability factors need to be addressed in subsequent program phases.

A 90-second evacuation through the hatch-type exits at the front and rear of the vehicle may not be possible for the 140-passenger configuration. Further study is required to determine appropriate evacuation rates for maglev vehicles. Because maglev vehicles do not carry large amounts of fuel on-board, as do airplanes, the 90-second evacuation goal may be too stringent.

Vehicle evacuation through nose and tail hatch-type exits can be difficult because of the hatch size and orientation imposed by the low aerodynamic drag nose and tail section design; egress through these exits may be especially difficult for physically challenged and/or elderly passengers.

Finally, the guideway surface, where the evacuated passengers/crew will wail, consists of fiber-reinforces plastic support structure for the LSM windings. If thermal projections for guideway heating under high frequency train operations prove to be correct, evacuated passengers may be exposed to and burns if they do not remain on the plastic portion of the guideway.

8. SAFETY PERFORMANCE GOALS AND SPECIFIC DESIGN REQUIREMENTS

The proposed SCD maglev technologies have features that are unique to this mode of ground transportation. These features include:

- High speed (>482 kmph [300 mph]) at or near ground level;
- Lightweight vehicle structure, more like an airframe than a conventional passenger railcar;
- Propulsion, suspension, and braking systems that are not adhesion dependent;
- Highly automated command, control, and communications equipment; and
- Guideway alignments that could make evacuation in an emergency difficult.

Alone and in combination, these features present hazards that are presently outside the experience of the U.S. railroad industry and the FRA regulatory environment.

The existing FRA regulations applicable to passenger train safety are contained in the Code of Federal Regulations, Title 49, Transportation (49 CFR), Parts 200-240 [15]. The FRA regulations relate to safety concerns that are primarily applicable to steel-wheel-on-railroad technology and were adopted as the result of years of conventional railroad operating experience. Many of the existing FRA regulations and guidelines can be directly applied to maglev systems and others can be applied in concept to achieve a high level of safety. However, several safety requirements contained in existing FRA regulations are not applicable to the SCDs or other maglev systems proposed for U.S. operations.

Safety requirements must address generic maglev safety issues while at the same time be applicable to any proposed maglev system technology. They must also be stringent enough to ensure safe maglev operation while not limiting the innovative engineering effort required to maximize this new technology. The use of traditional methods to create technology-specific requirements is currently not possible because U.S. maglev system development is still in the concept definition phase.

This chapter presents a preliminary list of ***safety performance goals*** and ***specific design requirements*** for maglev systems. Each ***safety performance goal*** contains two elements: (1) an undesirable top level event and a probability goal which must be verified through quantitative analysis, or (2) an acceptable qualitative approach. Acceptable methods for showing compliance with ***safety performance goals*** are outlined in Appendix A. The list of ***safety performance goals*** should not be considered exhaustive. Using the PHA described in section 2.4.2 of this report, a more comprehensive set of ***safety performance goals*** should be developed by the organization(s) which have design responsibility over subsequent phases of maglev development.

Based on known hazards and proven design solutions for mitigating those hazards, a preliminary list of ***specific design requirements*** is also provided. ***Specific design requirements*** present particular design characteristics that must be incorporated in proposed maglev systems. Compliance with the ***specific design requirements*** shall be verified through analysis, testing, and/or inspection, as appropriate.

Although many of the identified safety design requirements are generic and apply to any maglev design concept, certain requirements apply to specific technologies. For example, maglev vehicle concepts that do not incorporate landing gear will not have to comply with specifications that relate to landing gear. Unless otherwise noted in supporting text, each requirement is considered applicable to any proposed maglev design concept. several of the safety design requirments include quantities (e.g., temperature, g-force valuaes, time etc.) which are to be determined). Insufficient information is available at this time to provide the TBD quanities. The additional analysis required to provide this information is outside the scope of this report. Appendix F summarizes the preliminary list of *safety performance goals* and *specific design requirements* and identifies their applicability to specific SCDs and subsystems.

8.1 VEHICLE STRUCTURE AND INTERIOR DESIGN

Proposed maglev vehicle structures must be thoroughly analyzed for accident survivability. Collisions could lead to massive structural collapse and can lead to serious and fatal injuries to the train crew and passengers. In addition to vehicle-to-vehicle collisions, the maglev structural design must also consider impacts caused by high speed landings, birdstrikes, bullets, and obstructions.

To increase speeds through curves, the Bechtel, Grumman, and Foster-Miller SCDs propose incorporating actively controlled tilt mechanisms. Failures of the tilting mechanisms must be reviewed with respect to failing to tilt and inadvertent tilting.

8.1.1 Safety Performance Goals

As a result of a collision, casualties could occur as a result of a occupant compartment crush and subsequent loss of volume, occupant compartment penetration, occupant ejection, and secondary impacts of an occupant with the interior of the compartment, with another occupant, or with a loose object such as luggage. To protect occupants, *maglev vehicle design should provide for controlled structural collapse to dissipate the vehicle kinetic energy as well as limit accelerations levels, preserve occupant compartment structural integrity to provide as least a minimum survival time, and restrict the impact forces that are applied to occupants during secondary contacts to accepted human tolerance levels [11].*

8.1.2 __Specific Design Requirements__

Since maglev vehicles will be required to be lightweight, vehicle structures will likely resemble aircraft structural designs more than locomotive structures. Therefore, MU locomotive requirements contained in 49 CFR, Part 229.141 should not not apply to maglev vehicles. In general, the maglev structure requirements should be defined in terms of loadings, crashworthiness, damage tolerance, corrosion, lightning protection, and maintenance specifications. Additionally, structures designed to support on-board equipment structures must be designed to withstand forces caused by a high-speed landing. ***The equipment and its mountings shall be designed to withstand, without separation, the ultimate inertia loads resulting from a high-speed landing.*** This requirement is particularly important to on-board systems carrying hazardous materials (i.e., cryogenic dewars and fuel cells).

The use of composite materials, as proposed by the Foster-Miller and Magneplane SCDs, must consider the special maintenance, failure detectability, and delamination. ***For maglev systems that incorporate composites materials, matrix material surfaces exposed to ultraviolet light must be painted to prevent chemical changes and degradation of the material properties.*** Methods to ensure that structural failure are detectable should be included in the design. The lamination process and orientations of the lay-up must be strictly controlled to ensure structural strength.

Interior vehicle design for passenger survivability and structural design for energy-absorbing capabilities during collisions are addressed in Reference 11.

8.2 PROPULSION, NORMAL BRAKING, AND EMERGENCY BRAKING

The four SCD vehicles are propelled by various configurations of linear synchronous motors (LSM) which also provide normal service braking through regenerative/reversal of the motor. Various methods for emergency braking are proposed. Assuring the ability to stop within a specified distance is absolutely critical to the safety of guided transportation systems, since it is not possible to maneuver the vehicle to avoid an object. Additionally, unexpected or excessively high deceleration rates must be prevented to avoid passenger injuries from falls inside the vehicle.

8.2.1 Safety Performance Goals

Since failure of the power supply could occur, the propulsion motors and associated regenerative braking does not, by itself, assure fail-safe braking. Additional independent means of emergency braking is generally required. To assure that the brake design and performance meets safety standards, ***complete loss of braking capability shall be shown to be improbable through the use of appropriate analyses.***

In general, LSM configurations have failure modes that are potentially hazardous due to inadvertent excessive braking forces. For example, certain motor winding failures can result in an uncommanded dynamic braking action caused by the magnets interacting with the LSM windings. To prevent injuries to unrestrained passengers, especially elderly or handicapped passengers due to unexpected sudden braking, ***uncommanded braking due to system malfunctions of the normal or emergency braking systems shall be shown to be remote through the use of appropriate analyses.***

The SCDs propose various methods for emergency braking, including skids, landing wheels with brakes, drag chutes, and an approach which maintains clearance from the guideway down to virtually zero speed. Regardless of the design approach used, ***there shall be no significant damage to the vehicle or the guideway as a result of contact between the two during normal or emergency braking.***

8.2.2 Specific Design Requirements

To prevent injuries to unrestrained passengers, especially elderly or handicapped passengers, due to excessively high braking deceleration rates, ***normal and emergency braking systems shall be designed to comply with the braking deceleration rates specified in APTA** Guidelines for the Design of Rapid Transit Facilities, **Section 4.5 [16]***, and further that ***no single failure in the LSM propulsion system or braking systems will cause these rates to be exceeded.*** The APTA specified values are discussed in Section 4.7, Brake Installation and Performance, of Reference 9. Specifically the APTA recommends that the following maximum braking rates be used:

Service Braking 1.55 - 2.01 m/sec^2 (5.11 - 6.63 ft/sec^2)
Emergency Braking 2.01 - 3.58 m/sec^2 (6.63 - 11.80 ft/sec^2

These recommendations are based on a review of the ability of elderly seated passengers to safely resist acceleration forces. Because the power supply to the propulsion system could be interrupted, to assure fail-safe braking, ***the design shall incorporate an emergency braking system that is independent of the LSM propulsion/braking system that does not require an external power supply, and that has the capability of bringing the vehicle to a complete stop from any normal operational speed.***

The maglev propulsion and normal braking systems are controlled by computer. To achieve the safety levels required, ***a redundant or fault-tolerant design shall be used for the computer and its supporting equipment, such as power supplies and sensors.***

Additionally, the recommendations provided for emergency braking systems in Section 4.7 E, Brake Installation and Performance Recommendations of Reference 9, and Volume 4, Section 3.6.2.4, Proposed Specifications for Vehicle Braking Systems of Reference 11, should be considered for application as design requirements.

8.3 SUSPENSION, LEVITATION, AND LATERAL GUIDANCE

This section specifies requirements for controlling hazards associated with the suspension, levitation, and lateral guidance systems. The hazards of concern involve vehicle/guideway contact at high speed and the containment of cryogenic materials.

8.3.1 Safety Performance Goals

The sudden loss of levitation and/or guidance control at high speed will likely result in abrupt contact between the vehicle and the guideway. Serious injuries can occur when deceleration forces result in high contact velocities between occupants and the vehicle interior. In order to reduce the probability of vehicle/guideway contact, ***the malfunction of levitation and/or lateral guidance systems resulting in deceleration forces greater than (TBD) shall be shown to be improbable through the use of appropriate analyses.*** With further analysis, an applicable deceleration force value can be derived from Reference 11.

Three of the four SCDs employ some kind of retractable landing gear or skid for controlled delevitation and landing. If such a landing device is inadvertently deployed at high speed and contacts the guideway, substantial deceleration forces could result. To reduce the probability that passengers will be subjected to dangerous deceleration forces, ***the inadvertent deployment of landing gear or skids that result in guideway contact and deceleration forces greater than (TBD) shall be shown to be improbable through the use of appropriate analyses.*** Applicable deceleration force values can be derived from Reference 11.

The proposed Grumman guideway incorporates a vehicle wraparound design providing additional safety to the system by physically preventing "derailments." The Bechtel, Foster-Miller, and Magneplane SCDs do not include a vehicle "wrap around" feature or any other means to physically prevent vehicles from lifting up and off the guideway. If a levitation and/or guidance malfunction causes the nose of such vehicles to pitch up while traveling at high speed, aerodynamic forces could be sufficient to force these vehicles out of control and off the guideway. To control these hazards, ***the failure of levitation and/or lateral guidance function(s) that could potentially cause the vehicle to depart the guideway shall be shown to be improbable through the use of appropriate analyses.***

SCD contractors whose designs incorporate aircraft type landing gear must consider the potential fire hazard associated with rubber tires. If rubber tires contact the guideway surface at high speed, the resultant high temperatures from friction could ignite the tires. To control this hazard, landing gear should never be deployed above a certain threshold speed, and therefore, ***inadvertent deployment of rubber tire landing gear at speeds greater than (TBD) kmph shall be shown to be improbable through the use of appropriate analyses.*** Further analysis is required to determine the speed at which sufficient friction between the guideway and tires would be generated to start a fire.

To provide passenger comfort through superelevated guideway curves, several maglev concepts employ an active vehicle tilting mechanism. Failure of this mechanism to tilt the vehicle, or tilting in the wrong direction when entering a curve, can subject passengers to unexpected lateral g-forces. Under these circumstances, standing passengers could fall or be thrown across the vehicle interior resulting in serious injuries. To reduce the probability of this hazard, ***malfunction of the active tilting mechanism that results in lateral g-forces greater than (TBD) shall be shown to be remote through the use of appropriate analyses.*** With further analysis, applicable g-force values can be derived from Reference 11.

8.3.2 Specific Design Requirements

A failure of the on-board magnets will result in immediate loss of levitation and guidance. The most common cause of superconducting magnet failure is a propagation of magnet quenching. To control the probability of magnet quenching to an acceptable level, a ***superconducting magnet stability margin could be defined as winding operating current (I) divided by the winding critical current (Ic). A preliminary maximum magnet stability margin could be set at 0.8 for the most demanding magnet operating point and with worst case operation environment conditions.***

The 20% safety factor, as represented by the preliminary magnet stability margin of 0.8, is incorporated to account for the adverse effects of magnet operating point and/or operation environment conditions which, in practice, might exceed anticipated worst-case conditions. Further research and development are needed to validate a final magnet stability margin which will account for all operational uncertainties including winding aging, fatigue-induced deterioration, etc.

An alternative magnet stability margin limit may be proposed for this specification if supported by adequate superconducting magnet application performance data.

Compliance with the superconducting magnet stability margins shall be validated by full-scale magnet testing under worst-case operating point and magnet operation environment conditions. The testing operation environment conditions shall include but not necessarily be limited to the cryogenic coolant temperature and/or temperature spectrum, the coolant phase mix, the coolant flow rate, physical vibration and/or shock and such electromagnetic field transients as could induce winding ac losses.

Cryogenic fluids, if not properly contained, are potentially hazardous to passengers and crew. If leaking cryogenic fluid is allowed to accumulate in a confined space where its temperature can rise, the available oxygen can be displaced by the cryogenic material due to thermal expansion, causing asphyxiation. Direct contact with cryogenic fluids can cause "cold burns" and lung damage can result from cryogenic gas clouds. The following requirements are recommended to safely contain onboard cryogenic material:

- *Cryogenic pressure vessels shall be designed in accordance with pressure vessel design criteria and burst safety factors outlined in FRA regulation 49 CFR, Part 229.49 [15] and ASME Boiler and Pressure Vessel Code [17].*
- *The on-board cryogenic cooling system, including any transfer piping, shall be located outside of passenger/crew compartments where such compartments shall be defined by relatively gas-tight walls, bulkheads, floors, and access doors.*
- *Provision for vehicle blow-off of cryogenic gas via cryogenic system pressure relief valves shall be located as remotely as possible from vehicle exterior doors, emergency exits, and cabin air circulation inlets.*
- *The cryogenic cooling system shall incorporate redundant pressure relief valves to prevent system overpressurization.*

Materials surrounding the cryogenic system may be exposed to extremely low temperatures resulting in materials embrittlement. *All cryogenic equipment containing supercooled materials shall be designed to function for life at operating temperatures and resist embrittlement. Additionally, other vehicle structures which are adjacent to cryogenic equipment should be insulated from supercooled materials to preclude embrittlement of those structures.*

When rubber tire type landing gear are used, there is a potential for tire bursting that could result in damage to adjacent equipment. *Critical equipment which could be damaged by tire failures shall not be installed in the vicinity of rubber tire type landing gear. A zonal analysis shall be performed to demonstrate compliance with this requirement.*

8.4 ON-BOARD POWER SYSTEM

On-board electrical power system failures and malfunctions can result in critical or even catastrophic hazards. Hazards include passenger exposure to high voltage; disruption of safety-critical systems; lack of lighting and air conditioning resulting from loss of power; and fires caused by shorts in circuit wiring. The requirements defined in this section are based on the SCD safety review and are created to mitigate these safety hazards.

8.4.1 Safety Performance Goals

On-board power system supplies power to several safety-critical systems, including train control, emergency braking, and the fire detection system. Loss of power to these systems can cause a wide variety of hazards; therefore, ***the loss of the on-board electrical power supply must be shown to be improbable through the use of appropriate analyses.***

8.4.2 Specific Design Requirements

FRA and Federal Aviation Administration requirements for electrical systems and equipment, are contained in 49 CFR, Part 229 [15], and 14 CFR, Parts 25.1351 through 25.1363 [18]. In general, the requirements apply to power generation and external power connections, independence of sources, fire immunity of sources, electrical equipment installations and electromagnetic compatibility, cable routing, battery design, and alternate power supply connection. As previously discussed in Reference 9, these requirements, as well as NFPA 130, Standard for Fixed Guideway Transit Systems, [19] and the IEEE 11-80 Standard for Rotating Electrical Machinery for Rail and Road Vehicles [20] could be modified to be applicable to maglev technology.

The Bechtel SCD proposes using two methanol fuel cells to provide on-board electrical power. There are two hazards that were identified with chemical fuel cells. First, methanol fuel cells may emit hazardous gases. ***Systems that incorporate chemical fuel cells shall isolate all fuel cells, related equipment, and emissions from the passenger area.*** Second, pure methanol burns invisibly to the human eye. It is common practice in the auto racing industry to adulterate methanol with a contaminant to ensure flames appear when methanol is burning. ***Systems that incorporate methanol fuel cells shall ensure that burning methanol is visible to the human eye.***

The Grumman SCD proposes using a battery to supply power for the emergency braking system. The effectiveness of emergency braking depends on the availability of the battery system. ***Systems that rely on battery systems for safety-critical functions must provide battery health monitoring and a battery fail indication to ensure batteries are available prior to departing a station.***

The Magneplane SCD proposes using lead-acid batteries for back-up power. Although these types of batteries have been used in automobiles for many years, it is important that explosive hydrogen gas does not accumulate in a confined space. ***Systems that incorporate lead-acid batteries must provide a fail-safe ventilation system to ensure the hydrogen gas is properly exhausted.***

8.5 MAGNETIC SHIELDING

Although recent studies have raised concern about potential health hazards associated with magnetic fields, there is no universally accepted safe exposure level. Research continues in this area and requirements for maglev should be based on the most recent consensus within maglev and medical research communities.

8.5.1 Safety Performance Goals

To reduce magnetic field levels, some SCD contractors propose using active field cancellation systems. Malfunction of these systems could result in passenger magnetic exposures above specified safe standards. ***Malfunction of field canceling type systems which result in significant loss of field canceling performance shall be shown to be remote through the use of appropriate analyses.***

8.5.2 Specific Design Requirements

The American Conference of Governmental Industrial Hygienists (ACGIH) has established static magnetic field limits of 10 gauss for persons with implanted pacemakers [21]. In addition, International Non-Ionizing Radiation Committee (INIRC) of the International Radiation Protection Association (IRPA) has developed an interim standard limiting human exposure to power frequency electric and magnetic fields [22]. Based on the INIRC and ACGIH recommendations, magnetic field limits are proposed maglev systems. ***The magnet configuration, location, and field shielding shall limit passenger and crew magnetic field exposure to the following levels:***

Seat Level Maximum	=	***10 Gauss ac***	***10 Gauss dc***
Platform Level Maximum	=	***10 Gauss ac***	***10 Gauss dc***
Emergency Passageway	=	***10 Gauss ac***	***10 Gauss dc***

8.6 FIRE PROTECTION

Specification of fire safety requirements should include a discussion of fire prevention, detection, containment, and suppression. The FRA fire safety guidelines [23] and the NFPA 130 Standard for Fixed Guideway Systems [19] include requirements for selection of conventional railroad passenger car and rail transit system materials; NFPA 130 specifies other fire protection requirements. The FRA is currently sponsoring research relating to passenger train fire safety.

The German approach to maglev fire safety is documented in the RW MSB document safety requirements document [23] and recommends a two-fold approach consisting of fire prevention and emergency evacuation planning. In addition to describing maglev-specific requirements, the RW MSB document cites several requirements contained in other documents including those promulgated by the German Standards Institute (DIN), International Union of Railways (UIC), and the U.S. FAA regulations contained in 14 CFR, Part 25 [18].

The specific requirements defined in this section were developed as a result of the SCD safety review.

8.6.1 Safety Performance Goals

The failure of a fire detection or suppression system is not, by itself, a hazard. However, if the failure occurs along with a fire, the result can be catastrophic. In order to reduce the probability of injuries or deaths resulting from an undetected fire, *the loss of a vehicle, wayside or station fire detection or suppression system must be shown to be remote through the use of appropriate analyses.*

8.6.2 Specific Design Requirements

Fires located in remote, unmanned locations can cause serious damage and result in a degradation of safety because of loss of guideway power. This hazard applies to all maglev systems and was not adequately addressed in the SCDs. *Remote wayside locations require fire prevention, detection, and suppression measures.*

The Bechtel SCD proposes using on-board fuel cells to provide electrical power. The fire hazards associated with methanol fuel cells were identified during the SCD safety review. Further studies are needed to determine the feasibility of incorporating fuel cells on maglev vehicles and restrictions on the locations of on-board fuel cells.

8.7 GUIDEWAY DESIGN

The guideway must be capable of supporting all vehicle and externally applied loads without damage or distortion over its service life, including exposure to earthquakes and tornadoes. In addition, it must accommodate the mechanical attachment of all guideway-mounted equipment needed for propulsion, levitation, guidance, communication, monitoring, etc. Generally, designing for the structural loads involves no new technology, although determining some of the loads may be difficult. Also, the use of ferromagnetic materials near the high magnetic fields of the operating system should be minimized; this may complicate the materials selection.

8.7.1 Safety Performance Goals

Apart from the design of the overall guideway structure, particular attention must be paid to the fastener system used to attach equipment to the guideway. In particular, linear motor coils are fastened to the guideway structure and are subject to frequent load cycles from vehicle propulsion and braking forces. Failure of the fastening or coil would likely result in improper vehicle guidance and levitation due to the coil becoming free of the guideway. This could result in a Category I event. Therefore, ***the separation of any coils from the guideway shall be shown to be improbable through the use of appropriate analyses.***

8.7.2 Specific Design Requirements

For the reasons stated above, ***all equipment attached to the guideway with mechanical fasteners (bolts, rivets, etc.) shall use redundant fastening systems such that the failure of individual fasteners can be tolerated with no loss of the structural integrity of the attachment.*** The objective is to retain secure attachment with some individual fasteners failed. This will allow a reasonable and safe interval between inspections, and will assure that no critical or catastrophic mishap can result from a single fastener failure.

The initial fastener failures in a redundant fastener system are inherently latent failures, therefore ***all fastener system designs shall provide for easy detection of failures by inspection without the use of special tools or instruments, and preferably with no disassembly of equipment.***

All power lines required for operation of the maglev system will also be an integral part of the guideway design. To prevent injury to employees or evacuated passengers on the guideway, ***all high-voltage power lines shall be shielded or otherwise protected to prevent possible contact with live wires by any person.***

8.8 GUIDEWAY SWITCH

A switch allows vehicles to exit or enter the main line around stations, maintenance depots, etc. This function is the same as existing railroad switches. However, because the high speeds of maglev result in less time for the operator to react to a switch failure or malfunction, the reliability and fail-safe operation of the switch are critical.

8.8.1 <u>Safety Performance Goals</u>

If a maglev vehicle enters a switch indicating an incorrect position, there is little time for the operator to react. Striking a disabled vehicle, obstacle, or entering guideway construction would cause heavy damage to the moving vehicle; therefore, ***the incorrect indication of a switch position must be shown to be improbable through the use of appropriate analyses.***

While the vehicle is moving through the switch, the switch must remain in the commanded position. If the switch moves during this time, the vehicle is likely to make contact with, or depart the guideway causing serious damage. Therefore, ***the movement of a switch while the vehicle is in the switch, or unable to stop before the switch, must be shown to be improbable through the use of appropriate analyses.***

Proposed switching mechanisms that incorporate movable beams will require numerous highly synchronized actuators along the length of each beam. If the actuators are not properly synchronized, the movable beams can be permanently deformed or weakened. Therefore, ***the asynchronous operation of moveable beam actuators, which could result in structural weakening or misalignment of the beam, shall be shown to be improbable through the use of appropriate analyses.***

8.8.2 Specific Design Requirements

In order to prevent a vehicle from moving through a switch positioned in an unknown or incorrect position and striking a foreign object, the ***switch position must be continuously monitored.***

The full length of moveable switch beams shall be monitored for integrity to ensure that beam damage resulting from the asynchronous operation of the beam acutators is annunciated.

Switching mechanisms that use moveable beams must ensure that the switch remains in the desired position. ***The switch must be mechanically locked into the desired position and verified.***

Switches generally use many mechanical and electrical components to operate. In addition, during bending, the beam may be subjected to high stresses capable of initiating fatigue cracks. Malfunction or failure of switches can cause severe hazards, therefore, as identified in Reference 8, ***switch equipment must be placed on the safety-critical maintenance list.***

Switch beams are generally longer than the normal elevated guideway beams and respond much more to thermal variations than normal beam sections. As recognized in Reference 8, ***switch beams must be able to withstand loads under all operating conditions, both normal and emergency.***

Parts 213.133 through 213.143 of 49 CFR [15] specify requirements for conventional railroad switches. In general, the CFR requires that the switch be reliable enough to assume two positions and, when in a position, be capable of supporting the loads required by normal operations. As recognized in Reference 8, the switch requirements in 49 CFR, Parts 213.133 through 213.143 could be revised to reflect the requirements in Chapter 8, Switches, of the RW MSB [24].

8.9 GUIDEWAY MONITORING

The loss of a monitoring system is usually, by itself, not a hazard. However, if the failure occurs along with the condition that the monitoring system is supposed to detect, the result can be hazardous. This section is concerned with the hazards associated with the loss of guideway monitoring systems coupled together with the unwanted condition.

8.9.1 Safety Performance Goals

The maglev guideway can fail very quickly, as in the event of an earthquake, or it can gradually deteriorate resulting in a complete failure of the guideway under load. The latter is of concern due to the silent nature of the failure. In order to reduce the probability of a vehicle contacting or departing the guideway due to an undetected structural failure, ***the loss of guideway integrity monitoring must be shown to be improbable through the use of appropriate analyses.***

Vehicles traveling at high speed are vulnerable to damage from relatively small objects. Designing the vehicle to withstand impact with smaller objects can be done fairly easily. However, larger objects can cause substantial damage and possible loss of control of the maglev vehicle. In order to reduce the probability of the maglev vehicle striking the guideway due to an undetected foreign object, ***the loss of guideway obstacle monitoring must be shown to be improbable through the use of appropriate analyses.***

8.9.2 Specific Design Requirements

Routes that are primary candidates for maglev systems in the United States provide a broad range of climatic conditions involving high and low temperatures, wind, rain, snow, ice, earthquakes, fog, lightning, dust, and sand. In order to reduce the probability of a maglev vehicle striking a foreign object on the guideway or departing the guideway, ***the entire guideway must be continuously***

monitored for both obstacles and integrity under all operating conditions (e.g., night, snow, etc.)

Guideway monitoring systems must monitor the entire maglev guideway. Some portions of the guideway will be in remote locations where maintenance on the guideway will be difficult and take additional time to respond. In order to prevent some common failures and reduce functional failures, ***the guideway monitoring systems must have an emergency back-up power source, independent from the primary source.***

Due to the possibility of a guideway monitoring system failure in a remote location, ***loss of guideway monitoring must be immediately detected by Central Control.***

8.10 POWER SYSTEM AND DISTRIBUTION

Electrical power and distribution systems are hazardous for three reasons. First, when power systems fail, the propulsion system is also lost. Second, power system failures often result in a fire hazard caused by short circuits. Third, power systems emit electromagnetic fields that can induce voltages on nearby equipment and transmission lines.

8.10.1 Safety Performance Goals

Systems that incorporate vehicle floor-mounted levitation coils may experience excessive deceleration forces caused by LSM failures. The vehicle aerodynamic and magnetic drag induced by these systems during LSM failures may be hazardous to passengers, therefore, ***the loss of system power to a substation block resulting in loss of power to the LSM must be shown to be remote through the use of appropriate analyses.***

The Magneplane system incorporates emergency evacuation onto the guideway, which contains LSM coils. If power to the LSM cannot be removed, passengers may be exposed to high voltages and electrical shocks from the LSM, therefore, ***the inability to remove guideway power from LSM windings must be shown to be improbable through the use of appropriate analyses.***

8.10.2 Specific Design Requirements

Electromagnetic interference emitted from the power distribution system may effect the maglev communication system. These stray voltages may result in the communications system being ineffective to transmit signals resulting in loss of communication and coordination during an emergency. As recognized in Reference 8, the EMI/EMC requirements in Chapter 10, Lightning Protection Electromagnetic Compatibility, Electrostatic Discharge, of RW MSB [18] should be modified for U.S application.

In addition, as stated in section 8.4.2 of this report, the FAA requirements identified in 14 CFR, Parts 25.1351 through 25.1363 [18], as well as NFPA 130 [19] and IEEE 11-80 [20] have been previously identified as potential requirements for maglev systems. These requirements should be modified to be applicable to maglev technology.

In order to verify the performance of safety-critical monitoring systems, periodical checks must be incorporated. As noted in Reference 9, ***systems responsible for fault monitoring shall be periodically tested to ensure system integrity.***

Communications, train control and other safety-critical systems may require high quality conditioned electrical power. If the supply power becomes out-of-tolerance, the equipment performance may be reduced. ***In general, electrical power used to supply safety-critical systems including communications, train control, and fire systems shall be monitored for failure and out-of-tolerance conditions. This monitoring shall include overvoltage, undervoltage, overfrequency, underfrequency and phase-to-phase differential current. Any failure or out-of-tolerance condition shall be annunciated.***

The Magneplane system incorporates emergency evacuation onto the guideway. The guideway contains LSM windings. If power to the LSM cannot be removed, passengers may be exposed to high voltages and electrical shocks from the LSM. ***Systems that incorporate emergency evacuation onto guideways containing LSM windings must provide an indication to show that it is safe to walk on the LSM.***

8.11 COMMUNICATIONS, COMMAND, AND CONTROL

This section specifies requirements for controlling hazards associated with an integrated Communications, Command and Control (C^3) system. In operational terms, the function of C^3 is to coordinate, detect, and protect operational elements (i.e., vehicles, guideway, stations, and all other operational interfaces).

8.11.1 <u>Safety Performance Goals</u>

The role of the C^3 system is to provide a highly automated means for effectively monitoring and managing the overall operation of the maglev system under normal, abnormal, and emergency conditions. The C^3 system is used by every subsystem in the maglev system and the loss of the system can cause a wide variety of hazards; therefore, ***the loss or malfunction of the C^3 system must be shown to be improbable through the use of appropriate analyses.***

Accurate train location detection is essential for determining a safe route and speed profile application within a system. This information is also essential to command correct interlocking switch positions along the guideway. In order to reduce the probability of a vehicle collision, ***the loss or malfunction of the train location and speed detection function of the C^3 system must be shown to be improbable through the use of appropriate analyses.***

Berthing verification and door control are safety-critical functions of the C^3 system. Inadvertent door opening at high speeds and during berthing can result in injuries and fatalities.

Therefore, *the malfunction of the berthing verification and door control functions of the C^3 system must be shown to be improbable through the use of appropriate analyses.*

8.11.2 Specific Design Requirements

Any failure of subsystems, equipment, or components within the C^3 system that may lead to an unsafe state must be self-detecting. Self-detecting failures will result in vehicles stopping or operating at a restrictive safe speed.

Microprocessors are used to perform many safety-critical functions in a highly automated C^3 system. Software validation and verification procedures must be applied to reduce the likelihood of unsafe software failures. *RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification [25], should be used for assessing and controlling the application of software in safety-critical functions.*

8.12 SYSTEMS OPERATIONS AND MAINTENANCE

8.12.1 Maintenance Performance Goals

The maintenance program for the maglev system will be based on a hierarchy of function and schedules resulting in daily, weekly, monthly, and yearly inspections and servicing to ensure the safety of the passengers and operators. Each subsystem, structure, or component will be assigned a priority based on the safety-critical nature of its function.

The preliminary list of safety-critical subsystems requiring maintenance priority includes: vehicle tilt mechanism, retractable wheel assembly, C^3 system, batteries, helium coolant system, superconducting magnets, and a vehicle speed verification system.

The preliminary list of safety-critical guideway structures requiring maintenance priority includes: guideway bearing supports,

external tendons, track slab, outriggers, spine girder, emergency egress stairs, rail alignment, linear synchronous motor windings, and switch mechanisms.

8.12.2 Specific Design Requirements

The high operating speed of a maglev system and the consequences of component failures will dictate a higher percentage of completed scheduled maintenance than would be experienced in rail systems. ***A stringent training requirement for maintenance crews and verification of completed tasks, similar to the airlines, is required.***

The maglev system will be automatically controlled at the central control facility. The high operating speed of a maglev system and the consequences of human error will dictate a higher degree of expertise. ***A stringent training requirement for central control operators, similar to air traffic controllers, is required.***

The cryogenic fluids used to cool the superconducting magnets will require special handling and servicing techniques. ***Maintenance personnel will require special training to safely handle cryogenic servicing and maintenance.***

Because of the complexity of maglev systems and the critical nature of high speed operations, ***a record of on-board equipment operating states, just prior to incidents and accidents, should be made available through the use of a continuous loop data recording mechanism.*** Contractor(s) shall prepare a proposed list of critical operating data that will be continuously recorded in a crashproof storage medium.

8.13 ENVIRONMENTAL EFFECTS

Potential U.S. routes for maglev applications provide a broad range of climatic conditions involving high and low temperatures, wind, rain, snow, ice, earthquakes, fog, lightning, dust and sand. The relative importance of environmental effects will depend primarily on the operating region of the maglev system.

8.13.1 Safety Performance Goals

The equipment shall be designed so that when exposed to the worst-case limits of any of the environmental stresses specified herein or any natural combination of them, it will perform within its specified design-performance limits and will not suffer degradation of its functional performance, structural integrity, or longevity.

8.13.2 Specific Design Requirements

In general, environmental conditions will impact all maglev systems to a varied degree. Accordingly, different environmental criteria must be developed for each maglev location. One possible method is to partition the vehicle into sections, each having its own criteria based on the environmental conditions experienced. This will provide the most cost-effective method for defining the requirements. *The equipment and structures shall be designed to operate normally without any degradation of performance or integrity when exposed to worst-case limits of any applicable environmental conditions.*

All equipment and structures shall be designed to operate without degradation in a maximum high ambient temperature of (TBD).

All equipment and structures shall be designed to operate without degradation in a minimum low ambient temperature of (TBD).

All equipment installed on-board the vehicle shall be able to withstand (TBD) g forces that are representative of peak loads caused by wind gusts and high speed landings.

If the equipment is installed in a location subject to exposure to fuel or fuel vapor, hydraulic fluid, lubricating oil, solvents, cleaning fluid, fire extinguishant, or insecticide in the course of *normal maglev operations, then the equipment shall be designed to operate with a wetted surface without degradation for a period of (TBD) hours.*

Equipment not installed in the volume of the vehicle shall be designed to withstand, without degradation, sand and dust of (TBD) particles per million for (TBD) hours.

Equipment installed in locations where it is subjected to falling water or driving rain or where water is sprayed on it from any angle in the course of normal maglev operations must be designed for waterproofness.

All equipment shall be designed to withstand, without degradation, operation over a temperature range of (TBD) at relative humidities from 0 to 100 percent.

System components which contain material potentially nutrient to fungus shall withstand exposure to contamination by a culture of various fungi at the following conditions:

Relative Humidity:	*95 percent*
Temperature:	*30° C (86° F)*
Duration	*28 days*

All equipment shall be installedd to withstand, without a degradation of performance, operational shock loads of (TBD) G peak or (TBD) milliseconds.

All equipment installed on-board the vehicle shall meet vibration requirements defined by the worst-case vibration expected on the vehicle.

All equipment shall be designed to be free of detrimental effects of lightning-induced transients.

Based on the historical data of seismic activity in the specific location, the maglev system shall be designed to meet category A, B, or C performance requirements of the American Association of State Highway and Transportation Official's Standard Specifications for Highway Bridges [26].

8.14 EMERGENCY RESPONSE

An effective emergency response capability should be planned for and incorporated into maglev designs. Important elements include emergency communications, on-board power, vehicle configuration, overall evacuation strategy, and emergency evacuation within guideway locations (i.e., switch zone and superelevated zone).

8.14.1 Safety Performance Goals

The C^3 system must be able to support the necessary responses to emergencies. For some emergencies, normal lines of communications may be lost and reliance on the C^3 system is essential for coordination and fast emergency response time. In order to reduce the probability of delayed emergency response, *the loss or malfunction of the communication function of the C^3 system must be shown to be remote through the use of appropriate analyses.*

The Bechtel SCD proposes incorporating a "safe stopping" zone, located every 4 km (2.5 mi.), where emergency evacuation is permitted. The vehicle will coast to a stop using the kinetic energy of the vehicle in combination with a controlled application of the LSM dynamic braking system. If the vehicle is traveling at speeds greater than 80m/s (180 mph), Bechtel states it will always reach the safe stopping zone. Considering that not reaching the safe stopping zone in an emergency may increase the severity of passenger injuries, *failing to reach the "safe stopping" zone shall be shown to be improbable through the use of appropriate analyses. If this requirement cannot be satisfied, then a means to safely evacuate passengers shall be provided along the entire guideway.*

During an emergency evacuation, cabin tilting mechanisms as described in the Bechtel, Grumman, and Foster-Miller SCDs may be hazardous. A failure of the tilting mechanism may decrease the effectiveness of an emergency evacuation and increase the severity of passenger injuries. To ensure that tilting mechanisms meet safety requirements, ***a failure of the tilting mechanism that impedes emergency evacuation shall be shown to be improbable through the use of appropriate analyses. If this requirement cannot be satisfied, then it shall be shown by analysis and testing that passenger evacuation, including elderly and physically challenged passengers, can be achieved with a tilting mechanism failed in the worst-case position.***

8.14.2 Specific Design Requirements

Electrical power systems must be designed to provide power to safety-critical equipment during emergencies and power outage situations. To accomplish this, a list of safety-critical equipment must be developed and a dedicated emergency buss must be designed to power the safety-critical equipment. Emergency cabin lighting, voice communication and passenger evacuation systems are examples of safety-critical equipment and therefore should be powered by a dedicated emergency buss.

Specific design requirements for sizing evacuation exits, determining exit locations, providing emergency lighting, and incorporating fire detection and suppression systems are required. The FRA [15 and 23], AAR [27], AREA [28], NFPA 130 [19], and FAA [18] requirements already describe these systems for non-maglev applications. References 7-9 discuss these issues as they relate to maglev systems. References 13 and 14 discuss evacuation, rescue, and passenger safety issues for automated guideway systems which could be also applied to maglev systems. In addition, the FRA is sponsoring the development of recommended emergency preparedness guidelines for passenger trains [12]. In order to properly define maglev-specific requirements, each of these documents should be reviewed and tailored to the specific maglev system technology and operating environment. The specific requirements defined in the remainder of this section were developed as a result of the SCD safety review.

The Magneplane SCD proposes emergency evacuation onto the guideway along the LSM windings. ***Systems that incorporate emergency evacuation onto the guideway must provide an indication to the crew and passengers that it is safe to evacuate (i.e., power to the LSM has been removed, the guideway temperatures are not excessive, train operations have been stopped in the area of evacuation, etc.).***

Emergency evacuation of a maglev vehicle is recommended only when there is imminent danger to passengers who remain in the vehicle. Examples of imminent danger include vehicle fires and rupture of cryogenic systems causing supercooled materials to enter the passenger cabin area. Although each SCD has generally provided a means to evacuate passengers from vehicles to a point of safety, there were some exceptions. In particular, evacuation from superelevated guideways and on switch zones will require more attention as maglev concepts are further developed.

Assuming worst case equipment failure modes and environmental conditions, there should be a means for passengers to evacuate from stalled vehicles along the entire guideway, including switch zones and superelevated curves, to a point of safety. The point of safety in an emergency is that area where passengers can be free of risk of injury.

9. REFERENCES

1. Bechtel Corporation. Maglev System Concept Definition, Final Report. Prepared for National Maglev Initiative (NMI), A Joint Department of Transportation (DOT), Army Corps of Engineers (ACE) and Department of Energy (DOE) Program. San Francisco, CA. Final Report. September 30, 1992.

2. Foster-Miller, Inc. Maglev System Concept Definition Report. Prepared for NMI, A Joint DOT, ACE, and DOE Program. Waltham, MA. Final Report. October, 1992.

3. Grumman Aerospace Corporation. System Concept Definition of a Superconducting Electromagnetic System. Prepared for NMI, DOT, ACE, and DOE Program. Bethpage, NY. Final Report. September 1992.

4. Magneplane International. System Concept Definition Report for the National Maglev Initiative. Prepared for NMI, A Joint DOT, ACE, and DOE Program. Bedford, MA. Final Report. September 1992.

5. Department of Defense. Military Standard 882C, System Safety Program Requirements. Washington, DC. January 19, 1993. Superseding MIL-STD-882B, Notice 1, July 1, 1987 (March 30, 1984).

6. Federal Aviation Adminstration, U.S. Department of Transportation (USDOT). Advisory Circular (AC): System Design and Analysis, AC 25.1309.1A. Washington, DC. 6/21/88.

7. Dorer, R.M. and W.T. Hathaway. Safety of High Speed Magnetic Levitation Transportation Systems: Preliminary Safety Review of the Transrapid Maglev System. Prepared for Office of Research and Development, FRA, USDOT. Prepared by Volpe National Transportation Systems Center, USDOT (VNTSC/USDOT). Cambridge, MA. Interim Report. Report No. DOT/FRA/ORD/90/09. November 1990.

8. Dorer, R.M., et. al. Safety of High Speed Magnetic Levitation Transportation Systems: German High-Speed Maglev Train Safety Requirements - Potential for Application in the United States. Prepared for Office of Research and Development, FRA, USDOT, by VNTSC/USDOT. Cambridge, MA. Interim Report. Report No. DOT/FRA/ORD-92/02. February 1992.

9. Bing, A.J., et. al. Safety of High Speed Magnetic Levitation Transportation Systems: Comparison of U.S. and Foreign Safety Requirements for Application to U.S. Maglev Systems. Prepared for Office of Research and Development, FRA, USDOT by Arthur D. Little, Inc. (ADL). Cambridge, MA. Final Report. Report No. DOT/FRA/ORD-93/21. September 1993.

10. Bing, A.J., Bogani A.B., and T.J. Rasmussen. Maglev Signal/Control Assessment. Prepared for VNTSC/USDOT. Prepared by ADL. Cambridge, MA. Draft, January 1990.

11. ADL - Overall Contract. Safety of High Speed Guided Ground Transportation Systems: Collision Avoidance and Accident Survivability, 4 Volumes. Prepared for Office of Research and Development, FRA, USDOT. Cambridge, MA. Final Report. March 1993.

- Bing, A.J. Volume 1: Collision Threat. Prepared by ADL. Report No. DOT/FRA/ORD-93/02.I.

- Harrison, J., et al. Volume 2: Collision Avoidance. Prepared by Parsons Brinckerhoff Quade and Douglas under subcontract to ADL. Report No. DOT/FRA/ORD-93/02.II.

- Galganski, R.J. Volume 3: Accident Survivability. Prepared by Calspan Corp. under subcontract to ADL. Report No. DOT/FRA/ORD-93/02.III.

- Bing, A. J. Volume 4: Proposed Specifications. Prepared by ADL. Report No. DOT/FRA/ORD-93/02.IV.

12. Markos, S.H. Recommended Emergency Preparedness Guidelines for Passenger Trains. Prepared for Office of Research and Development, FRA, USDOT. Prepared by VNTSC/USDOT. Cambridge, MA. Final Report. Report No. DOT/FRA/ORD-93/24. Scheduled for publication in November 1993.

13. Benjamin, D.E. Evacuation and Rescue in Automated Guideway Transit. Prepared for UMTA USDOT. Prepared by Vought Corporation. Dallas, TX. 2 Volumes. Final Report.

- Volume I: Data Collection, Scenarios, and Evaluation. Report No. UMTA-MA-06-0048-79-2. December 1979.

- Volume II: Guidebook. Report No. UMTA-MA-06-0048-79-3. December 1979.

14. Dauber, R.L. Passenger Safety and Convenience Services in Automated Guideway Transit. Prepared for UMTA, USDOT. Prepared by Vought Corporation. Dallas, TX. 2 Volumes. Final Report.

- Volume I: Data Collection, Scenarios, and Evaluation. Report No. UMTA-MA-06-0048-79-4. December 1979.

- Volume II: Guidebook. Report No. UMTA-MA-06-0048-79-5. December 1979.

15. Code of Federal Regulations, Title 49, Transportation, Parts 200-240. Federal Railroad Administration. Office of the Federal Register, National Archives and Records Administration. October 1, 1992.

16. American Public Transit Association (APTA). Guidelines for Design of Rapid Transit Facilities. Washington, D.C. 1981.

17. American Society of Mechanical Engineers. (ASME) Boiler and Pressure Vessel Code, Sections II and VIII. New York, NY. 1971.

18. Code of Federal Regulations, Title 14, Aeronautics and Space, Part 25, Airworthiness Standards: Transport Category Airplanes. Federal Aviation Administration. Office of the Federal Register, National Archives and Records Administration. January, 1, 1993.

19. National Fire Protection Association (NFPA). NFPA 130, Fixed Guideway Transit Systems. Batterymarch Park, Quincy, MA. 1993.

20. Institute of Electrical and Electronic Engineers. (IEEE). IEEE 11-80. Standard for Rotating Electrical Machinery for Rail and Road Vehicles.

21. Rail Passenger Equipment; Reissuance of Guidelines for Selecting Materials to Improve their Fire Safety Characteristics. [Docket No RSPC-84-1, Notice 3], Federal Railroad Administration. Federal Register, Vol. 54. No. 10, January 17, 1989, pp. 1937-1840.

22. RW MSB. High-Speed Maglev Trains Safety Requirements. Cologne, Germany. March 1991. English translation published by FRA/VNTSC/RSPA/USDOT. Report No. DOT/FRA/ORD-92/01. January 1992.

22. Miller, G. "Exposure Guidelines for Magnetic Fields," American Industrial Hygienists Association Journal, Vol. 48 (12): 957-968. 1987.

23. International Non-Ionizing Radiation Committee (INIRC) of the International Radiation Protection Association (IRPA). Guidelines on Protection Against Non-Ionizing Radiation, Chapter 6, Interim Guidelines on Limits of 50/60 Hz Electric and Magnetic Fields. Eds.: A.S. Duchene, J.R.A. Lakey and M.H. Repacholi. Pergamon Press. 1991.

These guidelines were first published as "IRPA/INIRC Guidelines on Limits of Exposure to 50/60 Hz Electric and Magnetic Fields" in Health & Physics, Volume 58, No. 1, pp. 113-122. January 1990.

24. Dietrich, F.E., W.E. Ferro, and W.L. Jacobs. Safety of High Speed Magnetic Levitation Transportation Systems: Comparison of Magnetic and Electric Fields of Conventional and Advanced Electrified Transportation Systems. Prepared for Office of Research and Development, FRA, USDOT. Prepared by Electric Research and Management, Inc. State College, PA. Report No. DOT/FRA/ORD-93/07. August 1993.

25. Radio Technical Commission for Aeronautics (RTCA) DO 178B. Software Considerations in Airborne Systems and Equipment Certification. Washington D.C. December 1, 1992.

26. American Association of State Highway and Transportation Officials. Standard Specifications for Highway Bridges.

27. Association of American Railroads (AAR). Manual of Standards and Recommended Practices, Various Sections and Revision Dates. Mechanical Division, Operations and Maintenance Department. Washington, D.C.

28. American Railway Engineering Association (AREA). Manual for Railway Engineering. Volumes I and II. Washington, D.C. 1990.

APPENDIX A. SYSTEM SAFETY PROGRAMS APPLIED TO CONCEPT DEVELOPMENT AND DESIGN

System safety engineering applies scientific and engineering principles for timely identification of hazards and initiation of actions necessary to prevent or control hazards within the system. Effective management and integration of a program's professional personnel are essential to achieve the stated goals of system safety engineering. The efforts should start at the earliest possible time in the system life cycle to identify and then eliminate or control potentially unacceptable hazards.

Not all systems require the same level of effort to achieve the goal of an optimum level of safety. Each system must have the specific requirements identified. A major requirement of a sound system safety approach is to clearly and formally establish what safety tasks are required to meet the requirements for a specific product and who has the responsibility, accountability, and authority for each of these tasks.

A model system safety program, focusing on conceptual design through the maglev prototype development, is defined below. The purpose of this guide is to provide a baseline from which a maglev system design safety plan can be structured, and to provide a checklist of standard requirements for the plan. It encompasses the following elements:

- Program Description - A general technical overview of the program and maglev system should be provided. This section should provide the basis for selecting the design safety program tasks.
- Safety Organization and Interfaces - This section should clearly establish the responsibility, accountability, and authority (RAA) for conducting the safety tasks in the program. It should explain the functional interfaces among the various elements having the RAA. An organizational diagram showing where the safety RAA resides within the program should be provided.

- Safety Scheduling and Tracking - The master program management schedule and tracking system should include identified safety tasks and milestones. It is important that they are included because without formal management recognition and tracking of safety tasks, they can be overlooked under the pressure of high priority issues.

- System Safety Design Specifications - The methods that will be used to identify and/or set safety criteria for maglev should be described in this section. These should include specific references to safety standards and design specifications that are mandated for the program and also standards not required but which the program intends to use. In addition, the controls which management will use to ensure compliance with the requirements should be set forth.

- Safety Analysis - The safety analysis techniques and processes to be used should be described in this section. The system concept definition program should include a Preliminary Hazard Analysis (PHA). A PHA is essential to an advanced design effort because the requirements for subsequent safety analyses are based on the categorization of hazards from the PHA (see section describing PHA).

  This section should also identify any subcontractor responsibilities for analysis and should establish whether a standard format or procedure is to be required for the subcontractor.

- Safety Verification - The methods to be used to verify that the level of safety required for a system or Line Replaceable Unit (LRU) has been met should be described.

- Training - Training required for engineers, managers, and subcontractors in safety processes and procedures should be described. Responsibility for conducting and documenting this training should be established.

- Certification Program - The technological complexity of the maglev system development necessitates implementing a system of self-audit, or certification, to ensure that the objectives and requirements of the design safety program are being met. This section should describe such an audit procedure.

A.1 SAFETY ANALYSIS TOOLS

Designing for safety entails analyzing the proposed design of systems, subsystems, and Line Replaceable Units (LRU's). Consideration of the effects of their interfaces and interrelationships with such factors as facilities, support equipment, operational procedures and environments, and maintenance programs should be examined. During the design phase, the safety analyses should accomplish the following:

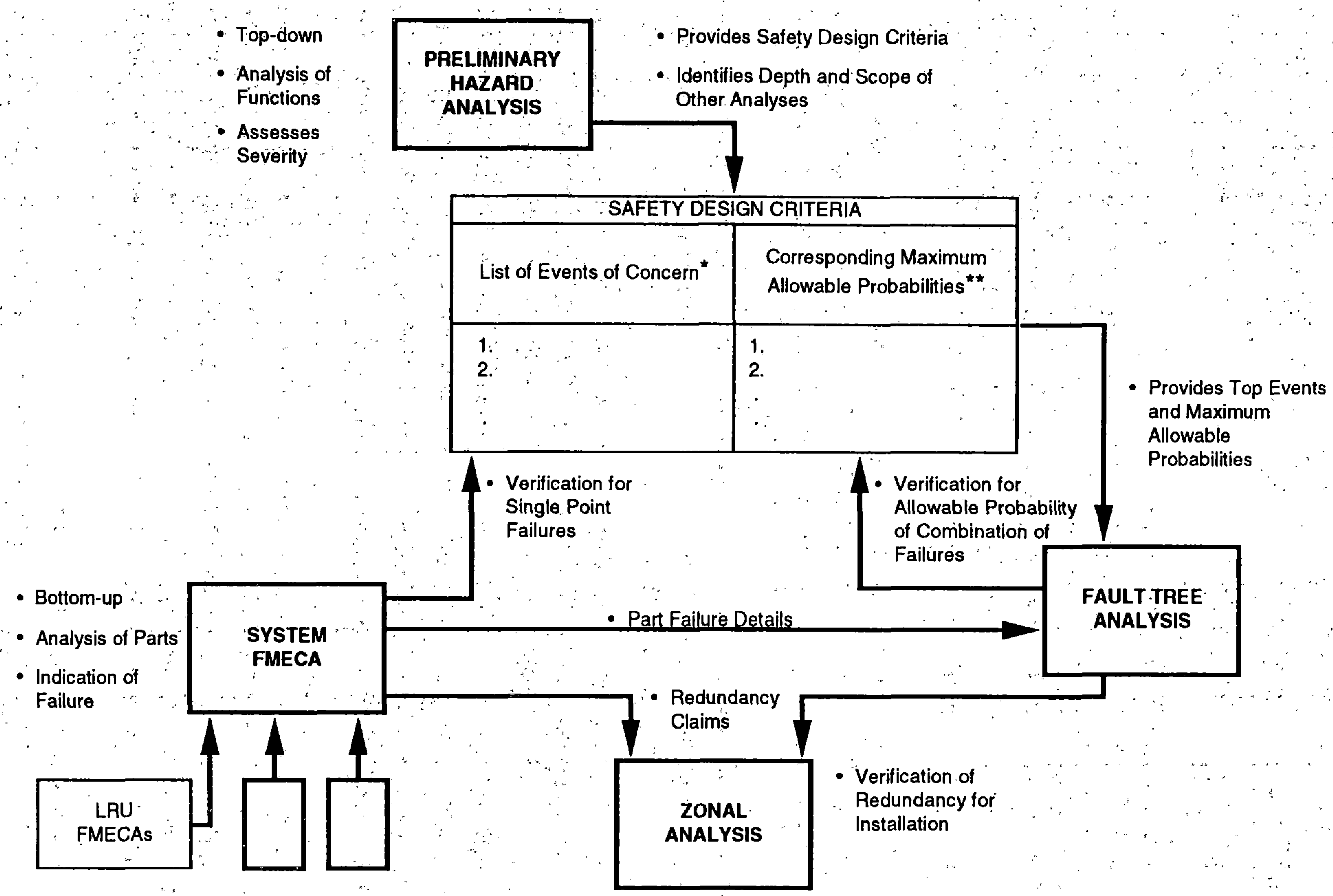
- Identify potential hazards and establish appropriate safety criteria.
- Assess the design based on safety criteria.
- Modify proposed designs to satisfy the criteria.
- Demonstrate compliance with the criteria.

These tasks may be accomplished by using four interrelated analysis tools. These four tools are the core of the system safety analysis process of setting criteria, guiding the design, and verifying compliance with the criteria. They are supplemented, complemented, and/or augmented by a variety of other safety activities and analyses. The four tools are derived from the philosophy and methodology contained in the Military Standard System Safety Program Requirments (MIL-STD-882), and the Federal Aviation Administration Advisory Circular, Design and Analysis, (AC 25.1309-1A).

The relationship between these four tools is shown in Figure A-1 and discussed in the following sections. Figure A-2 identifies each design phase and corresponding analytical tasks and outcomes. It should be noted that most of the analyses are performed more than once. The purpose of preliminary analyses is to provide an early means to validate the system architecture.

A.1.1 PRELIMINARY HAZARD ANALYSIS (PHA)

A PHA is a systematic, high-level examination of a proposed system's functions to identify and classify potential maglev system hazards and undesired events that its functional elements can cause or contribute to, not only due to malfunction, but also in normal operation. A PHA addresses the vulnerability of system functions; it is not an assessment of any particular hardware or software design.



NOTES: * Mishaps

** Depending on Probability Value, May Include Separation Requirements and Prohibitions on Single-Point Failures

FIGURE A-1. SYSTEM SAFETY ANALYSIS: CONCEPTUAL AND FUNCTIONAL RELATIONSHIPS OF PHA, FMECA, FTA, AND ZA

PHASE	ANALYSIS TASKS	RESULT/OUTPUT
SYSTEM CONCEPT DEFINITION	• PHA • Review with design discipline specialists	• For a new design: Safety events of concern & numerical safety criteria • For an existing design: safety criteria for design modifications
PRELIMINARY DESIGN	• Preliminary FMECA • Preliminary FTA	• Evaluate alternative designs
PROTOTYPE DEVELOPMENT	• Final FMECA, FTA • Zonal Inspection • FMECA Validation • PHA Assumptions Validation	• Safety-validated design • Validation of numerical safety criteria • Minimum Equipment List (MEL) • Certification Maintenance Requirements (CMR)

FIGURE A-2. OUTPUTS OF SAFETY ANALYSES

A PHA is a qualitative analysis and is conducted using experienced engineering judgment. For functions that are not complex, evidence of satisfactory service experience of similar functions based on other high speed rail, conventional railroad or transit applications may provide sufficient information. For complex functions requiring new designs, a new formal PHA should be prepared to provide a thorough identification of potential hazards.

The purpose of the PHA is to develop safety design requirements for the system and establish the framework for subsequent safety analysis and a certification plan. It provides information about potential hazards and mishaps, and assigns hazard severity categories for each. A probability requirement is assigned to each severity category.

A.1.2 FAILURE MODES AND EFFECTS CRITICALITY ANALYSIS (FMECA)

A FMECA is a systematic, comprehensive, bottom-up evaluation that analyzes the effects of potential failures in an LRU or system, as installed, from design data. The procedure assesses the impact of these failures on system or LRU operation, and consequently, on the operational safety of the maglev train. Information provided in the FMECA includes:

- Identification of single-point failures and hazard-level classification, which should confirm the adequacy of fail-safe design features.
- Identification of potential hazards due to significant multiple failure conditions involving latent, undetected failures.
- Identification of additional analyses, such as fault trees, or design changes which may be required.
- A system overview with a description of the system and its operation, possibly including schematics.
- Documentation of the effect of significant design changes.

The FMECA should be considered a concurrent part of the system design process. The FMECA should be started early in the design effort, even though little design detail is normally available at that time. The FMECA will thus begin at a relatively high level, and will be iteratively expanded and revised as the design progresses. As it is being developed, the FMECA systematically challenges the design by probing the ways the system can fail and assessing the effects of these failures. This provides continuing insights into possible design weaknesses which may warrant modification. Such modifications can then be readily implemented as a natural part of the design development cycle. As the system design progresses through the development phase, and design modifications are made in response to discovered needs, the FMECA is updated to reflect the changed design and is used in the process of evaluating and approving the changes.

A.1.3 FAULT TREE ANALYSIS (FTA)

An FTA is an analytical tool used for identifying and properly relating events which alone or in combination with other events could result in an undesired condition. It can also serve as a mathematical model for determining the probability of a specified undesired event. The fault tree itself is a top-down graphical representation of the logical relationships among failure and error events. It provides a concise and orderly description of the various combinations of possible events within a system which could result in some predefined top event.

Mishaps can be established from PHAs. Usually, top events candidates are derived from mishaps classified in the PHA as Category I or II. By applying the deductive technique of the FTA, one can focus on finding the primary failure modes and failure combinations that cause or contribute to the specific postulated mishap ***even when more than one subsystem is involved***. Like the FMECA, the FTA cannot be completed until the design is complete. In fact, the FMECA should be complete before the FTA because the FMECA can provide various detail system data for the fault tree, such as system effects and monitor parameters. However, a preliminary qualitative fault tree can often provide guidance for decisions about system architecture early in the design process.

A fault tree analysis is not inherently difficult, complicated, or expensive to prepare. It becomes simple or complex depending on the complexity of the system involved and the choice of the top event. The Boolean logic and mathematical calculations can be handled by commercially available computer programs.

A.1.4 ZONAL ANALYSIS (ZA)

A ZA is the systematic inspection of the geographic locations of the components and interconnections of a system, evaluation of potential system-to-system interactions with and without failures, and assessment of the severity of potential hazards inherent in the

ZA has evolved as a safety assessment tool from a recognition that two significant design-related accident causes have sometimes been overlooked in the past. These causes are:

- The unexpected interaction of unrelated system functions due to the installed proximity of subsystem elements, usually upon failure of one of the functions. This type of event is often called "Cascade Failure."
- The simultaneous loss of redundant subsystem functions from a single event due to the installed proximity of redundant subsystem elements. This type of event is often called "Common-Mode Failure."

A simple example of the first is where a flammable-fluid carrying line is routed through a zone or compartment that contains an ignition source, such as electrical switching equipment. A fluid leak can be cascaded into a serious failure condition due to the presence of a spark. An example of the second situation is locating redundant control computers side-by-side in the same rack or cabinet in the trajectory of a high-speed rotating machine. A structural failure of the rotating part could destroy both supposedly redundant computers.

Clearly, high-energy rotating devices, flammable or corrosive fluids, and pressure vessels are all likely candidates for causing damage to adjacent assemblies, but there are also many more subtle situations which the ZA must address. For instance, it may not be intuitive that hydraulic hoses and electric wire bundles need to be segregated, but if the electric wires supply power to a redundant electrical backup for a hydraulically powered function, good engineering judgment calls for segregating the hoses and wires to reduce the probability of a single failure or external event disabling both. Additionally, events which occur slowly over time (e.g., corrosion, collected moisture that could freeze, etc.) are examined by the ZA.

A.1.4.1 When to Conduct the Zonal Analysis

It is obvious that the ZA cannot be completed until the hardware is installed, because the final analysis is based on the inspection of the production-installed hardware and interconnections. Unfortunately, the maturity of the design at this stage makes resistance to change very high. Therefore, it is preferable to conduct the analysis as a continuous process during the design and to establish rules governing installation of components and subsystems to avoid common-mode and cascade failures. In some cases, as with vehicles and some control centers, it may be cost-effective to construct full scale development fixtures early in the design program to allow engineers designing unrelated subsystems to interface with one another while developing their installations. When a development fixture is used early in the program, the final ZA performed on the production articles should identify fewer or no necessary changes. If it is not possible to provide a full development fixture, the use of models, CADD, and/or zone mockups should be considered.

A.1.4.2 General Procedure for Conducting a Zonal Analysis

In order to conduct this analysis, the complete transportation system, including vehicles, stations, control centers, and right-of-way installations, is divided into zones. All of the equipment, cable runs, pipe runs, etc., in each zone is listed. A study is then made of the effects of failures of this equipment on other subsystem equipment within the zone and of threats from outside the zone. A generic procedure that can be adapted to a specific program is described below:

- Divide the complete transportation system into logical zones. For example, the vehicle would logically divide into its compartments for passengers, power equipment, etc., while a station or control center might be divided into rooms dedicated to various purposes.
- For each zone, list all of the system equipment contained in the zone. The lists should include wire bundles, ducts, fluid lines and any other interconnecting hardware.

- Divide the complete transportation system into logical zones. For example, the vehicle would logically divide into its compartments for passengers, power equipment, etc., while a station or control center might be divided into rooms dedicated to various purposes.

- For each zone, list all of the system equipment contained in the zone. The lists should include wire bundles, ducts, fluid lines and any other interconnecting hardware.

- Following this identification of equipment installed in each zone, the subsystem FMECAs or equivalent analyses should be reviewed to determine which equipment on the list have failure modes which can damage other equipment. The equipment that could be damaged may be in the same zone or in a different zone. The analysis should not be limited to considering only equipment located in the same zone. One could erroneously conclude two adjacent zones are "safe" when, in fact, two redundant elements of a subsystem may be only inches apart, separated by the zone boundary.

- Inspect each zone to determine whether the equipment in that zone, identified above as having failure modes that can effect other equipment, has been installed such that the postulated damage is likely to occur. The focus of the inspection should be on finding unwanted subsystem-to-subsystem interactions and/or redundancy segregation violations. Findings should be documented.

- When the inspections of all zones are completed, determine what the effect of each identified event is on the transportation system and/or its patrons and operators. Provide substantiation for accepting the existing installation or initiate design corrective action on any problems identified.

- Continue the process until all system installations, in all zones, including changes for corrective actions, have been systematically inspected.

A.1.4.3 Design Defenses Against Cascade and Common-Mode Failures

There are certain design precautions and techniques that can considerably reduce the chances that cascade and common-mode failures will occur. The ZA should verify that the following design features have been incorporated:

Separation - This is accomplished by placing a physical barrier between equipment, wires, etc. in such a way that they cannot come in contact with each other. An example of separation is a wire that is shielded from other wires that are located in the same bundle. The hazard is having the shielded wire short to another wire in the bundle. Encasing the wire in a grounded metal shield assures that any other wire will short to ground before it can short to the shielded wire. Separation in lieu of segregation is adequate where there are no significant hazards resulting from total loss of function due to common-mode failures or external events.

Segregation - This is accomplished by locating equipment, wires, etc. that perform redundant functions in different locations such that total loss of a safety-significant function (as determined by the PHA) is unlikely to occur due to a single external event or subsystem interaction.

Dissimilar Redundancy - The use of dissimilar redundancy can be a powerful method of safeguarding against total loss of a vital function. Various methods of achieving this are currently used on transportation systems, either deliberately or, in some cases, fortuitously. It simply means that the function, or at least an emergency mode of it, can be carried out in a different way if the normal way fails. Common widely used examples are emergency braking of the vehicle and alternative communication methods. The virtue of dissimilar redundancy is that because the alternative means of conducting the function are fundamentally different in their design, it is much less likely for an external or cascading event to affect them all in the same way.

A.2 HAZARD SEVERITY CATEGORIES

The PHA is used to assign hazard severity categories and safety criteria and establish what, if any, additional analyses are required. In order to assign hazard severity categories, a definition of hazard severity categories must be stated. MIL-STD-882 is the most widely used reference for definitions of hazard severity categories. The Hazard Severity Categories identified in MIL-STD-882 are:

DESCRIPTION	CATEGORY	MISHAP DEFINITION
CATASTROPHIC	I	Death or system loss
CRITICAL	II	Severe injury, severe occupational illness, or major system damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system damage
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or system damage

MIL-STD-882 cautions that these "severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the client and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness."

The following severity category descriptions have been adapted from MIL-STD-882 for maglev systems.

- **CATEGORY I (Catastrophic):** Death to passenger or employee, loss of maglev system.
- **CATEGORY II (Critical):** Severe injury to passenger or employee; hazard or single-point failure may lead to catastrophe if action is not taken to control the situation or rescue the individual. Critical systems are involved and the maglev vehicle is unable to move to the evacuation area. Time of response is important in preventing death or system loss.
- **CATEGORY III (Marginal):** Minor injury not requiring hospitalization or the hazard present does not by itself threaten the safety of the maglev system or passengers. No critical systems are disabled, but could be if additional failure(s)/malfunction(s)/hazard(s) occur.
- **CATEGORY IV (Negligible):** Less than minor injury. Does not impair any of the critical systems.

A.3 SAFETY DESIGN STANDARDS BASED ON SEVERITY CATEGORIES

MIL-STD-882 discusses methods for assessing the causes, severities, and likelihood of potential mishaps. Design standards relate the severity of the mishap to the probability of it occurring. The following definitions for terms used to describe the frequency of mishaps are adapted from MIL-STD-882 for maglev systems:

- **FREQUENT** mishaps are not unusual events. They could occur several times in annual operations.
- **PROBABLE** mishaps could occur several times in the lifetime of the maglev system.
- **OCCASIONAL** mishaps are expected to occur at least once in the lifetime of the maglev system.
- **REMOTE** mishaps are unlikely to occur during the lifetime of the maglev system.

  IMPROBABLE mishaps are those so unlikely that they are not expected to ever occur during the lifetime of the maglev system.

Using the preceding definitions, maglev systems should be designed and constructed so that:

- **FREQUENT** and **PROBABLE** mishaps are no more severe than **CATEGORY IV.**
- **CATEGORY III** mishaps are at least **OCCASIONAL.**
- **CATEGORY II** mishaps are at least **REMOTE.**
- **CATEGORY I** mishaps are **IMPROBABLE.**

A quantitative analysis may be used to support experienced engineering and operational judgment and to supplement qualitative analyses. Quantitative analyses are often used to estimate the probability of catastrophic or critical mishaps involving systems that are complex, that have insufficient service experience to help substantiate their safety, or that have attributes that differ significantly from those of conventional systems. For those cases where a quantitative analysis of the probability of a mishap is made to help judge the adequacy of the hardware configuration used to perform a function, the following probability ranges are commonly used worldwide in the commercial airplane industry. They quantify the terms used above, and represent the allowable average risk for each hour of exposure to the occurrence of the mishap:

FREQUENT	Greater than 1×10^{-3}
PROBABLE	1×10^{-3} to 1×10^{-5}
OCCASIONAL	1×10^{-5} to 1×10^{-7}
REMOTE	1×10^{-7} to 1×10^{-9}
IMPROBABLE	1×10^{-9} or less

A.4 SOFTWARE SAFETY

Safety criteria for digital computer-based equipment is based on the safety significance of the functions performed by such equipment. Hazard level categorization is one of the first steps in determining requirements. This is done during the PHA.

Each equipment/system function is categorized as Category I, II, III, or IV according to the effects of malfunctions or design errors. If the equipment/system provides more than one function, the most critical function of the system will determine the category of the whole system unless the system has been partitioned into elements having different categories.

The recommended source of guidance for software levels applied to maglev equipment/systems is RTCA/DO-178B "Software Considerations in Airborne Systems and Equipment Certification"* In this reference, software level is based upon the contribution of software to potential hazards as determined by the PHA. The software level implies that the level of effort required to show compliance with requirements varies with the hazard category.

---

* Radio Technical Commission for Aeronautics, December 1, 1992.

The software level definitions are:

Hazard Level	Software Level
Category I	Level A
Category II	Level B
Category III	Level C
Category IV	Level D

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of System Power Reference Figure 2-1 Items 3.1.1(h) 3.1.2(b) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.2.1(a) 3.2.1(d) 3.2.3(h)	Covered in Bechtel Hazard Nos. 5, 11, 21, 22, 23, 24, and 25. No. 5 is collision with a stalled vehicle, a Category I catastrophic event. Prevention techniques are the use of conflict probes and vehicle sensors which tell control to stop vehicle. No. 11 is loss of levitation, a Category II critical event. Prevention and mitigation techniques agree with concept design. No. 21 is guideway equipment fire which disables guideway power, a Category II critical event. Prevention and mitigation discussed below under Baseline Hazard "Fire". No. 22 is vehicle stops on guideway stranding occupants, a Category III marginal event. Bechtel states that passenger rescue is a procedural matter that will be developed during later program phases. Nos. 23, 24, and 25 involve the unavailability of doors and passenger comfort functions, Category III marginal events. Mitigation through manual overrides and emergency power systems.	ON-BOARD POWER *BEC SCD A3.6* :- Back-up batteries for emergency power. Primarily for hotel functions. LEVITATION *BEC SCD A3.8* - Sensors to warn of power loss to single magnets. This will cause vehicle to stop at next station. Air bearings provided on vehicle for safe landing in case of total power failure to magnets. *BEC SCD C1.6.1* - Air bearings can provide zero speed lift at any place on the guideway so vehicle can be towed. *BEC SCD C6.9*: Air bearings are backed up by hydraulic actuators that can lift the vehicle for takeoff. PROPULSION *BEC SCD A4.1* - Design allows vehicle to move in either direction along guideway in case of power failure on the other guideway. *BEC SCD A4.3* - Back-up batteries used to assure dynamic braking remains available in the event of total power failure. *BEC SCD A4.3 &4.4* - Redundancy levels in port and starboard motor systems are such that continued operation is possible with failures present in either side.	*BEC SCD C1.10.1*: Not clear what electrical power source is used for fire protection system. Normal on-board electrical power is generated by methanol-powered fuel cells. This introduces unique hazards and operational issues.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of System Power (continued)		*BEC SCD A4.7* - Safe headway automatically maintained if system failures cause reduced speed. Battery back-up proposed for regions where transmission line failures are common. *BEC SCD A4.8* - Controlled braking system is used to simultaneously stop all vehicles in case of total power loss from utilities, or loss of guideway integrity. Battery back-up power at each station to move vehicles stopped near the station the short remaining distance. *BEC SCD A4.4* - Special mounting scheme used to allow quick replacement of port and starboard motor windings. *BEC SCD A7.2* - Automated diagnostic system used to detect problems before they result in loss of power. Preventive maintenance program proposed to prevent major repair shutdowns. Ability to operate vehicles on one guideway in both directions while other guideway is under repair. *BEC SCD C1.11* - Program of daily maintenance, quarterly inspections, and periodic system overhauls for vehicles is proposed.	

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control System and/or Communication System Reference Figure 2-1 Items 3.1.1(g) 3.1.1(h) 3.1.1(l) 3.2.3(a)	Not specifically addressed by the Bechtel Team PHA, but is partially covered in many of the Bechtel Hazards because loss of control and/or communications could result in the following hazards identified by the Bechtel Team: No. 4, vehicle enters open switch, a Category I catastrophic event. Preventive measures proposed include multiple zone controllers and central must agree before switch moved. All prevention depends on operative communication system, however. Nos. 5, 6, 7 & 14 involve vehicle collisions, Category I or II depending on speed. Prevention measures primarily involve probes and sensors which rely on the control and communication systems. No. 8, excessive speed results in guideway contact or derailment , a Category I event. Preventive measures rely on controllers and sensors.	*BEC SCD A6.1* - The communication and control systems for each direction of travel share common facilities, but are functionally independent. *BEC SCD A6.2* - Higher level controllers (station, central) have responsibility for safe operation of entire system. Zone controllers can act autonomously to override effects of failures at higher levels. Adjacent zone controllers take corrective action due to failure of zone controller. *BEC SCD A6.5* - Adjacent zone controllers can maintain system integrity at reduced speed if central control is unavailable. *BEC SCD A6.6* - Central control can operate for zone and station controllers in the event of their failure. *BEC SCD C4.2.2* - Any communicated data error results in corrective action by controllers.	BEC SCD A6.2: Not clear if separate zone controllers used for each travel direction. The types of corrective action performed by a zone controller not described. BEC SCD A6.7: Multiple breaks in fiber optic cables could disable system. No discussion on this effect. Design based on fault tolerant parallel processor. Software development to achieve safety levels has not been thoroughly addressed.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation or Guidance and Levitation/ Guidance/ Magnet Failure Reference Figure 2-1 Items 3.1.2(d) 3.2.1(a) 3.2.3(h)	Covered in Bechtel Hazard Nos. 11 and 22. No. 11 is loss of levitation, a Category II critical event. Prevention and mitigation provided by redundant fail operational vehicle system, and on-board batteries to maintain levitation to allow safe stop or coast-through if guideway power lost. No. 22 is vehicle stops on guideway stranding occupants, a Category III marginal event. Bechtel states that passenger rescue is a procedural matter that will be developed during later program phases.	*BEC SCD A4.3* - Each vehicle has two independent invertors driving port and starboard motors. If a motor system fails the other will provide enough thrust for full speed operation which supports normal levitation. *BEC SCD C1.6.1* - Air bearing can be used for lift at low or zero speed anywhere on the guideway. *BEC SCD B7.4* - The propulsion system can be reconfigured to provide full lift down to a speed of five m/s before air bearing need be energized. *BEC SCD C1.6.8* - Lateral guidance wheels used to stabilize vehicle when air bearings are in use. *BEC SCD C1.6.9* - If air bearing system fails, hydraulic actuators can raise vehicle for takeoff. Airstart cartridges provided for air bearing energy to allow for takeoff if compressed air system fails. *BEC SCD C1.2.5* - The emergency tow vehicles will provide air supply for air bearings when required.	BEC SCD C1.5.1 states that on-board power can be used for air compressors for air bearings. In BEC SCD C1.5.3 air compressors are not included in uses of emergency on-board power if there is failure of both on-board fuel cells. No mention of whether emergency on-board power can activate airstart cartridges mentioned in C1.6.9 if both air compressors fail. Cryogenic cooling is provided by liquid helium carried aboard in a tank located in the nose section of the vehicle. This location should be reviewed for hazards such as effects of vapor leaks, collision-caused rupture, etc.

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Guideway Integrity Reference Figure 2-1 Items 3.1.1(f) 3.1.1(h) 3.1.3(a) 3.2.2(a) 3.2.2(b) 3.2.2(c) 3.2.2(i)	Covered in Bechtel Hazard Nos. 2, 3, 6 and 12. No. 2 is guideway fails structurally causing derailment, a Category I catastrophic event. Preventive means are construction standards and an inspection program. Seismic and wind sensors also used. No. 3 is vehicle strikes obstruction, a Category I event. Prevented by above grade guideway throughout, sensors, and providing for small obstructions to be pushed off guideway by vehicle (but see concept design approach). No. 6 is vehicle collides with vehicle entering traffic, a Category I event. Prevented by conflict probes and multiple concurrence of controllers to release vehicles. No. 12 is vehicle strikes guideway due to environmental factors, a Category II critical event. Prevented by guideway sensors, vehicle monitors and automatic speed reduction if vehicle is becoming unstable.	*BEC SCD A4.8* - Linear motor windings to be connected to dynamic braking resistors to provide fail safe braking in emergencies such as loss of guideway integrity. *BEC SCD A7.1* - Automated test vehicles to make daily inspection trips to ascertain guideway condition. *BEC SCD A6.2* - Zone controllers maintain current database on their section of guideway, including weather conditions. Tailored velocity profile provided to each vehicle based on conditions. *BEC SCD C5.2.2* - Debris on track cleared by automatic test vehicle. Design guideway to minimize debris accumulation. Track monitors provide surveillance of track condition and signal zone controllers to halt oncoming vehicles.	The box-beam monorail design of the guideway provides no mechanical interlock between the vehicle and the guideway.

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Guideway Obstruction Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(h) 3.1.2(f) 3.1.3(e)	Covered in Bechtel Hazard Nos. 3 and 5. No. 3 is vehicle strikes obstruction, discussed above under baseline hazard of Loss of Guideway Integrity. No. 5 is collision with stalled vehicle, discussed above under Loss of System Power.	All design concepts for mitigating hazards associated with loss of guideway integrity also apply here. *BEC SCD B9.2* - A guideway shorting scheme is used to perform block switching. If a vehicle enters a deactivated block, the shorted winding provides a strong braking force that minimizes the potential for collision. *BEC SCD A3.9* - Automated control system will be designed and validated to ensure the probability of collision is less than 10^{-9} per hour of operation. This is in agreement with FAA standard for catastrophic events. *BEC SCD A5.4* - Each invertor station has a preferred stopping area where vehicles can make unscheduled stops in relative safety. *BEC SCD A5.5* - Internal combustion powered vehicles used to tow disabled trains to safe area. *BEC SCD A2.4* - Safe headway distance established by required vehicle stopping distance. *BEC SCD C1.2.4* - Effect of small object impacts mitigated by placing baggage and equipment compartments between front of vehicle and passenger/crew compartment. *BEC SCD C4.2.2* - Guideway sensors will monitor and transmit data on the integrity of the guideway. This includes foreign obstacles and intruders.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Fire Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(e) 3.1.2(f) 3.1.3(e) 3.2.3(a)	Covered in Bechtel Hazard Nos. 1, 9 and 21. No. 1 is fire aboard vehicle, a Category I catastrophic event. PHA list several approaches used to mitigate the effects of a fire on passengers. Some are not mentioned elsewhere in the design descriptions and some fire prevention techniques used in design not mentioned in PHA. No. 9 is fire in passenger station, also a Category I event. PHA lists several standard approaches used to mitigate fire effects in public buildings. No significant design discussion on stations provided elsewhere in report. No. 21 is fire in guideway equipment that disables power or control, a Category II critical event. PHA state automatic detection and suppression equipment provided, but design descriptions only address monitoring. Means for dealing with power loss and/or control problems apply, such as adjacent zone taking over for fire damaged equipment.	*BEC SCD C1.10.1* Vehicles will have fixed and portable fire protection systems. Fixed are electrically powered detection and extinguishing units for non-cabin areas. Portable systems are used in cabin areas. Some vehicles will carry oxygen masks or hoods. *BEC SCD C1.5.2* - On-board power fuel cells us methanol for fuel which is less likely to ignite than gasoline, diesel, or jet fuels. It burns slower and cooler. *BEC SCD C1.13.5* - Type A aircraft doors used on both sides of vehicle, front and back. *BEC SCD C4.2.1* - An on-board attendant or technician can press a "panic button" to indicate some extraordinary condition such as fire requiring an immediate stop. Emergency measures are activated when button is pressed.	Very little on fire prevention approaches. PHA and design discussion focused on detection and suppression. No information on station design. Weak correlation between PHA and design discussion on dealing with fire hazards. Evacuation plan for vehicles and stations not provided. See evacuation discussion in this report. Methanol tanks are located in forward section, vulnerable to a collision.
Evacuation and Rescue Reference Figure 2-1 Items 3.1.1(h) 3.1.2(e) 3.1.3(h)	Partially covered in Bechtel Hazard No. 22 No. 22 is vehicle stops on guideway stranding occupants, a Category III marginal event. Bechtel states that passenger rescue is a procedural matter that will be developed during later program phases.	See Section 7.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Operation Restrictions Reference Figure 2-1 Items 3.1.1(f) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.1.3(f) 3.1.3(h)	Not addressed. Operational restrictions not used as a means for mitigating the effects of identified hazards.	No specific restrictions identified other than speed and acceleration limits. Speed reductions are called for under certain circumstances such as peak use periods. Reduced speed allows shorter headways and higher system capacity with no increase in power consumption or reduction in headway safety margins. Vehicle acceleration and non-emergency deceleration is limited to values compatible with standing and walking passengers.	
Manual Override, Security and Training *Reference* Figure 2-1 Items 3.1.2(f)	Not addressed	*BEC SCD A6.5* - The station control system has some manual control functions that can be performed by station personnel, such as low speed vehicle operation and communication with stopped vehicles. *BEC SCD E3.2.6 and E3.2.7* - Manual mode recovery procedures outlined which involve technician boarding vehicle to perform resets in conjunction with Central Control. *BEC SCD E3.2.3* - Controlled access security alarms used at station guideway and other system facilities. *BEC SCD E3.5 and E4.6* - A training program for system operating and maintenance personnel is suggested and briefly described. The thrust of the program is to prepare trainees to operate the system and to diagnose and correct malfunctions.	This baseline hazard was not well addressed in the Bechtel team report.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Maintenance of Safe Headway Reference Figure 2-1 Items 3.1.1(g) 3.1.2(f) 3.1.3(e) 3.2.2(d) 3.2.2(i)	Partially covered in Bechtel Hazard Nos. 5 and 7. No. 5 is collision with a stalled vehicle, discussed above under Loss of System Power. No. 7 is vehicles collide due to incorrect headway, a Category I catastrophic event. Prevention techniques are the use of conflict probes and vehicle sensors which tell control to stop or slow vehicle. All control elements are able to slow or stop vehicles.	*BEC SCD B9.2* - A guideway shorting scheme is used to perform block switching. If a vehicle enters a deactivated block, the shorted winding provides a strong braking force that minimizes the potential for collision. *BEC SCD C4.2.2* - Collision avoidance sensors monitor and assure the correct number of blocks are maintained between vehicles. Emergency stopping procedures are activated if safety margins are violated. *BEC SCD A2.4* - Safe headway limit established by conservative vehicle stopping distance values. *BEC SCD A2.7* - During peak capacity periods, vehicles speeds will be reduced to allow shorter safe headway. *BEC SCD A4.7* - Safe headway automatically maintained if system failures cause reduced vehicle speeds.	BEC SCD A3.9 says that automated control system will be validated to ensure that the probability of a collision will be less than 10^{-9} per hour of operation. The safety assurance plan section of the report does not discuss where quantitative analyses have been or will be used.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Vehicle/ Guideway Dynamics Reference Figure 2-1 Items 3.1.1(f) 3.1.3(f) 3.1.3(h) 3.2.1(e)	Partially covered in Bechtel Hazard Nos. 8 and 12. No. 8 is excessive speed results in guideway contact or derailment, a Category I event. This hazard is discussed under the "Loss of Control System" event. No. 12 is vehicle strikes guideway due to environmental factors, a Category II critical event. This hazard is discussed under the "*Climatic/Weather Related*" *event*.	*BEC SCD C6.* - Bechtel has analyzed vehicle/guideway dynamics using the Draper five-degree-of-freedom model to simulate the SCD baseline vehicle.	The results of the analysis indicates there is a significant probability of contact between the vehicle and the guideway. Several of the assumptions made for the analysis may have influenced the result adversely, and the configuration modeled did not accurately represent the baseline vehicle. For example, the vehicle modeled has two bogies, while the baseline has six. Further analyses of the system dynamics will need to be conducted in a later phase of the program.
Electro-magnetic Interference Reference Figure 2-1 Items 3.1.1(h) 3.2.1(a) 3.2.2(b) 3.2.2(f)	Not addressed.	*BEC SCD C4.2.2* - Comment that use of capacitive rather than inductive based sensors provide better resistance to EMI.	Bechtel provides considerable analysis and discussion on the Flux Canceling EDS design and the magnet designs, but there is no discussion or design approach presented to deal with EMI effects on system control and communication equipment. The discussion of the magnetic field impact is focused on the guideway structure.

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Guideway Maintenance Operations Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(f)	Not addressed.	*BEC SCD A7.* - A comprehensive plan for guideway and vehicle maintenance is proposed which focuses on preventive measures and automatic diagnostics based largely on a concept referred to as the Integrated Prognostics and Diagnostics System. A goal of 100% fault prediction for non-electronic components has been established. *BEC SCD C1.11* - A vehicle maintenance schedule is provided. It identifies three levels: daily, quarterly, and 3-year overhaul. *BEC SCD E* - The Bechtel Operations and Maintenance Plan is described. It includes facilities and personnel requirements, and covers responses to system failures and emergencies.	The maintenance planning supplied in the Bechtel SCD focuses on the vehicle and wayside system equipment. The guideway itself is treated relatively lightly. Although the maintenance load for the guideway may well be less than for active systems, a program for periodic preventive maintenance will be needed.
Magnetic Exposure of Passengers Reference Figure 2-1 Items 3.1.1(e) 3.2.1(a)	Covered in Bechtel Hazard No. 20. No. 20 is vehicle occupants exposed to excessive electro-magnetic fields, a Category II critical event. Prevention is claimed by the use of the Bechtel team quadrapole magnet design which is inherently self canceling, preventing exposure to fields greater than those currently allowed under EPA rules. However, they recognize that "safe" level of exposure is not well defined.	*BEC SCD B4.0* - Use of "flux canceling EDS" design results in high efficiency with large fields in the vicinity of the guideway and negligible fields in the vehicle cabin. *BEC SCD B4.1* - Upper and lower rows of magnets on vehicle create a field that falls off relatively rapidly with distance. A unique method used for laminating the ladder also helps the field fall quickly with distance.	Analysis limited to field effects on occupants of vehicle. Need to consider maintenance crews, people in stations and in vicinity of guideway.

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Climatic/ Weather Related Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(m) 3.1.2(f) 3.1.3(a) 3.1.3(e) 3.2.2(f) 3.2.2(i)	Partially covered in Bechtel Hazard No. 12 No. 12 is vehicle strikes guideway due to environmental factors. A Category II critical event. Prevented by guideway sensors, vehicle monitors and automatic speed reduction if vehicle is becoming unstable due to high winds, etc. Central control has environmental data for upstream zones. Zone controllers have environmental results for several upstream zones.	Note: See also "Loss of guideway integrity" and "Guideway obstruction. *BEC SCD B8.3* - The control system allows reduced power operations in event of partial power failure. DC distribution cables and most communication line are underground thereby providing isolation from severe weather. *BEC SCD C1.7.7* - Cabin pressurization prevents dirt, dust, smoke, and other unwanted contaminates from entering cabin. *BEC SCD C1.10.2* - Lightning rods are used on the guideways but not on vehicles. This will attract lightning to the rods on the guideway instead of the vehicle. Surge protectors are part of every inverter station. Two flying beryllium wires hang down from under the vehicle and make contact with a cadmium-plated copper strip attached to the length of the guideway. This provides a constant vehicle ground in event of a vehicle lightning strike. *BEC SCD C4.2.2* - Sensors along the guideway relay data on weather/environment to zone controllers and vehicles. Proper "look ahead" distance is determined and speed is reduced or braking applied as required based conditions.	BEC SCD C1.9.5: SCD efforts to lighten vehicle were so successful that the center of gravity moved significantly higher. <u>This aggravated the side wind stability problem. This deficiency is not addressed in the baseline design</u>, but will be in later phase. The vehicle grounding scheme using flying wire should be evaluated for the effect on its functioning with various amounts of ice on the copper strip attached to top of the beam. The sensor systems that have the authority to automatically stop the vehicle must be designed to have a very low probability of false alarm.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climatic/ Weather Related		*BEC SCD C5.2.2* - Wind blown sand and debris can cause pitting of the vehicle exterior, reducing aerodynamic efficiency. The impact of wind blown sand on the guideway structural integrity should be minimal. Impact on the guideway-mounted electronics is unknown to Bechtel at this time, but all installations are mounted with a cover. Sand accumulation should have little or no impact on the magnetic fields required for levitation, propulsion, or guidance, according to Bechtel.	
Tunnels Reference Figure 2-1 Items 3.1.3(f)	Not addressed.	No specific discussion on safety hazards of passing through tunnel. General recognition that proper design is required to avoid hazards. *BEC SCD C5.1.2* - Performance compromises will be accepted for a vehicle traveling within a tunnel since it is small portion of total trip time. Drag increase in tunnel depends on tunnel dimension. Size will be optimized based on tunneling cost compared to propulsion cost. Pressure waves generated by operating through a tunnel affect vehicle structure and ride quality. Bechtel recommends a tunnel blockage ratio of 0.1 (blockage ratio = vehicle area/tunnel area). With ratios under 0.2 the pressure change outside vehicle is not significant. Drag force at ratio of 0.2 is 3 times that outside tunnel. At ratio of 0.1 drag increases only 80%.	

APPENDIX B. BECHTEL EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Reference Figure 2-1 Items 3.1.2(c) 3.2.1(c)	Bechtel Hazard No. 10: Vehicle exterior breached by object, a Category I catastrophic event.	Vehicle designed to deflect small projectiles. Projectiles which pierce vehicle skin must pass through multiple bulkheads before passenger compartment is breached. Vehicle windows will be high strength, able to deflect projectiles.	Side hits from gunfire not addressed in design.
3.1.1(h) 3.1.1(m) 3.2.1(a)	Bechtel Hazard No. 13: Vehicle occupant injured by high voltage, a Category II critical event.	All high voltage aboard vehicle is inaccessible; located exclusively in compartments accessible only to maintenance personnel.	
3.1.1(h) 3.1.1(m) 3.2.1(a)	Bechtel Hazard No. 15: Passenger injured by automatic door, a Category II critical event.	Doors are automatically monitored and operate like elevator doors to prevent closing and trapping a passenger. Provide local emergency door open button.	
3.1.1(h) 3.1.1(m)	Bechtel Hazard No. 16: Vehicle door opens at high speed, a Category II critical event.	Automatic door opening is mechanically blocked when vehicle is in motion. Emergency door must be manually opened by the emergency operator.	Emergency operator concept not explained.
3.1.1(h) 3.1.1(m)	Bechtel Hazard No. 17: Passenger trips entering or leaving vehicle, a Category II critical event.	Platform area and vehicle entry designed to minimize trip potential.	No design information provided for stations.
3.1.1(h) 3.1.1(m)	Bechtel Hazard No. 18: Passenger trips and is injured inside vehicle, a Category II critical event.	Vehicle interior designs similar to commercial airliners. Allowed vehicle tilt and roughness less than current commercial aircraft.	
3.1.1(g) 3.1.1(m) 3.1.2(b) 3.1.2(f) 3.1.3(e) 3.2.1(d)	Bechtel Hazard No. 19: Sudden high negative acceleration, a Category II critical event.	Vehicle speed changes in response to failures are gradual adjustments. Interior design minimizes hazards and provides hand holds. Seating similar to airline seats.	

APPENDIX C. FOSTER-MILLER EVENT/ISSUE MATRIX

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of System Power Reference Figure 2-1 Items 3.1.1(h) 3.1.2(b) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.2.1(a) 3.2.1((d) 3.2.3(h)	Table 7-2 - - p. 7-14 through 7-18. *Shorting of the main bus* resulting in loss of propulsion and primary braking. Heavier trains could strike the rear of lighter trains - momentum difference. <u>Resolution:</u> Provide redundant power station and system wide dynamic braking if power loss occurs.	*FM SCD 6.2.6 Major Failure Mode and Recovery* - A significant disruption of operation is identified as loss of traction power substation. Power stations are not redundant. In addition, system wide dynamic braking is not discussed.	Loss of propulsion and primary braking is potentially a Category II hazard. The PHA resolution of this hazard is to provide redundant power stations, however, the SCD addresses a single string system. Design considerations for vehicle jerk forces during skid landings are not addressed.
	Table 7-2 - - p. 7-14 through 7-18. *Open circuit on the main bus* resulting in loss of primary braking. <u>Resolution:</u> Provide quench magnets so skids provide braking and aerodynamic braking.		
	Table 7.7 - - p. 7-28 through 7-29. Propulsion failure along guideway resulting in towing train to a depot. <u>Resolution:</u> Design guideway to accommodate maintenance vehicles on guideway.		Maintenance vehicles on the guideway are not addressed in SCD.
	Table 7-2 - - p. 7-14 through 7-18. Destruction of electrical power supply plant resulting in loss of primary power for propulsion, braking and levitation. <u>Resolution:</u> Provide back-up power supply.	*FM SCD 5-4 System Power Utilization* - Back-up power is not discussed.	Loss of back-up power is potentially a Category II hazard.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System Reference Figure 2-1 Items 2.1.1(g) 3.1.1(h) 3.1.1(l) 3.2.3(a)	Table 7-2 - - p. 7-14 through 7-18. *Cut fiber optic wires to guideway coils* resulting in loss of propulsion control. <u>Resolution:</u> Make it difficult to get at wires and control braking by controlling bus voltage.	*FM SCD 6.1.6* Control Subsystem - The Communication Control Microprocessors are located along the guideway to control the local commutation of the propulsion coils. The Wayside Control Microprocessor is responsible for Automatic Train Protection (ATP) and Automatic Train Operation (ATO).	Methods for installing fiber optics are not discussed. Not all communications are fiber-optically linked. For example (Section 6.1.5 Communication Linkages) communications between trains and wayside control microprocessor are digital radio link, expect to operate in 933 MHz band. Loss of propulsion control is potentially a Category I hazard since the braking and propulsion systems are interrelated. A zonal, installation analysis is required.
	Table 7-2 - - p. 7-14 through 7-18. *Collision with trains* resulting in damage to trains and fatalities. <u>Resolution:</u> Provide sensors to detect trains and stop trains before collision. Make trains crashworthy.	*FM SCD 6.1.3* Control Subsystems - The Foster-Miller Team control system will be based on a moving block automated system. Three levels will be incorporated: • Central Control Facility (CCF) - will contain Centralized Traffic Control (CTC) system. • Wayside Control Microprocessor - located along the guideway, will be responsible for train supervision and protection. • Train presence and guideway sensors - to provide information to the control systems.	The System Configuration is similar to ATC systems in operation today. Software partitioning of vital from non-vital functions must be performed.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation or Guidance and Levitational Guidance/ Magnet Failure Reference Figure 2-1 Items 3.1.2(d) 3.2.1(a) 3.2.3(h)	Not addressed in hazard analysis	*FM SCD 4.3.5* - Selected Levitation Configuration. Based on the analysis, vertical sidewall null-flux levitation scheme was selected.	This is potentially a Category II hazard. Loss of magnetic suspension represents a serious safety issue. Hazards relating to magnet quenching due to vibration, impact, loss of coolant, cryostat vacuum failure, etc. need to be addressed.
Loss of Guideway Integrity Reference Figure 2-1 Items 3.1.1(f) 3.1.1(h) 3.1.3(a) 3.2.2(a) 3.2.2(b) 3.2.2(c) 3.2.2(i)	Table 7-7 - - p. 7-28 through 2-29 *Ground settling around guideway pylons.* Resolution: Determine tolerance levels acceptable for both the train and guideway. Design the guideway accordingly.	*FM SCD 3.9 Guideway Instrumentation p. 3-117*: A complete guideway monitoring systems is required and shall include: 1) a system to record vehicle passage for deterioration, misalignment, excessive precipitation build-up, harsh weather conditions and presence of foreign object. 2) embedded fiber optic sensors to provide structural integrity, strains and temperature to train control system via a direct optical signal to the wayside system. 3) a drone inspection vehicle to be used once per day over the entire route.	In spite of a lack of communication between the author of the safety analysis and the designer, this hazard appears to be adequately mitigated. This is potentially a Category I catastrophic hazard.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Guideway Obstruction Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(h) 3.1.2(f) 3.1.3(e)	Table 7-2 - - p. 7-14 through 7-18. Miscellaneous objects on guideway: Damage to front of train and magnets. Results in loss of braking, propulsion and levitation. <u>Resolution:</u> Guideway to train sensors to detect objects. Redundant train systems.	*FM SCD 3.9 Guideway Instrumentation p. 3-117*: A complete guideway monitoring system is required and shall include: 1) a system to record vehicle passage for deterioration, misalignment, excessive precipitation build-up, harsh weather conditions and presence of foreign objects. 2) embedded fiber optic sensors to provide structural integrity, strains and temperature to train control system via a direct optical signal to the wayside system. 3) limited security fencing, overhead shielding video incident detection system and video security cameras 4) a drone inspection vehicle to be used once per day over the entire route.	This is a potentially Category I catastrophic event. The resolution in the PHA does not adequately resolve the hazard.
	Table 7-2 - - p. 7-14 through 7-18. *Passengers dropping ferromagnetic objects onto guideway* at stations resulting in damage to guideway coils, train, magnets and bogies. <u>Resolution:</u> Isolate passengers from guideway similar to aircraft boarding.	Not addressed in SCD.	This is potentially a Category II hazard. The superconducting magnet cryostats are particularly prone to damage from ferromagnetic debris impact due to magnetic attraction.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Guideway Obstruction (continued)	Table 7-2 - - p. 7-14 through 7-18. *Objects consistently and randomly found on guideway routes.* <u>Resolution:</u> Maintenance locate and remove objects. Develop public awareness programs.	*FM SCD 3.9 Guideway Instrumentation p. 3-117*: A complete guideway monitoring systems is required and shall include: 1) a system to record vehicle passage for deterioration, misalignment, excessive precipitation build-up, harsh weather conditions and presence of foreign object. 2) embedded fiber optic sensors to provide structural integrity, strains and temperature to train control system via a direct optical signal to the wayside system. 3) limited security fencing, overhead shielding video incident detection system and video security cameras 4) a drone inspection vehicle to be used once per day over the entire route.	This is potentially a Category I hazard. It is too critical to mitigate with public awareness programs and maintenance actions. Mitigating this hazard may include monitoring the entire guideway for objects. The PHA does not adequately resolve this hazard.
	Table 7-2 - - p. 7-14 through 7-18. *Maintenance tools left on bogies and guideways* resulting in damage to train and/or guideway magnets. <u>Resolution:</u> Probe vehicle after maintenance.	Not addressed in SCD.	This is potentially a Category II hazard. Although this appears to be an obscure hazard, it has potential to be significant, particularly with respect to tools left near the bogies.
	Table 7-2 - - p. 7-14 through 7-18. *Heavy objects hung in path of moving train* resulting in damage to front of train and injuries to train operator. <u>Resolution:</u> Reinforce front and remove windows.	Not addressed in SCD.	Design criteria should be developed that prevents things from being hung in front of the train.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Guideway Obstruction (continued)	Table 7-2 - - p. 7-14 through 7-18. *Snow* - Impair visibility and build-up on guideway. <u>Resolution:</u> Slanted guideway surfaces.	*FM SCD 3.9* Guideway instrumentation includes embedded fiber optic that will detect temperatures. Incorporate a system to record vehicle passage for deterioration, misalignment, excessive precipitation build-up, harsh weather conditions and presence of foreign object.	The proposed guideway cross-section may be prone to snow accumulation. The PHA resolution is inadequate.
	Table 7-2 - - p. 7-14 through 7-18. *Birds, squirrels and animals on guideway* resulting in damage to front of train. <u>Resolution:</u> Slanted guideway surfaces.	Not addressed in SCD.	This is potentially a Category II hazard. The PHA resolution is not viable to mitigate the hazard. A review of the selected guideway Cross-section (Figure 3-50 p. 3-38) shows that slanted surfaces were not selected.
	Table 7-2 - - p. 7-14 through 7-18. *Collision of train and people on guideway* resulting in damage to train and fatalities. <u>Resolution:</u> Slope guideway to keep people off. Sensors to detect people on guideways. Horns located at pre-determined intervals on guideways to alert people of approaching train.	Not addressed in SCD.	This is potentially a Category II hazard. A review of the selected guideway Cross-section (Figure 3-50 p. 3-38) shows that slanted surfaces were not selected.
	Table 7-2 - - p. 7-14 through 7-18. *Magnetic dust/clay builds up on train/guideway magnets.* Effect of this hazard is not discussed. <u>Resolution:</u> Perform train magnet maintenance.	Not addressed in SCD.	Foster-Miller is placing much of the safety assurance burden on the proper maintenance of the guideway and maglev system. Furthermore, the reference of this hazard is not clear.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	**CONCEPT DESIGN FOR MITIGATING HAZARDS**	
Guideway Obstruction (continued)	Table 7-2 - - p. 7-14 through 7-18. *Power Lines fall over guideway* resulting in train derailment. Resolution: Design front of train to channel cable over the top. Install a cable cutter similar to helicopters.	Not addressed in SCD.	This is a very obscure hazard.
Fire Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(e) 3.1.2(f) 3.1.3(e) 3.2.3(a)	Table 7-2 - - p. 7-14 through 7-18. *Train damage, chemical vapors, fatalities and injuries* Resolution: Fire detection and suppression system.	*FM SCD 7.1.2 Fire Prevention, Detection and Protection:* Ensure the fire codes as defined by the FRA are met including fire sensors and extinguishers. Provide fire retardant materials. In the event of an on-board fire, stop the train and walk out the main doors. Provide battery power to cars to ensure adequate emergency lighting and ventilation.	There are no FRA codes pertaining to fire detectors and extinguishers. This is potentially a Category I hazard. The hazard analysis is not complete. The concept design has many mitigating measures that are not considered by the safety analysis. Relevant fire hazard mitigation is available from aircraft and mass transit vehicle experience.
Evacuation and Rescue Reference Figure 2-1 Items 3.1.1(h) 3.1.2(e) 3.1.3(h)	Table 7-7 - - p. 7-28 through 2-29 *Emergency access/egress from train in tunnel.* Resolution: Design train and tunnel to safely evacuate people off train and through tunnel. Provide satisfactory lighting. Table 7-7 - - p. 7-28 through 2-29 *Emergency access/egress on elevated structures* Resolution: Design locations of emergency exits to safely exit persons to the guideway or ground.	*7.1.3 p. 7-4 Evacuation Plans*	An emergency evacuation plan is provided and discussed in detail under the emergency evacuation section of this report.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Evacuation and Rescue (continued)	Table 7-7 - - p. 7-28 through 2-29 *Handicap egress from train on elevated guideway.* <u>Resolution:</u> Design mechanism to interact between train and guideway to safely remove passengers from train to guideway or ground. Table 7-2 - - p. 7-14 through 7-18. Safe methods of evacuating passengers off the guideway in emergencies. <u>Resolution:</u> Provide air slides, fireman's tube, walkways on guideway. Repelling concept utilizing seat belts. Provide spring loaded ropes.		
Operation Restrictions Reference Figure 2-1 Items 3.1.1(f) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.1.3(f) 3.1.3(h)	Not addressed in Hazard Analysis	*FM SCD 6.2* 5- Major Failure Mode and Recovery - Two significant disruptions which may occur to maglev operations are a disabled train and loss of a traction power substation. In either case, the guideway for one direction would be blocked for an extended period. The usual approach to handling such problems is to initiate "reverse running" on the remaining track via emergency crossovers provided to move trains from one track to another.	The operation of longer car consists is desirable if it minimized the possibility of secondary collisions at short headways.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Manual Override, Security and Training Reference Figure 2-1 Items 3.1.2(f)	Not addressed in Hazard Analysis	Not addressed in SCD	Hazards associated with manual operations, security and training should be addressed.
Maintenance of Safe Headway Reference Figure 2-1 Items 3.1.1(g) 3.1.2(f) 3.1.3(e) 3.2.2(d) 3.2.2(i)	Table 7-2 - - p. 7-14 through 7-18. Computer Virus results in false commands to train, guideway, switching that may result in train collisions. Resolution: Provide anti-virus software and continuous monitoring of computers. Provide backup system.	*FM SCD 6.1.7* - Design Impacts - The minimum safe headway (i.e. time interval) between any two vehicles can be determined based on vehicle speed and the associated "worst case" braking capabilities. For the purposes of estimating a safe headway, it has been assumed that only air resistance and fail-safe skid deployment will act on the train.	Software virus is considered an obscure hazard. Software safety should be based on quality assurance, documentation of code, and verification/validation of software.
Vehicle Guideway Dynamics Reference Figure 2-1 Items 3.1.1(d) 3.1.1(f) 3.1.3(f) 3.1.3(h) 3.2.1(e)	Table 7-2 -- p. 14-18. Environmental corrosion of guideway and train components results in damage to structural integrity and catastrophic failures. Resolution: Periodic inspections similar to aircraft	Not addressed in SCD.	Vehicle/Guideway Dynamics need to be resolved with respect to: • Vertical switching • Tilting mechanism

APPENDIX C. FOSTER-MILLER EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Electro-magnetic Interference and Compatibility Reference Figure 2-1 Items 3.1.1(h) 3.2.1(a) 3.2.2(b) 3.2.2(f)	Table 7-2 -- p. 7-18. EMI fields and passenger exposure. Communication control and data processing malfunctions. <u>Resolution:</u> *Shielding methods and study effects on humans*	*FM SCD 8.3* discusses EMI in detail.	No issues with this design approach.
Guideway Maintenance Operations Reference Figure 2-1 Items 3.1.1(h) 3.2.1(a) 3.1.2(f)	Not addressed in PHA	*FM SCD 9.7* - Only operating and maintenance costs are addressed	There are many O&M issues not discussed by Foster-Miller..
Magnetic Exposure Reference Figure 2-1 Items 3.1.1(e) 3.2.1(a)	Table 7-2 -- p. 7-18. EMI fields and passenger exposure. Potential communication control and data processing malfunctions. <u>Resolution:</u> Shielding methods and study effects on humans	*FM SCD 8.3* discusses EMI in detail	Nearly all available techniques for magnetic field shielding are considered in the SCD, but a baseline shielding design is not defined. The potential hazard of shield failure is not discussed in the SCD.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climatic/ Weather Related Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(m) 3.1.2(f) 3.1.3(a) 3.1.3(e) 3.2.2(f) 3.2.2(g)	Table 7-2 - - p. 7-14 through 7-18. Tornadoes result in damage to guideways, trains and coils. Excess debris on guideway. Resolution: Design guideway to withstand tornadoes and provide slanted guideways. Table 7-2 - - p. 7-14 through 7-18. Environmental corrosion of guideway and train components due to UV, acid rain etc. Resolution: Perform periodic inspections.		Weather issues related to icing, wind, rain, lightning and earthquakes should be addressed during subsequent design phases.
Tunnels Reference Figure 2-1 Items 3.1.3(f)	Not addressed in PHA	*FM SCD 3.6.2* - No specific discussion of safety hazards. General recognition that proper design is required to avoid hazards. Drag is increased in tunnels	There are no safety issues associated with Foster-Miller design approach at this stage of design development.
Electrical Shock Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.2.1(a)	Table 7-2 - - p. 7-18. Electrical shock results in injuries and power failures. *Resolution:* Install circuit protection and security for unauthorized personnel.	Not discussed in SCD.	This hazard should be discussed in subsequent design phases.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Braking Reference Figure 2-1 Items 3.1.1(g) 3.1.1(m) 3.1.2(b) 3.1.2(f) 3.1.3(e) 3.2.1(d)	Table 7-2 - - p. 7-18. Passenger comfort and safety of seat belted and standings. <u>Resolution:</u> Maintain minimal braking rate below 0.2gs.	p. 2-41 Braking: The brake system is capable of multiple stops from speeds as high as 57m/sec and deceleration levels in excess of 0.25gs. *FM SCD 6.1.7* Design Impacts - The Foster-Miller design employs multiple separate braking systems to provide high redundancy for safety. The primary system is high speed braking is electrical regenerative braking system. When emergency braking is initiated, deceleration is controlled by regenerative braking system in conjunction with aerodynamic controls at a constant braking rate of 0.25 g. The landing gear brakes provide additional emergency braking. Finally, deployable skids are available during major system failure.	The hazard associated with high g braking on passengers should be addressed.
Doors Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.2.1(a)	Not addressed in PHA.	*FM SCD 7.1.4* Door Operation - Doors will be controlled by the attendant in each car. In addition, sensors in the door reopen should they encounter an object or person on closing.	Vehicle door operation can represent a significant hazard and should be addressed.

APPENDIX D. GRUMMAN EVENT/ISSUE MATRIX

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of System Power Reference Figure 2-1 Items 3.1.1(h) 3.1.2(b) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.2.1(a) 3.2.1(d) 3.2.3(h)	*Baseline hazard subdivided into eight hazards:* Loss of Utility Power to Wayside Substations (1.1-1.2) results in train losing propulsion/dynamic braking; possible collision. (Category I) Control provisions provide for on-board emergency braking capability.	*GM SCD 3.2.1.4.4 p. 3-164* The recommended braking approach for our baseline is as follows: • For normal operations the regenerative braking approach will be used. • During emergency power loss the eddy current brake in conjunction with the friction brake will be used for the high and low speed regions respectively.	
	Loss of or Reduction in AC Power to Guideway (1.3-1.7) results in train losing propulsion/dynamic braking; possible collision. (Category I) Control provisions provide for on-board emergency braking capability.	Same as Hazard 1.1-1.2	
	Inability to Remove Guideway Power (1.8) results in possible collision between trains. (Category I) Control provisions utilize "fail-safe" relay or redundancy technique for stator switches.	Not addressed	No discussion or description of stator switch design in SCD.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of System Power (continued)	Power Discontinuity Between Guideway Sections (1.9-1.10) results in variation in train propulsion/braking. (Category IV) Control provisions include interaction required between adjacent substation control equipment; design in "fail-safe" manner; utilize redundant control links.	Hazard is defined as a Category IV Minor event, therefore, design plan was not verified.	
	Inability to Dissipate Energy During Braking (1.11-1.12) results in loss of braking. (Category I) Control provisions provide for on-board emergency braking capability.	Same as Hazard 1.1-1.2	
	Inability to Provide Requested Regenerative Braking (1.13) results in train loses dynamic braking. (Category I) Control provisions provide for onboard emergency braking capability.	Same as Hazard 1.1-1.2	
	Excessive Regenerative Braking Occurs (1.14-1.15) resulting in possible minor injury. (Category III) Control provisions include use of highly reliable component and design in "fail-safe" manner	Hazard is defined as a Category III Marginal event, therefore, the design plan was not verified.	
	Braking Occurs When Not Desired (1.16-1.17) results in train stops/slows when not desired. (Category IV) Control provisions include design control in "fail-safe" manner.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System Reference Figure 2-1 Items 3.1.1(g) 3.1.1(h) 3.1.1(i) 3.2.3(a)	Hazard was subdivided into fifty-one hazards: <u>Loss of or Insufficient Propulsion Commanded (to Inverters) (3.1)</u> resulting in train running slower than desired or may stop. (Category IV) Control provisions include using redundant computers.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	
	<u>Excessive Propulsion Commanded (to Inverters) (3.2)</u> resulting in overspeed or collision. (Category I) Control provisions include designing command speed generation function in substation in "fail-safe" manner; also, remove propulsion in "fail-safe" manner and utilize "fail-safe" on-board emergency brake.	*GM SCD 3.2.3.13.3 p. 3-543* The intent in the Grumman design/implementation is to utilize fault tolerant, checked redundant computers to perform many safety critical functions both on-board and at the wayside substations. The term "checked redundant computers" implies that two or more computers will operate in parallel, and their outputs will be checked or compared for agreement. Should disagreement occur, the system/function will revert to a safe state. A redundant configuration of this nature helps ensure a high level of safety because it results in a low probability of unsafe failures. While this is not the only means of achieving a high level of safety, it is the one means intended at this time in the design. *GM SCD 3.2.1.4.4 p. 3-164* The recommended braking approach for the baseline is as follows: • For normal operations the regenerative braking approach will be used. • During emergency power loss the eddy current brake in conjunction with the friction brake will be used for the high and low speed regions respectively.	The referenced paragraph (p. 3-543) in the design plan column is located in the *3.2.3 Safety Assurance Plan* section of the SCD, not in the design requirements of the vehicle/stations. No software requirements are discussed for the various computer functions.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Loss of or Insufficient Dynamic Braking Commanded (3.3) resulting in overspeed or collision. (Category I) Control provisions include utilizing "fail-safe" on-board emergency brake.	Same as Hazard 3.2	
	Excessive Dynamic Braking Commanded (3.4) resulting in excessive deceleration causing minor injury. (Category III) Control provisions include using redundant computers.	Same as Hazard 3.2	
	Braking (at Substation) Commanded When Not Desired (3.5) resulting in excessive deceleration causing minor injury. (Category III) Control provisions include using redundant computers to control dynamic braking.	Same as Hazard 3.2	
	Incorrect Headway or Braking Distance Determined (3.6) resulting in possible collision. (Category I) Control provisions include designing safe headway determination function in substation computer in "fail-safe" manner.	Same as Hazard 3.2	
	Incorrect Comparison of Command and Actual Speed (3.7) resulting in possible overspeed and/or collision. (Category I) Control provisions include designing comparison of command and actual speed function in substation computer in "fail-safe" manner.	Same as Hazard 3.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Improper Generation of Speed Command (3.8) resulting in possible overspeed and/or collision. (Category I) Control provisions include designing speed command generation function in substation computer in "fail-safe" manner.	Same as Hazard 3.2	
	Incorrect Route Integrity Data Received (e.g., Switch Position, Obstacles on Guideway) (3.9) resulting in possible collision with train or object. (Category I) Control provisions include designing route integrity subsystem in "fail-safe" manner; includes protection from nonconflicting routes and detection of obstacles on guideway.	*GM SCD 3.2.3.1.4 p. 3-368* The two fiber optic lines run a ring version of Sonet at the Sonet OC-3 rate of 155.52 Mbps. The ring topology offers higher reliability than two parallel, one-way busses. Each T1 cable consists of 24 simplex lines. There are two such cables per region, one each for two of the four fiber optic rings, for hardware redundancy.	
	Improper Interpretation/Response to Route Integrity Input (3.10) resulting in possible overspeed and/or collision. (Category I) Control provisions include designing route integrity portion of substation computer in "fail-safe" manner.	Same as Hazard 3.9 Same as Hazard 3.2	
	Failure to Command Emergency Braking (3.11) resulting in emergency braking may not occur when needed; overspeed and/or collision could occur. (Category I) Control provisions include designing emergency brake control function in substation computer in a "fail-safe" manner; on-board computer must respond to loss of emergency brake command signal.	Same as Hazard 3.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Control and/or Communication System (continued)	<u>Incorrect Interpretation of Vital Train Operating Data (e.g., Location, Speed, Direction) (3.12)</u> resulting in possible overspeed and/or collision. (Category I) Control provisions include designing functions which use this vital data in substation computer in "fail-safe" manner.	*GM SCD 3.2.3.1.3 p. 3-361* The principle duty of the Regional Control Center (RCC) is reliable handling of the power distribution network that drives the vehicles. The basic functions we need to perform are: • Prevent injury to personnel • Prevent or minimize damage to power equipment and guideway • Minimize interruption of power • Contain failures • Minimize effect of faults on the utility system Strategies employed to achieve these goals are: provide ground fault protection, use fault-tolerant (hardware redundant) circuit breaker strategies, analyze in advance and have strategies (algorithms) to achieve the above goals in the event of over currents, etc. *GM SCD 3.2.3.1.5 p. 3-369* Safety considerations will require that the communication link between the vehicle and the regional centers be extremely reliable. Methods for achieving high reliability communications will be detailed below, but an interaction between control and communication functions requires that the quality of the communication link be measured, and a loss or deterioration of the communication link will force both the vehicle and the regional centers to command an emergency stop.	

APPENDIX D. GRUMMAN EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Incorrect Response to Critical Train Equipment Failure and Emergency Condition Status (e.g., Emergency Brake, Fire) (3.13) resulting in possible overspeed and/or collision; or unsafe fire situation could exist. (Category I) Control provisions include designing substation computer to handle this data in "fail-safe" manner (e.g., reduce speed command, remove propulsion)	Same as Hazard 3.12 Same as Hazard 3.2	
	Incorrect Response to Critical Substation Equipment Failure and Emergency Condition Status (3.14) resulting in possible overspeed and/or collision, or unsafe fire situation could exist. (Category I) Control provisions include designing substation computer to handle this data in "fail-safe" manner (e.g., reduce speed command, remove propulsion).	Same as Hazard 3.12 Same as Hazard 3.2	
	Start-Up Not Initiated (3.15) resulting in train not leaving station area or other location when desired. (Category IV) Control provisions include designing function in highly reliable manner.	Same as Hazard 3.12 Same as Hazard 3.2	
	Start-Up Initiated Prematurely (Propulsion When not Desired) (3.16) resulting in possible injury while boarding/deboarding or possible collision with another train. (Category I) Control provisions include designing start-up function to be "fail-safe", taking into account factors such as doors closed, headway, etc.	Same as Hazard 3.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Train Not Stopped/Positioned Properly In Station (3.17) resulting in possible injury to passenger while boarding/deboarding. (Category II) Control provisions include utilizing accurate position measurement devices in station area.	Not addressed.	No discussion or description of vehicle position measurement system in stations is in SCD.
	Switching Not Commanded When Desired (3.18) resulting in possible collision with another train. (Category I) Control provisions include designing switch control function in substation in "fail-safe" manner; utilize closed-loop technique; ensure adequate stopping distance and headway whether or not switch moves when commanded.	*GM SCD 3.2.2.4.3 p. 3-296* To ensure the fail-safe operation of the switch in the event of any component malfunctioning, a number of measures have been devised: • Each switch section is designed to return to the straight-through position in the event of a power loss or breakdown during operation. • Dual components will be used for cylinders, pumps, motors, etc. • Dual power supply. • Mechanically operated locking bars will be used to align the switch sections meeting at the machinery pier either for the switch-open or switch-closed position. Same as Hazard 3.2	
	Switching Commanded When Not Desired (3.19) resulting in possible train leaving guideway or suffer major damage. (Category I) Control provisions include designing switch control function in substation in "fail-safe" manner; utilize closed-loop technique.	Same as Hazard 3.18 Same as Hazard 3.2	

APPENDIX D. GRUMMAN EVENT/ISSUE MATRIX (Continued)

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Control and/or Communication System (continued)	Incorrect Train Location Determined (3.20) resulting in possible headway violation and collision. (Category I) Control provisions include designing train location determination function in "fail-safe" manner.	Same as Hazard 3.2	
	Incorrect Train Speed Determined (3.21) resulting in possible overspeed and collision. (Category I) Control provisions include designing actual train speed measurement function in "fail-safe" manner.	Same as Hazard 3.2	
	Incorrect Train Direction Determined (3.22) resulting in possible headway violation and collision. (Category I) Control provisions include designing train direction determination function in "fail-safe" manner.	Same as Hazard 3.2	
	Emergency Braking not Initiated (3.23) resulting in possible headway violation and collision. (Category I) Control provisions include designing emergency brake control circuit in "fail-safe" manner.	Same as Hazard 3.2	
	Emergency Brake not Initiated When Requested From Wayside (3.24) resulting in possible headway violation and collision. (Category I) Control provisions include designing emergency brake control circuit to handle wayside command in "fail-safe" manner.	Same as Hazard 3.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Emergency Brake not Initiated When Requested (3.25) resulting in possible headway violation and collision. Control provisions include designing emergency brake control function so that operator request is acknowledged in "fail-safe" manner and overrides normal signals	Same as Hazard 3.2	Manual override of emergency brake is not addressed in the design text.
	Insufficient Emergency Braking Initiated (3.26) resulting in possible overspeed or collision. (Category I) Control provisions include designing emergency brake control circuit in "fail-safe" manner.	Same as Hazard 3.2	
	Emergency Braking Commanded When not Desired (3.27) resulting in possible injury to passenger during braking. (Category III) Control provisions include making emergency brake hold-off function highly reliable.	Same as Hazard 3.2	
	Emergency Braking Utilized (Under Normal Circumstances) (3.28) resulting in possible injury to passenger during braking. (Category III) Control provisions include designing emergency braking within acceptable deceleration limits, and maintain proper guidance on guideway.	*GM SCD 3.2.1.4.4 p. 3-164* The recommended braking approach for our baseline is as follows: • For normal operations the regenerative braking approach will be used. • During emergency power loss the eddy current brake in conjunction with the friction brake will be used for the high and low speed regions respectively.	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Control and/or Communication System (continued)	Critical On-Board Equipment Failure or Emergency Condition Not Acknowledged (3.29) resulting in possible overspeed, collision, or on-board fire. (Category I) Control provisions include designing on-board processing system to handle such inputs in "fail-safe" manner and evoke emergency braking as appropriate.	Same as Hazard 3.2	
	Door Opening Not Commanded (3.30) resulting in passengers unable to egress vehicle, resulting in possible injury. (Category II) Control provisions include allowing passengers to open door in emergency.	*GM SCD 3.2.1.13.4 p. 3-225* The on-board attendant will be able, on demand, to override the automatic door control system. In addition, the vehicle also will contain an external and internal means to manually operate the doors in the event of power failure affecting door operations.	
	Door Opening Commanded When Not Desired (3.31) resulting in possible door opening during train movement. (Category I) Control provisions include designing door control function (door closure) in "fail-safe" manner with passenger override capability in emergency.	*GM SCD 3.2.1.13.4 p. 3-224* The C^3 system will control the opening and closing of the side doors and the vehicle will not move until all side doors are locked in the closed position and the C^3 system gives a "proceed" signal when all "doors closed" signals are indicated. The on-board attendant will be able, on demand, to override the automatic door control system. In addition, the vehicle also will contain an external and internal means to manually operate the doors in the event of power failure affecting door operations. Same as Hazard 3.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Doors Close On Passenger When Entering/Departing Vehicle (5.18) resulting in possible injury. Control provisions include employing door sensors to detect presence in doorway; employing proper timing and use proper door closing force.	Hazard is defined as a Category III Marginal event, therefore, the design plan was not verified.	
	Incorrect Speed/Movement Requests Made From Central (3.32) resulting in possible headway violation or overspeed resulting in collision. (Category I) Control provisions include designing substation control equipment in "fail-safe" manner to ensure safe operation.	*GM SCD 3.2.3.1.1 p. 3-357* Any failure of subsystems, equipment or components within the C^3 System that may lead to an unsafe state will be self-detecting. Self-detecting failures will result in vehicles stopping or operating at the correct speed or a more restrictive safe speed. No single component failure within the C^3 System will result in an unsafe condition.	
	Train Speed, Location, or Direction Displayed Incorrectly at Central (3.33) resulting in incorrect train status information displayed to central operator. (Category IV) Control provisions include designing vehicle monitoring in a highly reliable manner.	Same as Hazard 3.32	
	Train/Wayside Equipment Status Displayed Incorrectly at Central (3.34) resulting in incorrect equipment status displayed to central operator; unsafe situation could go unnoticed, resulting in overspeed or collision. (Category I) Control provisions include critical equipment failures of train or wayside should be handled by substation equipment in "fail-safe" manner.	Same as Hazard 3.32	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Emergency/Alarm Conditions Displayed Incorrectly at Central (3.35) *resulting in emergency/alarm* condition could go unnoticed, resulting in collision with object, another train, or person; also, train may not be stopped in fire situation. (Category I) Control provisions include acknowledgment of critical on-board and wayside emergency conditions and responded to by substation equipment in "fail-safe" manner.	Same as Hazard 3.32	
	Loss of Fiber Optic Data Link Between Substations (2.1) resulting in loss of sync in guideway power causing propulsion/braking variation; loss of adjacent train location/speed/route integrity data, resulting in possible collision between trains, switch, or with object. (Category I) Control provisions include designing substation computer in "fail-safe" manner to safely shutdown train when link is lost.	*GM SCD 3.2.3.1.4 p. 3-363* The DRB busses are the communications links between RCCx and RCC(x+1) as well as the communications channels internal to each region. The links are labeled 4 in Fig. 3.2.3-1. The DRBs form a fail-safe distributed network partitioned by geographical regions. The system Grumman is baselining used hardware redundancy to achieve a fail safe status. The plan is to use self-checking pairs in all the data links except for the RCCx to Vecom interfaces. Opto-isolators are used to protect the DRB from the high-voltager equipment. Shielded, armored, water-proof cabling is used to protect the bus lines in the harsh substation environment.	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Control and/or Communication System (continued)	Incorrect Encoding/Decoding of Propulsion/Braking Data in Substation (2.2) resulting in loss of sync in guideway power resulting in propulsions/braking variations. (Category IV) Control provisions include designing encoder/decoder scheme in "fail-safe" manner.	*GM SCD 3.2.3.1.3 p. 3-361* The principle duty of the Regional Control Center (RCC) is reliable handling of the power distribution network that drives the vehicles. The basic functions we need to perform are: • Prevent injury to personnel • Prevent or minimize damage to power equipment and guideway • Minimize interruption of power • Contain failures • Minimize effect of faults on the utility system Strategies employed to achieve these goals are: provide ground fault protection, use fault-tolerant (hardware redundant) circuit breaker strategies, analyze in advance and have strategies (algorithms) to achieve the above goals in the event of over currents, etc. *GM SCD 3.2.3.1.5 p. 3-369* Safety considerations will require that the communication link between the vehicle and the regional centers be extremely reliable. Methods for achieving high reliability communications will be detailed below, but an interaction between control and communication functions requires that the quality of the communication link be measured, and a loss or deterioration of the communication link will force both the vehicle and the regional centers to command an emergency stop.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)		*p. 3-374* On the vehicle the communication link consists of two antennas, separated by as great a distance as possible, and each antenna connected to multiple frequency transceiver. Redundant transceivers are fitted at each antenna location, with fault identification via electronic self-test. A necessary feature of the communication link is that a quantitative, continuous measure of link quality is needed for safety reasons. Diversity reception can easily provide this data.	
		GM SCD 3.2.3.13.3 p. 3-543 The intent in the Grumman design/implementation is to utilize fault tolerant, checked redundant computers to perform many safety critical functions both on-board and at the wayside substations. The term "checked redundant computers" implies that two or more computers will operate in parallel, and their outputs will be checked or compared for agreement. Should disagreement occur, the system/function will revert to a safe state. A redundant configuration of this nature helps ensure a high level of safety because it results in a low probability of unsafe failures. While this is not the only means of achieving a high level of safety, it is the one means intended at this time in the design.	The referenced paragraph (p. 3-543) in the design plan column is located in the *3.2.3 Safety Assurance Plan* section of the SCD, not in the design requirements of the vehicle/stations. No software requirements are discussed for the various computers.
	<u>Incorrect Encoding/Decoding of Train Location, Speed, or Route Integrity Data in Substation (2.3)</u> resulting in possible collision between trains, switch, or with object. (Category I) Control provisions include designing encoder/decoder functions to be "fail-safe".	Same as Hazard 2.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Control and/or Communication System (continued)	Loss of Central to Substation Data Link (2.4) resulting in loss of scheduling capability. (Category IV) Control provisions include using redundant link.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	
	Loss of Substation to Central Data Link (2.5) resulting in loss of train, alarm condition, or equipment status data; service disruption possible. (Category IV) Control provisions include using redundant link.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	
	Incorrect Encoding/Decoding of Nonvital Train Status Data (e.g., Speed, Location) at Substation or Central (2.6) resulting in incorrect train status data at central; service disruption possible. (Category IV) Control provisions include ensuring safety of system via wayside/on-board equipment.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	
	Incorrect Encoding/Decoding of Substation Equipment Status Data at Substation or Central (2.7) resulting in incorrect equipment status data at central; service disruption possible. (Category IV) Control provisions include designing substation equipment for safe shutdown if problem exists.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System *(continued)*	Incorrect Encoding/Decoding of Other Alarm Data (e.g., Intrusion, Fire) at Substation or Central (2.8) resulting in incorrect alarm data for emergency situations; possible service disruptions. (Category IV) Control provisions include designing substation equipment for safe shutdown if problem exists.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	
	Incorrect Encoding/Decoding of Control Signals From Central (2.9) resulting in incorrect propulsion/braking requested by central, resulting in collision. (Category I) Control provisions include designing for safe operation ensured at substation ("fail-safe" computer).	Same as Hazard 2.1-2.2	
	Loss of Train to Substation Vital Operating Data Lnk (e.g., Train Location, Speed, Direction) (2.10) resulting in wayside losing knowledge of vital train data; collision could occur between trains or overspeed could occur. (Category I) Control provisions include designing substation computer in "fail-safe" manner so that loss of train data results in safe stopping of affected trains.	Same as Hazard 2.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Incorrect Encoding/Decoding of Vital Train Operating Data (e.g., Location, Speed) (2.11) resulting in collision or overspeed condition. (Category I) Control provisions include designing encoder/decoder in "fail-safe" manner (on-board and at substation).	Same as Hazard 2.2	
	Loss of Train Equipment Status and Emergency Condition Data Link at Substation (2.12) resulting in improper speed command, resulting in overspeed or collision with another train. (Category I) Control provisions include designing substation computer in "fail-safe" manner so that loss of critical train data results in safe stopping of affected trains.	Same as Hazard 2.2	
	Incorrect Encoding/Decoding of Vital Train Equipment Status and Emergency Condition Data (2.13) resulting in improper speed command, resulting in overspeed or collision with another train. (Category I) Control provisions include designing encoder/decoder in "fail-safe" mannes(on-board and at substation).	Same as Hazard 2.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	Loss of Substation to Train Vital Data Link (e.g., Emergency Brake Signal) (2.14) resulting in train emergency braking may not occur when needed; possible collision/overspeed. (Category I) Control provisions include designing on-board computer in "fail-safe" manner so that loss of emergency brake signal results in emergency braking.	Same as Hazard 2.2	
	Incorrect Encoding/Decoding of Substation to Train Vital Data (2.15) resulting in train emergency braking may not occur when needed; possible collision/overspeed. (Category I) Control provisions include designing encoder/decoder in "fail-safe" manner (on-board and at substation).	Same as Hazard 2.2	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Levitation/ Guidance and Levitation/ Guidance/ Magnet Failure Reference Figure 2-1 Items 3.1.2(d) 3.2.1(a) 3.2.3(h)	Hazard subdivided into nine hazards: Loss of All Levitation/Guidance at Normal Speeds (4.1-4.3) resulting in undesired contact with guideway resulting in possible passenger injury. (Category II) Control provisions include use of multiple on-board storage batteries in highly reliable configuration; safe braking should be possible while maintaining vehicle/guideway integrity; configure power interconnections between batteries/pickup and magnets in highly reliable manner; use constant current supply for each superconducting magnet.	*GM SCD 3.2.1.4.4 p. 3-166* The requirement was not only to provide emergency braking, but also to provide a surface for emergency wheels to contact in case large lateral motions occur, thus preventing the magnet pole face from touching the rail. The evaluation of the guideway hat section vs. the thick section is shown in Fig. 3.2.1-95.....As a result it was concluded that the hat section was the best design for our baseline. *GM SCD 3.2.1.1.4 p. 3-66* The system is designed so that each magnet can be controlled separately. This requires an independent power supply for each SC magnet.	On-board batteries are mentioned periodically throughout the SCD. There is no detailed discussion or description of the batteries in the SCD. Unable to locate design redundancy techniques in Gap Control System Analysis
	Loss of or Reduced Levitation/Guidance During Passenger Boarding/Deboarding (4.4) resulting in passenger injury while boarding/deboarding. (Category II) Control provisions include using multiple magnets per vehicle and configure in highly reliable manner.	*GM SCD 3.2.1.1.4 p. 3-66* The system is designed so that each magnet can be controlled separately. This requires an independent power supply for each SC magnet. *p. 3-68* The power supply has provisions to absorb stored energy from the magnet in the event of a quench or in the event of a power failure. In the event of a power failure, the power supply passively limits the voltage to less than 280 volts. *GM SCD 3.2.1.1 p. 3-17* There are 48 magnets in all (24 on each side of the vehicle). The total number of loops required for complete control is 26 (1 for each of 24 magnet modules (MMs) and 2 for roll control.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation/ Guidance and Levitation/ Guidance/ Magnet Failure (continued)	Reduced Levitation Produced at Normal Speeds (4.5) resulting in possible undesired contact with guideway, resulting in passenger injury. (Category II) Control provisions include use of multiple magnets per vehicle and configure in highly reliable manner.	Same as Hazard 4.4	
	Excessive Levitation Produced at Normal Speeds (4.6) resulting in possible undesired contact with guideway, resulting in passenger injury. (Category II) Control provisions include use of multiple magnets per vehicle and configure in highly reliable manner.	Same as Hazard 4.4	
	Excessive Levitation Produced During Passenger Boarding/Deboarding (4.7) resulting in passenger injury while boarding/deboarding. (Category II) Control provisions include use of multiple magnets per vehicle and configure in highly reliable manner.	Same as Hazard 4.4	
	Levitation Produced When Not Desired (4.8) resulting in levitation produced, but this is normal mode. (Category IV) No control provisions are recommended.	Hazard is defined as a Category IV Minor event, therefore, the design plan was not verified.	If passengers are unprepared or loading baggage overhead, effect might result in injury.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation/ Guidance and Levitation/ Guidance/ Magnet Failure (continued)	Guidance Not Maintained During Emergency Braking (4.9) resulting in possible loss of train/guideway integrity, resulting in passenger injury. (Category II) Control provisions include consideration of means to maintain adequate train/guideway integrity during emergency braking	*GM SCD 3.2.1.4.4 p. 3-166* The requirement was not only to provide emergency braking, but also to provide a surface for emergency wheels to contact in case large lateral motions occur, thus preventing the magnet pole face from touching the rail. The evaluation of the guideway hat section vs. the thick section is shown in Fig. 3.2.1-95.....As a result it was concluded that the hat section was the best design for our baseline.	
	Overheating Occurs in Superconducting Magnets (4.10) resulting in levitation decrease, resulting in possible undesired train/guideway contact and possible passenger injury. (Category II) Control provisions include separately cooling each magnet and make structurally reliable.	*GM SCD 3.2.1.1.4 p. 3-72* It is convenient to store liquid nitrogen and liquid helium locally in each magnet. Reservoirs have been provided under the magnets for that purpose. Each individual cryostat carries enough liquid helium and nitrogen to sustain the superconductor (magnet) for at least 24 hours until a refill could be made at the station.	Separate helium and nitrogen cooling circuits. Do the magnets require both cooling circuits to be operating for proper cooling? The helium system consists of the magnets interconnected in series with transfer lines for filling.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation/ Guidance and Levitation/ Guidance/ Magnet Failure (continued)	Magnets Make Contact With Rails at Normal Speeds (4.11) resulting in undesired rail/magnet contact, resulting in possible injury. (Category I) Control provisions include designing magnet structure and connecting hardware in highly reliable manner.	*GM SCD 3.2.1.3 p. 3-135* The 50-passenger module undercarriage build-up is developed with an underfloor support frame and a chassis (primary suspension system frame) characterized by intersecting load paths and numerous penetrations (Fig. 3.2.1-77). The primary material used for these structures and method of fabrication are extruded and forged high strength aluminum alloy 7150 mechanically joined with high performance bolts. Connected to the primary suspension system frame are 32 structural magnet support fittings and 24 magnets (Fig. 3.2.1-78). The fittings are fabricated from forged high strength aluminum alloy 7150 and attachments. Aluminum alloy beams are connected to every two magnets and adjacent support fittings to form a suspension assembly unit that provides fore and aft shear load stability and uniformly transfers the magnetic lift load to the chassis (Fig. 3.2.1-79).	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Guideway Integrity Reference Figure 2-1 Items 3.1.1(f) 3.1.1(h) 3.1.3(a) 3.2.2(a) 3.2.2(b) 3.2.2(c) 3.2.2(i)	Hazard subdivided into fourteen hazards: <u>Guideway Support Column Collapse/Shift (6.1)</u> results in train leaving guideway. (Category I) Control provisions include designing and constructing according to appropriate standards; performing ground surveys/studies on guideway locations.	Grumman examined three different conceptual guideway integrity sensing system designs. *GM SCD 3.2.2.9 p. 3-322* A comparison of these (three) approaches . . . indicated that a combination of electrical and magnetic sensing approaches is the most reliable and cost effective combination to monitor guideway integrity. *Appendix C p. c-1* Concept design criteria for maglev guideways are listed. Design will be in accordance with the following specifications and design guides: • 1989 AASHTO Standard Specifications for Highway Bridges • 1991 Uniform Building Code Part III Earthquake Design and 1983 AASHTO Guide Specification for Seismic Design of Highway Bridges. The Load Factor Design Method will be used for the design of all portions of the guideway structure, including superstructure spans, foundations and piles. Load factors and groups as given in Appendix C shall apply in place of AASHTO values.	PHA does not mention installation of guideway integrity sensing system, although it is described in the design text. Grumman states that no system of this type exists today. If this is the case, a stringent development program must be implemented.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity (continued)		*GM SCD 3.2.2.8 p. 3-316* The maintenance for the guideway will be dictated in part by the regulations of the Federal Railroad Administration or other authority in place at the time of development/construction. In general, the maintenance program will be divided, based on schedules and hierarchy of function, into daily, weekly, monthly, and yearly inspection and servicing activities to ensure the integrity of the infrastructure, subsystems, and structural components.	
	Collapse/Shift of Guideway (Lateral) Support Arm (6.2) results in guideway track(s) losing support and train leaving guideway. (Category I) Control provisions include designing and constructing according to appropriate standards	Same as Hazard 6.1	
	Collapse Shift of Center Guideway Girder (6.3) results in guideway track(s) losing support and train leaving guideway. (Category I) Control provisions include designing and constructing according to appropriate standards.	Same as Hazard 6.1	
	Collapse of Guideway Track (6.4) results in train leaving guideway. (Category I) Control provisions include designing and constructing according to appropriate standards.	Same as Hazard 6.1	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Guideway Integrity (continued)	Improper Lateral Alignment of Guideway Track Sections or Rails (6.5) results in undesired contact between train and guideway; sudden stop could occur. (Category I) Control provisions include designing and constructing according to appropriate standards and to account for loads and thermal effects; conduct periodic inspections visually and/or with instrumentation.	Same as Hazard 6.1	
	Improper Vertical Alignment of Guideway Track Sections or Rails (6.6) results in undesired contact between train and guideway; sudden stop could occur. (Category I) Control provisions include designing and constructing according to appropriate standards and to account for loads and thermal effects; conduct periodic inspections.	Same as Hazard 6.1	
	Excessive (Longitudinal) Gap Between Guideway Track Sections or Rails (6.7) results in possible propulsion transients with little overall effect. (Category IV) Control provisions include designing and constructing according to appropriate standards and to account for loads and thermal effects; conduct periodic inspections.	Hazard defined as Category IV Minor event, therefore, design plan was not verified.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity (continued)	Rail Separates From Guideway Track (6.8) results in undesired contact between vehicle and rail, resulting in injury or death. (Category I) Control provisions include designing and choosing connecting hardware to handle expected loads.	Same as Hazard 6.1	
	Improper Placement of Stator Coils in Rails (6.9) results in proper gap not be created, causing undesired contact of train with guideway. (Category II) Control provisions include to properly design coil placement.	*GM SCD 3.2.1.1.3 p. 3-39* Discussed in detail the baseline magnet and coil design .	
	Improper Lateral Alignment of Guideway/Rails When Switching (6.10) results in undesired contact of train with guideway, or train could leave guideway. (Category I) Control provisions include making switch mechanism highly reliable and using sensors in closed loop technique to detect proper position is/is not attained; substation computer should ensure safety.	*GM SCD 3.2.2.4.3 p. 3-296* To ensure the fail-safe operation of the switch in the event of any component malfunctioning, a number of measures have been devised: • Each switch section is designed to return to the straight-through position in the event of a power loss or breakdown during operation. • Dual components will be used for cylinders, pumps, motors, etc. • Dual power supply. • Mechanically operated locking bars will be used to align the switch sections meeting at the machinery pier either for the switch-open or switch-closed position.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity (continued)		*GM SCD 3.2.3.13.3 p. 3-543* The intent in the Grumman design/implementation is to utilize fault tolerant, checked redundant computers to perform many safety critical functions both on-board and at the wayside substations. The term "checked redundant computers" implies that two or more computers will operate in parallel, and their outputs will be checked or compared for agreement. Should disagreement occur, the system/function will revert to a safe state. A redundant configuration of this nature helps ensure a high level of safety because it results in a low probability of unsafe failures. While this is not the only means of achieving a high level of safety, it is the one means intended at this time in the design.	The referenced paragraph (p. 3-543) in the design plan column is located in the *3.2.3 Safety Assurance Plan* section of the SCD, not in the design requirements of the vehicle/stations. No software requirements are discussed for the various computers. No discussion or description of the switch position sensors is located in the design text.
	Improper Vertical Alignment of Guideway/Rails When Switching (6.11) results in undesired contact of train with guideway, or train could leave guideway. (Category I) Control provisions include making switch mechanism highly reliable and using sensors in closed loop technique to detect proper position is/is not attained; substation computer should ensure safety.	Same as Hazard 6.10	
	Separation of Rail From Guideway Surface When Switching (6.12) results in undesired contact of train with guideway, or train could leave guideway. (Category I) Control provisions include design switch mechanism and all connecting hardware to handle expected loads.	Same as Hazard 6.1	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity (continued)	Switch Mechanism Does Not Move or Moves Too Slowly (6.13) resulting in collision with train or switch element. (Category I) Control provisions include using sensors to detect proper position is/is not attained; substation computer should ensure safety accordingly. Switch Mechanism Switches When Not Desired (6.14) resulting in collision with train or switch element. (Category I) Control provisions include using sensors to detect proper position is/is not attained; substation computer should ensure safety accordingly.	Same as Hazard 6.10 Same as Hazard 6.10	
Guideway Obstructions Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(h) 3.1.2(f) 3.1.3(e)	Obstacle Present On Guideway Track (6.21) results in collision with object, resulting in sudden deceleration or train leaving guideway; injury/death results. (Category I) Control provisions include monitoring guideway integrity (for foreign objects), probably via guideway mounted sensors/surveillance systems.	Grumman examined five different conceptual obstacle detection system designs. *GM SCD 3.2.2.8.3, p. 3-330* Based on its excellent poor weather performance and moderate cost, Grumman recommends that the range gated TV system be considered the baseline.	PHA does not recommend any reliability design approach for obstacle detection system although hazard is classified as a Category I Catastrophic event. Unable to determine if obstacle detection system is designed with redundancy from the design text.

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Fire Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(e) 3.1.2(f) 3.1.3(e) 3.2.3(a)	Vehicle fire hazard was subdivided into two hazards: Fire Occurs On Train From Electrical Component/Subsystem Overheating (5.6) resulting in possible passenger injury. (Category I) Control provisions include properly sizing and routing wires, and designing to handle appropriate power; use circuit breakers as appropriate; also, detect fire condition and stop vehicle safely to allow egress.	*GM SCD 3.2.3.13.5 p. 3-550* When considering fire protection, it is necessary to consider fire prevention, containment, detection, and suppression. First of all, fire resistant materials and proper equipment placement are key concerns in order to preclude (as much as possible) the initiation of a fire as well as its spread. Once a fire has started, it is necessary to detect the situation and warn appropriate personnel (e.g., operator and central control). This requires the use of fire/smoke detectors and proper communication links. It also is necessary to incorporate means of suppressing the fire (e.g., fire extinguishers). Some of the potentially applicable sources of requirements for fire protection are as follows: • Federal Register, Volume 54 - materials selection • Amtrak Spec No. 352 - flammability, smoke emission, toxicity • Amtrak Spec No. 323 - wire insulation • NFPA 130 - fire protection for vehicles • FAA 49 CFR, Part 25 - aircraft	The referenced paragraph in the design plan column is located in the *3.2.3 Safety Assurance Plan* section of the SCD, not in the design requirements of the vehicle. PHA did not address fire in wayside station. PHA did not address fire in ROW or adjacent to ROW.
	Fire Occurs On-Board Requiring Passenger Egress (5.11) resulting in possible severe injury or death. (Category I) Control provisions include sensing fire condition and reporting to substation and central; stop train safely via substation or on-board control; make detection highly reliable and stop in "fail-safe" manner; install fire extinguishers in passenger compartment; permit egress onto guideway center section.	Same as Hazard 5.6	Same as Hazard 5.6

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Evacuation and Rescue Reference Figure 2-1 Items 3.1.1(h) 3.1.2(e) 3.1.3(h)	Hazard was subdivided into four hazards: Emergency Egress Required From Guideway In Elevated Areas (6.17) resulting in passengers unable to exit guideway, resulting in possible further injury (e.g., falling, hit by other train). (Category I) Control provisions include providing provisions to egress guideway (perhaps via retractable ladders on support columns) at regular intervals; provide communication links between guideway areas and control at regular intervals; have passengers remain in train until transfer to other train on adjacent guideway tracks, or less preferably, to other train on same guideway track.	See Emergency Evacuation/Response Plan evaluation.	
	Emergency Egress Required From Guideway In Tunnels (6.18) resulting in passengers unable to leave guideway resulting in further injury or injury from exposure. (Category I) Control provisions include having passengers leave tunnel area via center guideway section and egress guideway via ladder at support columns; provide communication link at intervals in longer tunnels.	See Emergency Evacuation/Response Plan evaluation.	
	Passenger Trips/Falls On Center Guideway (6.19) resulting in injury/death. (Category I) Control provisions include designing center guideway surface to provide appropriate traction for personnel.	See Emergency Evacuation/Response Plan evaluation.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Evacuation and Rescue (continued)	Emergency Condition Requires Response Personnel Access to Guideway (6.20) resulting in response personnel unable to access guideway. (Category I) Control provisions include providing means for response personnel to access/egress guideway at regular intervals; provide access road if needed.	See Emergency Evacuation/Response Plan evaluation.	
Operation Restrictions Reference Figure 2-1 Items 3.1.1(f) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.1.3(f) 3.1.3(h)	Operation restrictions were recommended for several hazards, mainly climatic/weather related.	The standard procedure for mitigating any hazard that can reduce significantly the safety of the passengers is to stop the vehicle.	
Manual Override, Security and Training Reference Figure 2-1 Items 3.1.2(f)	Manual override is used as a control provision for several hazards. Security and Training were not addressed.	Manual override is used as a control provision for several hazards. Security and Training were not addressed.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Maintenance of Safe Headway Reference Figure 2-1 Items 3.1.1(g) 3.1.2(f) 3.1.3(e) 3.2.2(d) 3.2.2(i)	Covered in C^3 hazards	Covered in C^3 hazards	
Vehicle/ Guideway Dynamics Reference Figure 2-1 Items 3.1.1(d) 3.1.1(f) 3.1.3(f) 3.2.2(d) 3.2.2(i)	Not addressed.	The dynamic interactive effects of a high-speed vehicle traveling over a geometrically imperfect flexible span was assessed in a five-degree-of-freedom analysis performed by Grumman. The Grumman conclusion from the analysis is that the baseline guideway structure is sufficiently stiff to meet its guideway deflection requirements.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Electro-magnetic Interference (EMI) Reference Figure 2-1 Items 3.1.1(h) 3.2.1(a) 3.2.2(b) 3.2.2(f)	Train Operates in Vicinity of External Electromagnetic Fields (7.10) resulting in possible unsafe operation of equipment and possible biological effects on humans. (Category I) Control provisions include locating guideways/stations away from external EMF sources; also, design safety critical equipment to be "fail-safe" relative to expected levels of EMF.	*GM SCD 3.2.3.4.3 p.3-415* Since the EMS type maglev system is very similar in power generation and distribution to other electrified urban and intercity transportation systems, the safety impacts from EMF emissions are expected to be as minimal as they are for the existing systems. The levitation magnets are the primary difference between maglev and existing electrified transportation system. However, the magnets planned for the Grumman Team's maglev system use iron core magnets and iron rails, which concentrates the magnetic flux in the iron. This design minimizes the magnetic field to the passenger or the external environment.	
Guideway Maintenance Operations Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(f)	Not addressed.	The Grumman maintenance program will be divided, based on schedules and hierarchy of function into daily, weekly, monthly, and yearly inspection and servicing activities to ensure the integrity of the infrastructure, subsystems, and structural components. Several subsystems have been identified early as requiring maintenance priority including the C^3 system, batteries, helium coolant system, superconducting magnets, and vehicle speed verification system.	Grumman recognizes the importance of a structured and systematic maintenance program to the high operational integrity of the maglev system. As the design progresses, specific tasks need to be identified and categorized by applicable inspection intervals. Grumman also realizes that the high operating speeds and consequences of component failures will dictate a higher percentage of completed scheduled maintenance than would be experienced in rail systems. In this respect it would be similar to the airlines, with a more stringent training requirement for maintenance crews and verification of completed tasks.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Magnetic Exposure of Passengers Reference Figure 2-1 Items 3.1.1(e) 3.2.1(a)	System Vehicle/Guideway/Wayside Components Generate EMF (7.11) resulting in possible unsafe operation of equipment and possible biological effects on humans. (Category I) Control provisions include to incorporate shielding as necessary to reduce passenger/crew safety critical equipment exposure; also, design safety critical equipment to be "fail-safe" relative to expected levels of EMF; also, choose design system or incorporate shielding as necessary to limit effect of EMF on personnel in vicinity of guideway	*GM SCD 3.2.3.4.3 p. 3-417* Preliminary analysis indicates that the magnetic field from the levitation magnets both inside and within less than 1 m outside of the Grumman Team's maglev concept vehicle will be 1 to 5 G. Levels along the guideline ROW for our vehicle can be expected to decrease as a function of 1/r2 where r = distance. Calculation of the spatial distribution of magnetic fields throughout the vehicle and its surroundings is more fully discussed in Subsection 3.2.1.9, where it is concluded that some shielding will be needed to meet the lower field limits specified by the Statement of Work. *GM SCD 3.2.1.9 p. 3-210* A 3-D magnetic analysis has been completed to evaluate the predicted dc magnetic field levels within and in the vicinity of our baseline vehicle without shielding. The results show that the dc fields without shielding are below 0.1 mT (1 Gauss) at the seat level and between 0.1 and 0.5 mT (1 and 5 Gauss) at the floor. There is no shielding required to meet the first two dc levels. The basic design very nearly meets the lowest dc field level without shielding. A DC attenuation of about five will meet this level. This is very easily achieved by incorporating some local steel shielding. Thin sheet steel could be used as one face sheet of the honeycomb floor structure to provide this shielding. These shields are estimated to represent approximately a 364 kg. (800 lb.) weight penalty.	If it is discovered that the electromagnetic fields are higher than Grumman estimates, shielding may be required on and around the vehicle.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Magnetic Exposure of Passengers (continued)		*p. 3-212* A detailed analysis of the AC field map would entail a very rigorous analysis which is beyond that reasonable for a conceptual design study. We are fortunate, however, that our design is similar to that of the Transrapid, and they have made magnetic field surveys on the 06 vehicle. Examination of the Transrapid test data will provide a more accurate estimate of the ac field levels than would a limited analytical study. Our vehicle exhibits a dc field level about ten times that of the Transrapid, due to the increased leakage flux inherent in the large-gap suspension. We may therefore assume that the ac distribution may be about 10 times that of Transrapid. The first ac level (0.1 mT) would thus be met with no additional shielding for frequencies above 25 Hz and the second level (0.01 mT) for frequencies above about 140 Hz. If we assume that ac means any frequency above zero, then neither condition is inherently satisfied without shielding. If we provide the steel shielding noted above to meet either the 0.1 or 0.01 mT dc level, this will also satisfy the ac requirements at any higher frequency. Any conductor serves as an effective shield for ac magnetic fields due to the induced eddy currents that are produced.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climactic/ Weather Related Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(m) 3.1.2(f) 3.1.3(a) 3.1.3(e) 3.2.2(f) 3.2.2(i)	Hazard subdivided into eleven hazards: Trains Operate In Extremely High or Low Temperatures (7.1) results in potential unsafe operation. (Category I) Control provisions include designing safety critical substation, and on-board equipment in "fail-safe" manner relative to temperature related failures.	*GM SCD 3.2.3.2.1 p. 3-391* Low temperatures should not have an operational impact on the Grumman system because it is designed to operate at -29ªC (-20°F). *GM SCD 3.2.3.26 p. 3-397* The Grumman Maglev System should not be affected by these possible high temperatures because it is designed to operate in temperatures up to 49ªC (120°F), which is above the highest temperatures recorded in the potential route areas.	
	Train Operates In Heavy Snow Conditions (7.2) resulting in sudden deceleration or reduction in emergency braking capability, leading to injury or collision. (Category I) Control provisions include to operate at reduced speed if necessary in snow conditions to allow sufficient emergency braking distance - as directed verbally via central operator; train operator could activate automatic speed limiter; use special snow plow vehicle in heavy snow conditions.	*GM SCD 3.2.3.2.1 p. 3-391* The Grumman Maglev System has a 0.10-m (4-in.) levitated clearance between the vehicle and the guideway track. This clearance will be adequate for most moderate snow falls. It is also intended, during heavy snowfall conditions (with forecast of over four inches), to minimize and impact on operations by requiring a reduction in operating speed.	If the maglev system does not operate at night, the proposed snow plow vehicle must be employed each morning after a snowfall, possibly resulting in an impact on operations.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climatic/ Weather Related (continued)	Train Operates In Ice Conditions (7.3) resulting in undesired contact with guideway or train leaves guideway. (Category I) Control provisions include operating at reduced speed if necessary to allow sufficient emergency braking distance - as directed verbally via central operator; train operator could activate automatic speed limiter; automatic detection of ice condition and speed limiting is even better.	*p. 3-393* In freezing rain condition, icicle accumulation on the sides of the track will be prevented by providing a heavy armored leading edge on the front car that will knock off icicles which could form in this area. It will be necessary to reduce the operating speeds to provide for sufficient braking distance as deemed necessary.	A closer examination of the proposed methods of dealing with snow and ice is necessary.
	Train Operates In Side Wind Conditions (7.4) resulting in undesired contact with guideway or train leaves guideway. (Category I) Control provisions include designing train/guideway interface with high reliability/integrity; sense high wind conditions automatically and limit train speed accordingly to prevent unwanted train/guideway contact.	*GM SCD 3.2.3.2.2 p. 3-394* The Grumman Maglev System is designed for operation in steady side winds up to 23.3 m/sec (50 mph), head winds up to 13.2 m/sec (30 mph), and gusting up to 33 m/sec (75 mph). This design will result in minimal impact from most wind conditions, since the levitation magnets and the associated control system will adjust to these wind forces. Operations may have to be delayed or temporarily suspended during severe wind or wind gust conditions.	
	Train Operates In Head Wind or Tail Wind Conditions (7.5) resulting in no undesired hazard effects. (Category I) No control provisions are needed because safe braking capability is not reduced.	Not addressed.	Identified hazard effect of headwind or tailwind does not agree with assigned hazard classification of a Category I Catastrophic event.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climatic/ Weather Related (continued)	Train Operates In Rain Conditions (7.6) resulting in safe braking capability reduced. (Category I) Control provisions include designing horizontal guideway surfaces with proper curvature to prevent standing water; account for possible wet surfaces in emergency braking distance allowances.	*GM SCD 3.2.3.2.3 p. 3-394* The Grumman guideway structure is designed to accommodate a rain rate of 2 in/hr by providing appropriate drainage provisions and by not building in any "true" horizontal surface that could allow for standing water.	
	Train Operates In Earthquake Condition (7.7) resulting in possible undesired contact of train with guideway or train leaving guideway. (Category I) Control provisions include designing guideway to withstand moderate intensity ground shaking; may wish to sense seismic activity as soon as possible and reduce speed accordingly.	*GM SCD 3.2.3.2.4 p. 3-394* The Grumman Maglev System guideway structure is designed to meet seismic performance Category B (< 0.19 g) for northeast corridor routes. If built in a high-intensity ground-shaking area such as California, Category C and D (>0.19g) design specifications would be required.	To design for Category C and D, some revisions in the present guideway conceptual design would be required
	Train Operates In Low/Poor Visibility (7.8) resulting in possible collision with another train or object. (Category I) Control provisions include designing system operation to be automatic including automatic detection of objects on guideway.	*GM SCD 3.2.3.2.5 p. 3-395* The occurrence of fog . . . should not have any major impact on maglev operations and safety, since command and control and route integrity systems will have the capability to automatically sense and respond to any foreign obstruction on the guideway. However, it may be good practice to operate the Grumman Maglev System at reduced speeds during very short range visibility conditions.	
		GM SCD 3.2.3.2.7 p. 3-398 Design considerations may be needed to minimize possible problems from the relatively mild sand and dust that could be encountered. Such considerations may include operating the system at reduced speeds as deemed necessary by the dust/sand conditions.	Qualification testing for sand/dust should be required for safety critical function components.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climatic/ Weather Related (continued)	Train Operates In Lightning Conditions (7.9) resulting in possible electrocution of passenger/crew. (Category I) Control provisions include providing adequate lighting protection via structural design and special provisions.	*GM SCD 3.2.1.3 p. 3-145* In addition, vehicle lightning protection is provided by incorporating the requirements of NFPA 130 (Ref 8), as applicable, into the design, and by bonding copper or aluminum mesh to non-metallic external surfaces to serve as a high conductivity electrical path to dissipate a lightning strike.	
		GM SCD 3.2.3.2.5 p. 3-398 Appropriate and applicable regulations, guidelines, and standards relative to lightning protection will be reviewed and incorporated as necessary during subsequent detailed design phases.	Detailed design for lightning protection has not been incorporated in conceptual design.
	Train Generates High Noise Levels Internally (7.12) resulting in passenger/crews injury. (Category II) Control provisions include limiting noise to acceptable levels via aerodynamic design and insulation.	*GM SCD 3.2.3.4.3 p. 3-408* Although no interior noise level estimates were made, noise insulation in the cabin is planned to be sufficient to bring the noise levels below 65 dB.	Design for insulation in vehicle structure has not been incorporated in conceptual design.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Climatic/ Weather Related (continued)	Train Generates High Noise Levels Externally (7.13) resulting in injury to maintenance personnel and others in stations and in vicinity. (Category II) Control provisions include reducing noise levels to general public via aerodynamic design and shielding techniques; maintenance workers should wear protective gear; make provision (e.g. enclosures) to shield personnel in stations from high noise levels.	*GM SCD 3.2.3.4.3 p. 3-413* Hansen et al (1992) have evaluated the noise impact from introduction of maglev trains in two northeastern U.S. transportation corridors using Transrapid 07 noise data in connection with the noise criteria proposed by UMPTA (1990) for cumulative exposure and APTA (1981) for a single passby. This analysis assumed no noise mitigation techniques were used. Using the Boston to New York transportation corridor and the UMPTA (1990) criteria, the "impact" and "severe impact" classifications were predicted to occur for any residence, respectively, within 145 m (476 ft) and 70 m (230 ft) from the guideway. The maximum predicted passby noise levels at 145 m (476 ft) and 70 m (230 ft) from the guideway were, respectively, 78 dB (A) and 86 dB (A), which are both well above the APTA (1981) guidelines. *p. 3-415* Compared to other high speed rail systems, magnetically levitated vehicles produce less noise than current forms of rail transportation at comparable speeds.	
Reference Figure 2-1 Items 3.1.2(d) 3.1.2(e)	Loss of Vehicle Heating or Air Conditioning (5.2) resulting in passenger discomfort/illness and possible stopping of train. Control provisions include making system highly reliable and sensing abnormal conditions on-board and reporting to central.	Hazard is defined as a Category III Marginal event, therefore, design plan was not verified.	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Reference Figure 2-1 Items 3.1.2(d) 3.1.2(e)	Loss of Vehicle Lighting (5.3) resulting in difficulty in egress at night, with possible passenger injury. Control provisions include making system highly reliable and sensing condition and reporting to central.	Hazard is defined as a Category III Marginal event, therefore, design plan was not verified.	
3.1.2(d) 3.1.2(e)	Loss of Power to Safety Critical On-Board Subsystems (e.g., Computers, Emergency Brake System) (5.4) resulting in loss of safety critical on-board control functions. (Category I) Control provisions include designing on-board computer/control equipment in "fail-safe" manner - emergency braking should result.	*GM SCD 3.2.1.4.4 p. 3-164* The recommended braking approach for Grumman baseline is as follows: • For normal operations the regenerative braking approach will be used. • During emergency power loss the eddy current brake in conjunction with the friction brake will be used for the high and low speed regions respectively.	On-board batteries are mentioned periodically throughout the SCD. There is no detailed discussion or description of the batteries in the SCD.

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.2.1(a)	Passengers Exposed to High Voltage (5.5) resulting in possible passenger injury. (Category I) Controlling provision includes routing and containing wires in manner to prevent passenger contact/access.	*GM SCD 3.2.3.13.5 p.3-552* The arrangement of equipment and furnishings inside the vehicle also has safety implications. Concerns include factors such as aisle width, location of wiring/high voltage equipment, seating characteristics, and lighting. Sources of potentially applicable requirements include: • ADA of 1990, 49 CFR Part 38 - interior arrangement for disabled persons • 49 CFR Part 229 - operator cab arrangement • AAR Manual of Standards and Recommended Practices - lighting • FAA 49 CFR Part 25 - seating characteristics • 49 CFR Part 229.41 - moving parts, electrical equipment locations • FAA 49 CFR Part 25.787 - storage compartments.	The referenced paragraph (p. 3-552) in the design plan column is located in the *3.2.3 Safety Assurance Plan section* of the SCD, not in the design requirements of the vehicle.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Reference Figure 2-1 Items 3.1.3(h) 3.2.1(e)	Loss of or Reduced Tilt Capability On Curves (5.7) resulting in possible passenger injury. (Category III) Control provisions include designing tilt control circuit in "fail-safe" manner; use highly reliable components.	*GM SCD 3.2.1.5 p. 3-172* Figure 3.2.1-98 shows major components of the baseline tilt mechanism. A sensor package located in the cabin senses lateral acceleration and provides the input to the tilt system. The package will contain several accelerometers and a sensor logic system to guarantee fail-safe operation. *GM SCD 3.2.3.13.3 p. 3-543* The intent in the Grumman design/implementation is to utilize fault tolerant, checked redundant computers to perform many safety critical functions both on-board and at the wayside substations. The term "checked redundant computers" implies that two or more computers will operate in parallel, and their outputs will be checked or compared for agreement. Should disagreement occur, the system/function will revert to a safe state. A redundant configuration of this nature helps ensure a high level of safety because it results in a low probability of unsafe failures. While this is not the only means of achieving a high level of safety, it is the one means intended at this time in the design.	The referenced paragraph (p. 3-543) in the design plan column is located in the *3.2.3 Safety Assurance Plan* section of the SCD, not in the design requirements of the vehicle/stations. No software requirements are discussed for the various computers.
3.2.1(e)	Excessive Tilt Produced On Curves Or Straight Sections (5.8) resulting in possible passenger injury. (Category III) Control provisions include making highly reliable and employing stop mechanism to prevent excessive tilt.	Same as Hazard 5.7	

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Reference Figure 2-1 Items 3.1.3(h) 3.2.1(e)	Train Stops On Curve (5.9) resulting in possible passenger injury. (Category III) Control provisions include deactivating tilt if stopped on curves - make mechanism highly reliable.	Same as Hazard 5.7	
3.1.2(c) 3.2.1(c)	Loss of Structural Integrity Between Upper Vehicle and Bogie (5.10) resulting in possible severe injury/death. (Category I) Control provisions include designing in highly reliable manner with redundancy.	*GM SCD 3.2.1.5 p. 3-168* The vehicle tilting system is shown in Fig. 3.2.1-77. The body is supported from the chassis structure by three pairs of active tilt links and two pair of passive (follower) tilt links.	
3.1.2(c) 3.2.1(c)	Vehicle Hits Small Flying Object (5.23) resulting in possible crew/passenger injury. (Category I) Control provisions include designing vehicle front (e.g., window for operator and front end) and side windows to withstand collision with small object at cruise speeds.	*GM SCD 3.2.1.3 p. 3-145* Glazing and nose compartment materials must meet, at a minimum, the requirements of the 49 CFR, part 223 (Ref. 7), in order to protect passengers and crew from injury as a result of objects, e.g., birds, projectile, etc., striking the windows or leading surfaces of the vehicle. Existing CFR regulations are oriented toward relatively large object impacts. The high maglev vehicle speed introduces windshield and lead surface vulnerability to impact damage from small objects, like birds and these impacts may be more analogous to an aircraft than a train. Federal Aviation Administration aircraft glazing requirements (Ref. 9) need to be considered in modifying existing regulations for this high speed maglev system.	Grumman states that FAA glazing requirements need to be considered.
3.1.2(c) 3.2.1(c)	Vehicle Hits Large Flying Object (5.24) resulting in injury/death to crew or passengers. (Category I) Control provisions include using very high quality glazed window for train front ends and using other impact resistant materials.	Same as Hazard 5.23	

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Reference Figure 2-1 Items 3.1.2(c) 3.2.1(c)	Front/Rear End Collision Occurs With Another Train (5.25-5.26) resulting in possible injury/death due to structural seat problems. (Category I) Control provisions include designing redundancy into control system and seats and connecting hardware to resist structural damage in collisions.	*GM SCD 3.2.1.3.2 p. 3-152* To optimize the vehicle's energy absorbing capability at low speed, the vehicle is designed with energy absorbing bumper assemblies fitted to the front and rear of the vehicle.	The vehicle has a coupler assembly with an anti-climb feature that prevents one vehicle from riding up over the other vehicle during collision.
3.1.3(h)	Vehicle Leaves Guideway While Negotiating Curves (5.31) resulting in death/injury. (Category I) Control provisions include designing train/guideway interface with high reliability/integrity.	*GM SCD 5.1.4 p. 5-2* The Grumman EMS design wraps around the guideway, as does Transrapid. This provides additional safety to the system by essentially preventing derailments.	
3.1.1(h)	Trespassers On Guideway (8.1) Could result in injury/death to personnel on guideway and/or passengers. Control provisions include preventing unauthorized guideway access in stations and along ROW.		

APPENDIX E. MAGNEPLANE EVENT/ISSUE MATRIX

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of System Power Reference Figure 2-1 Items 3.1.1(h) 3.1.2(b) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.2.1(a) 3.2.1(d) 3.2.3(h)	*MP SCD 5.3.10.2.2.12.b* Power System failure - Single 115V or 34.5 Kv line fails <u>Resolution</u>: A single line failure will not cause the system to fail. Loss of two lines or more will result in system loss of power to the propulsion system.	*MP SCD 5.3.10.2.2.12.b* Figure 9 - provides a simplified block diagram of the electrical power system. Redundant lines are provided to the Linear Synchronous Motor (LSM).	The effects of this hazard are not discussed or classified. The discussion is limited to features that mitigate the hazard. The maintenance class is defined as Class C (equipment stays in service, repair at the end of day).
	MP SCD 5.3.10.2.2.12.b Power system converter failure -Propulsion loss will occur in the affected block. <u>Resolution</u>: A tie breaker may be used to connect an operating converter to the affected block to remove stranded vehicle.	*MP SCD 5.3.10.2.2.12.b* Figure 9 - provides a simplified block diagram of the electrical power system. Each block has one converter that can fail and result in loss of power to the affected block.	The effects of this hazard are not discussed or classified. The discussion is limited to features that mitigate the hazard.
	MP SCD 5.3.10.2.2.10.a Linear Synchronous Motor (LSM) failure due to short circuit to ground. <u>Resolution</u>: Provide short circuit overcurrent protection devices.	Only circuit breakers are discussed.	The effects of this hazard are not discussed or classified. The discussion is limited to features that mitigate the hazard. Other overcurrent protection, such as thermal protectors, devices are not discussed in the SCD.
	MP SCD 5.3.10.2.2.10.a Linear Synchronous Motor (LSM) failure due to short circuit phase to phase. <u>Resolution</u>: Provide differential current protection devices.		Substation failure is a potential single point failure resulting in loss of LSM.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System Reference Figure 2-1 Items 3.1.1(g) 3.1.1(h) 3.1.1(l) 3.2.3(a)	*MP SCD 5.3.10.2.2.13.6* Global Communication Center - Loss of global communications <u>Resolution</u>: Control will be assumed by local control system.	*MP SCD 3.2.1.k.18* Emergency Operations - Emergency operations are to be defined for all emergency failure conditions.	The effect of a failed control center on the entire system is not discussed. Only selected loss of function cases are presented. Important failure conditions such as transmission of incorrect command is not discussed. Such loss has important implications to reduced effectiveness of system trainset collision avoidance. Loss of vehicle to wayside communications link is not addressed in PHA. Such loss is anticipated to be the most probable communication system failure mode. Hazard mitigation techniques are required in that both vehicle propulsion and braking functions are dependent on this link. Global controller is responsible for performing essential and non-essential functions. Software safety techniques and configuration management will be required to ensure system safety.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Control and/or Communication System (continued)	*MP SCD 5.3.10.2.2.13.b* FDDI Dual fiber-optic cables fail. Resolution: Since FDDI's are loops of dual cables, a single break will not result in loss of communications. Communications may be routed through wayside controllers. *MP SCD 5.3.10.2.2.13.b* Bridge Router -Failure of the bridge router. Resolution: Prohibit trains from passing from one global area to another. *MP SCD 5.3.10.2.2.13.b* Wayside controller -failure results in loss of train control in affected block. Resolution: Deploy emergency brakes to all vehicles in system.	*MP SCD 3.2.1.k.15* Data/Audio Communications: Fiber-optic communication links shall be provided for communications.	The protection of dual cables depends upon adequate separation during installation. A zonal type installation analysis may be required. Hazard mitigation techniques must be robust because trainset headways depend on these links. The seriousness of this hazard has not been analyzed. It is not clear what happens when vehicles cannot pass from one area to another. The failure of wayside controller can be serious. Vehicle safety depends on proper operation of emergency brakes and global control. This is potentially a Category I hazard.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation or Guidance and Levitation/Guidance/Magnet Failure Reference Figure 2-1 Items 3.1.2(d) 3.2.1(a) 3.2.3(h)	*MP SCD 5.3.10.2.2.2.b* Vehicle Attitude Aerodynamic Control System - Failure of the attitude system Resolution: Design does not allow any single-point failures that can result in this hazard. A complete loss of the attitude system would be caused by loss of the flight control system and LSM. *Compressor and refrigeration system failure -* Resolution: In the event of a compressor or refrigeration system failure, the system will automatically switch over to a cryogenic helium storage tank. This tank can supply 30 minutes of cryogenic helium.	Supplement D, Section C: Control surface actuators are electro-mechanical, with each control surface actuated by dual actuators, each half tied to a separate control channel.	Vehicle aerodynamic controls failure would eliminate most of the vehicle damping but would not result in a loss of vehicle magnetic suspension. Ride quality would be degraded. This is potentially a Category II hazard. The effects of this hazard are not discussed. A detailed FMECA is required to demonstrate that there are no single point failures in the attitude control system. The probability of multiple failures resulting in this hazard should be provided. All possible failure modes should be analyzed including asymmetrical control surfaces. In addition, all phases of operation should be analyzed including high speeds and failures occurring at all attitude positions. Concerns regarding the possible release of cryogenic gas cloud should be addressed. (Risk of cryogenic burns).

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Loss of Levitation or Guidance and Levitation/Guidance/Magnet Failure (continued)	Cryogenic helium storage tank failure - Since this is a back-up system, it is not considered a hazard. Resolution: A failure of the cryogenic helium storage tank will be detected by pressure and temperature sensors.		
	MP SCD 5.3.10.2.2.2.b Vehicle Attitude Aerodynamic Control System - Failure of Control Surface resulting in degraded ride quality. Resolution: A complete failure is extremely improbable and detectable by control system. The landing gear is deployed and vehicle is operated at reduced speed. Class B maintenance action required.	Supplement D, Section C: Control surface actuators are electro-mechanical, with each control surface actuated by dual actuators, each half tied to a separate control channel.	The PHA states that a complete failure is extremely improbable. An analysis is required to prove that the system meets the requirements. Loss of levitation is potentially a Category I event.
	MP SCD 5.3.10.2.2.2.b Vehicle Attitude Aerodynamic Control System - Failure of LSM due to winding failure, converter failure or general loss of power. Resolution: *At high speeds, the control surfaces* dominate the LSM; this failure is not serious. The vehicle slowed due to loss of propulsion.		
	MP SCD 5.2.10.2.2.9.b Box Beam/Levitation Sheets Resolution: Provide continuous ride quality monitoring to detect abnormal alignment, deflection or damage.	MP SCD 3.2.2. Guideway monitoring shall be provided and include Closed Circuit Television (CCTV), Power distribution monitoring, ride quality monitoring, fencing and visual inspections.	This is not a PHA. It is a description of design features intended to prevent the kinds of failures that should be identified and discussed. The effects of levitation due to guideway sheet faults are not discussed or classified.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Levitation or Guidance and Levitation/Guid-ance/Magnet Failure (continued)	Provide box beam continuity span expansion joints and provide electrical signal to ensure guideway integrity.	MP SCD 3.2.2.c.1 Thermal Expansion. The baseline levitation plate box beam includes thermal expansion joints to accommodate aluminum expansion and contraction.	Monitoring of the guideway is provided.
	MP SCD 5.3.10.2.2.4.b Superconducting Magnets and Cryogenic Refrigeration. Failure of propulsion magnet cryostat will result in warming of the superconducting coils. Quenches in five other coils will be triggered by quench detection system. Levitation magnet cryostat failure - a failure of the levitation cryostats will initiate a quench in all levitation magnets.		The hazards effects are not discussed. The potential hazard associated with magnet quenching induced by severe vibration or excessive shock is not addressed.
	Cryogenic transfer line failure will result in loss of cryogenic helium flow to the associated cryostats. <u>Resolution:</u> The cryostats will be valved off to maintain the thermal capacity in the superconducting state to allow the train to reach the next magport.		The hazards effects are not discussed. The potential hazards associated with vehicle motion dynamics during a levitation magnet quench, quench detection and opposite magnet induced quench should be addressed.
	Distribution header cryostat failure will result in loss of cryogenic helium flow to the associated cryostats. <u>Resolution:</u> The cryostats will be valved off to maintain the thermal capacity in the superconducting state to allow the train to reach the next magport.		There are three hazards associated with on-board cryogenics: • Physiological effects • Embrittlement of materials

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity Reference Figure 2-1 Items 3.1.1(f) 3.1.1(h) 3.1.3(a) 3.2.2(a) 3.2.2(b) 3.2.2(c) 3.2.2(i)	MP SCD 5.3.10.2.1.c Guideway Monitoring is defined under system level responses analyses – guideway Monitoring shall be provided to detect problems.	MP SCD 3.2.2. Guideway monitoring shall be provided and include Closed Circuit Television (CCTV), power distribution monitoring, ride quality monitoring, fencing and visual inspections.	CCTV, ride quality monitoring and visual inspections may not mitigate this hazard for the following reasons: • CCTV is ineffective at night and during foggy conditions • Ride quality monitoring is reactive rather than a proactive method for detecting guideway integrity • Visual inspections rely on human performance.
	5.3.10.2.2.11.b Magswitch - Loss of control signal - Resolution: Global control system shall monitor the interlocks and take re-routing action.		
	5.3.10.2.2.11.b Magswitch - Loss of control contactor power supply Resolution: The switch reverts to straight-through condition and can be verified by interlocking signals.	Magswitch monitoring is not discussed in the SCD.	
	5.3.10.2.2.11.b Loss of vehicle propulsion coils - A sudden complete failure of all propulsion coils results in a Category I hazard. Many intermittent failures such as one coil failing can be detected before a dangerous condition arises. Resolution: The only way an undetected loss of coils can occur is when the vehicle is subjected to sudden and sever impact. The failure of the switch to operate does not constitute an independent hazard.	Magswitch monitoring is not discussed in the SCD.	A failure of the propulsion coils while the vehicle is in a switching mode may result in a Category I hazard.

EVENT/ ISSUE	DOCUMENTATION IN SCD: ANALYSIS REFERENCE	DOCUMENTATION IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Guideway Obstruction Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(h) 3.1.2(f) 3.1.3(e)	*MP SCD 5.3.10.2.1.d Guideway Obstacle Foreign objects in -* Resolution: Provide fences in selected areas, wide gaps between fences and guideway. To detect large objects, operators will patrol guideway at reduced speeds and in selected areas, guideway monitoring shall be used. If a vehicle strikes an object, on-board accelerometers will alert the system.	MP SCD 3.2.2 Guideway Monitoring includes: CCTV, Power Distribution, vehicle ride quality, visual inspections and structures (fencing).	This is potentially a Category I hazard. The hazardous effects of objects is not defined or classified. It appears that continuous monitoring of the guideway is required. Vehicle patrols, reduced speeds and accelerometers are systems are reactive to the hazard and do not mitigate the hazard. • CCTV is ineffective at night and during foggy conditions • Ride quality monitoring is reactive rather than a proactive method for detecting guideway integrity • Visual inspections rely on human performance.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Guideway Obstruction (continued)	*MP SCD 5.3.10.2.1.e* Snow is defined under system level responses analyses - Snow: Normal operation of the system generates enough heat in the levitation sheets to melt a substantial amount of snow and ice. The system shall operate at reduced speeds.	MP SCD 3.2.2.g.5. Guideway Surface wear and Heating. An analysis is provided to estimate the radiated energy of the guideway above the ambient temperate.	Ferromagnetic debris on the track presents a serious hazard, potentially damaging the vehicle magnet. The analysis of guideway heating is based on 20 second headways. 20 second headway are not practical in real world application at 134 m/s. Relying on levitation sheet induced current melting of snow may result in formation of potentially dangerous ice sheets during system non-operating periods if trough damage is inadequate. This mitigation of this hazard requires a thermal analysis to ensure that all temperature conditions. This is potentially a Category I hazard. Potential ice build-up on aerodynamic control surfaces is not addressed. Magswitch monitoring is not discussed in the SCD.

EVENT/ ISSUE	DOCUMENTATION IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Fire Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(e) 3.1.2(f) 3.1.3(e) 3.2.3(a)	*MP SCD 5.3.10.2.4 Fire Protection* -Passenger injuries are improbable. Resolution: Provide three hand fire extinguishers located in the passenger compartment, one extinguisher in the operator compartment, ventilation for removing smoke and ensure the materials meet fire requirements. No fuel carried on-board	MP SCD 3.2.1.c.1.15.3.13 Fire Protection (FAR 25.851) a minimum of three fire extinguishers shall be located in the passenger compartments.	Magneplane states that finish materials will meet strict combustibility and flame requirements. More consideration should be given to smoke emission. Magneplane provides information related to fire prevention and suppression. More consideration should be given to fire detection. In particular, fire detection of isolated, unstaffed wayside locations.
Evacuation and Rescue Reference Figure 2-1 Items 3.1.1(h) 3.1.2(e) 3.1.3(h)	*MP SCD 5.3.10.2.3 Emergency Egress-* A hatch-type exit will be provided at each end of the vehicle. After leaving the vehicle, the passengers can walk down the guideway to the nearest magport. Standard regulations for emergency egress shall apply.	MP SCD 3.2.1.e.14 Escape hatches are provided. (See Chapter 7 of this report.)	The Magneplane approach is limited since: • Handicapped and elderly may have difficulty going down stairs • LSM heating may be too hot for passenger to evacuate onto • Hatches may be small and difficult to evacuate.
Operation Restrictions Reference Figure 2-1 Items 3.1.1(f) 3.1.2(d) 3.1.2(f) 3.1.3(e) 3.1.3(f) 3.1.3(h)	*MP SCD 5.3.10.2.1 System-Level Responses* - Operational restrictions are covered by system-level responses analysis. These include operations during: wayside control or communications failure, global control or communications failure, guideway integrity and obstacle operations and weather (including earthquakes).	*MP SCD 3.2.3.a.3 Operational Requirements* A Global Control Center will operate the maglev system with information from the guideway position data, vehicles and high resolution displays. *MP SCD 3.2.3.a.3.1 Decision Support Systems (DSS)* - The DSS is a network of information used to monitor traffic and prepare advisories.	Several operational issues that should be discussed include: • The viability of 20 second headways • Failure management

EVENT/ ISSUE	ADDRESSED IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Manual Override, Security, and Training Reference Figure 2-1 Item 3.1.2(f)	Not addressed in PHA.	Not addressed in SCD.	Operational issues need to be discussed.
Maintenance of Safe Headway Reference Figure 2-1 Items 3.1.1(g) 3.1.2(f) 3.1.3(e) 3.2.2(d) 3.2.2(i)	Not addressed in PHA.	*MP SCD 3.2.3.a.1.1.1 Global Control and Communication* – The command, control and communication (c^3) is provided by Global, wayside and vehicle systems. The vehicle provides velocity, aerodynamic and magnetic stabilization data to the wayside controller. In turn the wayside controller transmits this data to the global controller. The Global controller performs logic calculations and provides feedback to the wayside controller and vehicle.	Based on an analysis provided by Magneplane, the achievable headways can be as low as 20 seconds. Since a collision is a potential Category I hazard, this spacing may result in too great of a collision probability.
Vehicle/Guide-way Dynamics Reference Figure 2-1 Items 3.1.1(d) 3.1.1(f) 3.1.3(f) 3.1.3(h) 3.2.1(e)	Not discussed in PHA.	*MP SCD 3.2.2.g* Magneplane provided a simulation model of the vehicle and guideway.	As previously mentioned, there are safety concerns associated with the vehicle remaining on the guideway under all conditions.

EVENT/ ISSUE	ADDRESSED IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Electro-magnetic Interference Reference Figure 2-1 Items 3.1.1(h) 3.2.1(a) 3.2.2(b) 3.2.2(f)	Not discussed in PHA.	Not discussed in PHA.	EMI effects on communication systems must be resolved.
Doors and Door Interlocks Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m)	*MP SCD 5.3.10.2.5.a* Four doors are provided; one at the front, rear and both sides. The doors are sliding and moved open and closed by compressed air. The doors shall have the following safety features: 1) Safeguards against inadvertent opening 2) opened from inside or outside 3)electrically interlocked to the vehicle control systems.	*MP SCD 3.2.1.c.1.15.3.2.* Doors shall comply with FAR 25.783.	
Guideway Maintenance Operations Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m) 3.1.2(f)	Not discussed in PHA.	*MPSCD 3.2.3.i.5* Guideway inspections will be performed every six months.	Although inspections are considered by Magneplane, there are many issues that need to be resolved in this area.

EVENT/ ISSUE	ADDRESSED IN SCD		COMMENTS
	ANALYSIS REFERENCE	CONCEPT DESIGN FOR MITIGATING HAZARDS	
Magnetic Field Exposure of Passengers Reference Figure 2-1 Items 3.1.1(e) 3.2.1(a)	*MP SCD 5.3.10.2.2.8* Shielding is performed by conventional coils operating at low power levels. The windings will be distributed in the floor and walls of the vehicle. Coils will be operated in a series/parallel configuration that will assure that total loss of shielding will not be caused by a single failure. *MP SCD 5.3.10.2.2.8* Loss of power <u>Resolution:</u> Loss of shielding will be detected by on-board sensors to ensure that passengers are not exposed to magnetic radiation. *MP SCD 5.3.10.2.2.8* Coil Failure <u>Resolution:</u> The failure of an individual coil cannot cause a loss of the entire shielding system. This is a Class C maintenance condition.	*MP SCD 5.3.8.3.6* The magnitude of magnetic fields are discussed in the environmental report. *MP SCD 3.2.1.i* Electromagnetic shield coils are provided. These coils will be located beneath the floor and in walls of the bogie sections of the vehicle. These would decrease the fields experienced by the passengers.	The potential hazard of magnetic radiation shielding failure is not discussed in the SCD. Monitoring at fields is not discussed in the SCD
Seating Handrails and Steps Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m)	*MP SCD 5.3.10.6* Standard aircraft style seating will be used. Handrails, steps, and other hardware will meet applicable safety standards.	*MP SCD 3.2.1.c.1.15.3.3* Seats shall comply with FAR 25.785.	It is not clear if Magneplane proposes passenger seat belts in the SCD. Emergency brake deployment may cause excessive g forces on standing passengers.

EVENT/ ISSUE	ADDRESSED IN SCD: ANALYSIS REFERENCE	ADDRESSED IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Landing Gear and Emergency Brakes Reference Figure 2-1 Items 3.1.1(h) 3.1.1(m)	*MP SCD 5.3.10.2.2.7.d* Landing gear and emergency brakes shall meet the following requirements: 1)Emergency braking and landing gear equipment will undergo a pre-flight check. Failures detected at this stage are not considered to be hazardous. 2) Each strut is independent. No single point failure can result in a loss of the emergency landing brake system. Failure of one extension mechanism results in vehicle settling unevenly. This is a Category IV hazard. Unexpected deployment of one extension mechanism results in uneven operation of the vehicle. Resolution: Aerodynamic and LSM control compensates for uneven operation. This is a Category IV hazard and Class B maintenance action.	*MP SCD 3.2.1.c.1.12* Landing gear shall be a system of retractable skids and shall support the vehicle at speeds less than 60 m.p.h.	Preflight checks and other operations are not discussed. The potential hazards associated with landing pad and/or emergency braking pad deployment failure in the event of magnetic levitation system and/or LSM failure at high speeds should be addressed.

EVENT/ ISSUE	ADDRESSED IN SCD: ANALYSIS REFERENCE	ADDRESSED IN SCD: CONCEPT DESIGN FOR MITIGATING HAZARDS	COMMENTS
Climatic/ Weather Related Reference Figure 2-1 Items 3.1.1(f) 3.1.1(g) 3.1.1(m) 3.1.2(f) 3.1.3(a) 3.1.3(e) 3.2.2(f) 3.2.2(i)	*MP SCD 5.3.10.2.1.e* - Global control will be connected to weather and disaster networks. Snow or ice: Normal heating of the will eliminate snow and ice. Operations will continue at reduced speeds. High Winds, Hurricanes, Tornadoes - The guideway will shelter the vehicle from crosswinds. The vehicles will remain in magports if winds are too extreme. Thunderstorms: The vehicles shall withstand lightning strikes similar to airplanes. Rain and Fog: Rain and fog will not affect the vehicle performance. Earthquake: Global control will be connected to local earthquake networks.	*MP SCD 3.2.2.g.5* Guideway Surface Wear and Heating - An analysis is provided to estimate the radiated energy of the guideway above the ambient temperature.	The calculations for guideway heating is based on 20 second headway
Tunnels Reference Figure 2-1 Items 3.1.3(f)	Not discussed in PHA.	*MP SCD 3.2.2.k* - The tunnel design and aerodynamic properties are discussed with respect to drag.	More development will be required to ensure all hazards associated with tunnels are identified and resolved.

APPENDIX F. MATRIX OF PROPOSED MAGLEV SAFETY REQUIREMENTS

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
1. VEHICLE STRUCTURE AND INTERIOR DESIGN	The equipment and its mountings shall be designed to withstand, without separation, the ultimate inertia loads resulting from a high speed landing.	ALL
	For maglev systems that incorporate composite materials, matrix material surfaces exposed to ultraviolet light must be painted to prevent chemical changes and degradation of the material properties.	FM, MP
	Maglev vehicle design should provide for controlled structure collapse to dissipate the vehicle kinetic energy as well as limit accelerations levels, preserve occupant compartment structural integrity to provide at least a minimum survival time, and restrict the impact forces that are applied to occupants during secondary contacts to accepted human tolerance levels.	ALL
2. PROPULSION, NORMAL BRAKING, AND EMERGENCY BRAKING	*Complete loss of braking capability shall be shown to be improbable through the use of appropriate analyses.*	ALL
	Uncommanded braking due to system malfunctions of the normal or emergency braking systems shall be shown to be remote through the use of appropriate analyses.	ALL
	There shall be no significant damage to the vehicle or the guideway as a result of contact between the two during normal or emergency braking.	ALL
	Normal and emergency braking systems shall be designed to comply with the braking deceleration rates specified in <u>APTA Guidelines for the Design of Rapid Transit Facilities</u>, Section 4.5. No single failure in the LSM propulsion system or braking systems will cause these rates to be exceeded.	ALL
	The design shall incorporate an emergency braking system that is independent of the LSM propulsion/braking system that does not require an external power supply, and that has the capability of bringing the vehicle to a complete stop from any normal operational speed.	ALL
	A redundant or fault-tolerant design shall be used for the computer and its supporting equipment, such as power supplies and sensors.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
3. SUSPENSION, LEVITATION, AND LATERAL GUIDANCE	*The malfunction of levitation and/or lateral guidance systems resulting in deceleration forces greater than (TBD) shall be shown to be improbable through the use of appropriate analyses.*	ALL
	The inadvertent deployment of landing gear or skids that result in guideway contact and deceleration forces greater than (TBD) shall be shown to be improbable through the use of appropriate analyses.	FM, GM, MP
	The failure of levitation and/or lateral guidance function(s) that could potentially cause the vehicle to depart the guideway shall be shown to be improbable through the use of appropriate analyses.	BEC, FM, MP
	Inadvertent deployment of rubber tire landing gear at speeds greater than (TBD) kmph shall be shown to be improbable through the use of appropriate analyses.	FM, GM
	Malfunction of the active tilting mechanism that results in lateral g-forces greater than (TBD) shall be shown to be remote through the use of appropriate analyses.	BEC, FM, GM
	A superconducting magnet stability margin could be defined as winding operating current (I) divided by the winding critical current (Ic). A preliminary maximum magnet stability margin could be set at 0.8 for the most demanding magnet operating point and with worst case operation environment conditions.	ALL
	Compliance with the superconducting magnet stability margins shall be validated by full-scale magnet testing under worst-case operating point and magnet operation environment conditions. The testing operation environment conditions shall include but not necessarily be limited to the cryogenic coolant temperature and/or temperature spectrum, the coolant phase mix, the coolant flow rate, physical vibration and/or shock and such electromagnetic field transients as could induce winding ac losses.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
3. SUSPENSION, LEVITATION, AND LATERAL GUIDANCE (Cont.)	*Cryogenic pressure vessels shall be designed in accordance with pressure vessel design criteria and burst safety factors outlined in FRA regulations 49 CFR, Part 229.49 and ASME Boiler and Pressure Vessel Code.*	ALL
	The on-board cryogenic cooling system, including any transfer piping, shall be located outside of passenger/crew compartments where such compartments shall be defined by relatively gas-tight walls, bulkheads, floors, and access doors.	ALL
	Provision for vehicle blow-off of cryogenic gas via cryogenic system pressure relief valves shall be located as remotely as possible from vehicle exterior doors, emergency exits, and cabin air circulation inlets.	ALL
	The cryogenic cooling system shall incorporate redundant pressure relief valves to prevent system overpressurization.	ALL
	All cryogenic equipment containing supercooled materials shall be designed to function for life at operating temperatures and resist embrittlement. Additionally, other vehicle structures which are adjacent to cryogenic equipment should be insulated from supercooled materials to preclude embrittlement of those structures.	ALL
	Critical equipment which could be damaged by tire failures shall not be installed in the vicinity of rubber tire type landing gear.	FM, GM

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
4. ON-BOARD POWER SYSTEM	*The loss of the on-board electrical power supply must be shown to be improbable through the use of appropriate analyses.*	ALL
	Systems that incorporate chemical fuel cells shall isolate all fuel cells, related equipment, and emissions from the passenger area.	BEC
	Systems that incorporate methanol fuel cells shall ensure that burning methanol is visible to the human eye.	BEC
	Systems that rely on battery systems for safety-critical functions must provide battery health monitoring and a battery fail indication to ensure batteries are available prior to departing a station.	ALL
	Systems that incorporate lead-acid batteries must provide a fail-safe ventilation system to ensure that hydrogen gas is properly exhausted.	MP

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
5. MAGNETIC SHIELDING	*Malfunction of field canceling type systems which result in significant loss of field canceling performance shall be shown to be remote through the use of appropriate analyses.*	BEC, MP
	The magnet configuration, location, and field shielding shall limit passenger and crew magnetic field exposure to the following levels: *Seat Level Maximum = 10 Gauss ac 10 Gauss dc* *Platform Level Maximum = 10 Gauss ac 10 Gauss dc* *Emergency Passageway = 10 Gauss ac 10 Gauss dc*	ALL
6. FIRE PROTECTION	*The loss of a vehicle, wayside or station fire detection or suppression system must be shown to be remote through the use of appropriate analyses.*	ALL
	Remote wayside locations require fire prevention, detection, and suppression measures.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
7. GUIDEWAY DESIGN	*The separation of any coils from the guideway shall be shown to be improbable through the use of appropriate analyses.*	ALL
	All equipment attached to the guideway with mechanical fasteners (bolts, rivets, etc.) shall use redundant fastening systems such that the failure of individual fasteners can be tolerated with no loss of the structural integrity of the attachment.	ALL
	All fastener system designs shall provide for easy detection of failures by inspection without the use of special tools or instruments, and preferably with no disassembly of equipment.	ALL
	All high voltage power lines shall be shielded or otherwise protected to prevent possible contact with live wires by any person.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
8. GUIDEWAY SWITCH	*The incorrect indication of a switch position must be shown to be improbable through the use of appropriate analyses.*	ALL
	The movement of a switch while the vehicle is in switch, or unable to stop before the switch position changes must be shown to be improbable through the use of appropriate analyses.	BEC, GM
	The asynchronous operation of moveable beam actuators, which could result in structural weakening or misalignment of the beam, shall be shown to be improbable through the use of appropriate analyses.	ALL
	Switch position must be continuously monitored.	ALL
	Moveable switch beams shall be monitored for integrity to ensure that beam damage resulting from the asynchronous operation of the beam actuators is annunciated.	ALL
	The switch must be mechanically locked into desired position and verified.	BEC, GM
	Switch equipment must be placed on the safety-critical maintenance list.	ALL
	Switch beams must be able to withstand loads under all operating conditions, both normal and emergency.	BEC, GM

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
9. GUIDEWAY MONITORING	*The loss of guideway integrity monitoring must be shown to be improbable through the use of appropriate analyses.*	ALL
	The loss of guideway obstacle monitoring must be shown to be improbable through the use of appropriate analyses.	ALL
	The entire guideway must be continuously monitored for both obstacles and integrity under all operating conditions (e.g., night, snow, etc.)	ALL
	The guideway monitoring systems must have an emergency back-up power source, independent from the primary source.	ALL
	Loss of guideway monitoring must be immediately detected by Central Control.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
10. POWER SYSTEM AND DISTRIBUTION	*The loss of system power to a substation block resulting in loss of power to the LSM must be shown to be remote through the use of appropriate analyses.*	ALL
	Inability to remove guideway power from LSM windings must be shown to be improbable through the use of appropriate analyses.	MP
	Systems responsible for fault monitoring shall be periodically tested to ensure system integrity.	ALL
	In general, electrical power used to supply safety-critical systems including communications, train controls, and fire systems shall be monitored for failure and out-of-tolerance conditions. This monitoring shall include overvoltage, undervoltage, overfrequency, underfrequency, and phase-to-phase differential current. Any failure or out-of-tolerance condition shall be annunciated.	ALL
	Systems that incorporate emergency evacuation onto guideways containing LSM windings must provide an indication to show that it is safe to walk on the LSM.	MP

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
11. COMMUNICATIONS, COMMAND, AND CONTROL	*The loss or malfunction of the C^3 system must be shown to be improbable through the use of appropriate analyses.*	ALL
	The loss or malfunction of the train location and speed detection function of the C^3 system must be shown to be improbable through the use of appropriate analyses.	ALL
	The malfunction of the berthing verification and door control functions of the C^3 system must be shown to be improbable through the use of appropriate analyses.	ALL
	Any failure of subsystems, equipment, or components within the C^3 system that may lead to an unsafe state must be self-detecting. Self-detecting failures will result in vehicles stopping or operating at a restrictive safe speed.	ALL
	RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification, should be used for assessing and controlling the application of software in safety-critical functions.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
12. SYSTEMS OPERATIONS AND MAINTENANCE	The preliminary list of safety-critical subsystems requiring maintenance priority includes: vehicle tilt mechanism, retractable wheel assembly, C^3 system, batteries, helium coolant system, superconducting magnets, and vehicle speed verification system.	ALL
	The preliminary list of safety-critical guideway structures requiring maintenance priority includes: guideway bearing supports, external tendons, track slab, outriggers, spine girder, emergency egress stairs, rail alignment, linear synchronous motor windings, and a switch mechanism.	ALL
	A stringent training requirement for maintenance crews and verification of completed tasks, similar to the airlines, is required.	ALL
	A stringent training requirement for central control operators, similar to air traffic controllers, is required.	ALL
	Maintenance personnel will require special training to safely handle cryogenic servicing and maintenance.	ALL
	A record of on-board equipment operating states, just prior to incidents and accidents, should be made available through the use of a continuous loop data recording mechanism.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
13. ENVIRONMENTAL EFFECTS	*The equipment and structures shall be designed to operate normally without any degradation of performance or integrity when exposed to worst-case limits of any applicable environmental conditions.*	ALL
	All equipment and structures shall be designed to operate without degradation in a maximum high ambient temperature of (TBD).	ALL
	All equipment and structures shall be designed to operate without degradation in a minimum low ambient temperature of (TBD).	ALL
	All equipment installed on-board the vehicle shall be able to withstand (TBD) g forces that are representative of peak loads caused by wind gusts and high speed landings.	ALL
	If the equipment is installed in a location subject to exposure to fuel or fuel vapor, hydraulic fluid, lubricating oil, solvents, cleaning fluid, fire extinguishant, or insecticide in the course of normal maglev operations, then the equipment shall be designed to operate with a wetted surface without degradation for a period of (TBD) hours.	ALL
	Equipment not installed in the volume of the vehicle shall be designed to withstand, without degradation, sand and dust of (TBD) particles per million for (TBD) hours.	ALL
	Equipment installed in locations where it is subjected to falling water or driving rain or where water is sprayed on it from any angle in the course of normal maglev operations must be designed for water proofness.	ALL
	All equipment shall be designed to withstand, without degradation, operation over a temperature range of (TBD) at relative humidities from 0 to 100 percent.	ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
13. ENVIRONMENTAL EFFECTS (CONT.)	*System components which contain material potentially nutrient fungus shall withstand exposure to contamination by a culture of various fungi at the following conditions:* *Relative Humidity: 95 percent* *Temperature: 30°C (86°F)* *Duration 28 days*	ALL
	All equipment shall be installed to withstand, without a degradation of performance, operational shock loads of (TBD) g peak for (TBD) milliseconds.	ALL
	All equipment installed on-board the vehicle shall meet vibration requirements defined by the worst-case vibration expected on the vehicle.	ALL
	All equipment shall be designed to be free of detrimental effects of lightning-induced transients.	ALL
	Based on the historical data of seismic activity in the specific location, the maglev system shall be designed to meet category A, B, or C performance requirements of the American Association of State Highway and Transportation Official's Standard Specifications for Highway Bridges.	ALL
		ALL

MAGLEV SUBSYSTEM	SAFETY REQUIREMENTS	SCD APPLICATION
14. EMERGENCY RESPONSE	*Failing to reach the "safe stopping" zone shall be shown to be improbable through the use of appropriate analyses. If this requirement cannot be satisfied, then a means to safely evacuate passengers shall be provided along the entire guideway.*	BEC
	A failure of the tilting mechanism that impedes emergency evacuation shall be shown to be improbable through the use of appropriate analyses. If this requirement cannot be satisfied, then it shall be shown by analysis and testing that passenger evacuation, including elderly and physically challenged passengers, can be achieved with a tilting mechanism failed in the worst-case position.	BEC, FM, GM
	The loss or malfunction of the communication function of the C^3 system must be shown to be remote through the use of appropriate analyses.	ALL
	Systems that incorporate emergency evacuation onto the guideway must provide an indication to the crew and passengers that it is safe to evacuate (i.e., power to the LSM has been removed, the guideway temperatures are not excessive, train operations have been stopped in the area of evacuation, etc.).	ALL
	Assuming worst case equipment failure modes and environmental conditions, there should be a means for passengers to evacuate from stalled vehicles along the entire guideway, including switch zones and superelevated curves, to a point of safety.	ALL

*U.S. G.P.O.:1993-301-717:80419